

**Cybersecurity in the era of emerging technologies in
accounting and finance: Towards an innovative integrated
strategic framework**

Huma Habib Shadan

**Thesis submitted for the fulfilment of the requirements for the
degree of Doctor of Philosophy.**

**Victoria University, Australia
Institute for Sustainable Industries & Liveable Cities**

December 2025

Abstract

Background

The rapid digitalisation of accounting and finance systems has revolutionised how financial data is recorded, processed, and safeguarded. However, this transformation has simultaneously heightened exposure to sophisticated cyber threats. As organisations transition toward cloud-based infrastructures and AI-assisted accounting platforms, the need for resilient, technology-integrated cybersecurity frameworks has become increasingly critical.

Present Literature Review Research

Existing studies across accounting and information systems emphasise emerging technologies, Blockchain for immutability, Quantum Computing for cryptographic resilience, Machine Learning for anomaly detection, and Game Theory for strategic defence. However, most prior research examines these technologies in isolation, lacking integration into a unified cybersecurity framework tailored to accounting and finance. This fragmentation limits the current literature's ability to address multi-layered cyber risks within digital accounting ecosystems.

Limitations of the Existing Literature Review

While previous literature establishes the technical potential of each technology, it often omits a comprehensive linkage between cybersecurity mechanisms and accounting governance. Studies rarely assess the empirical performance of fraud detection within accounting datasets or explainability for audit compliance. Additionally, little attention has been paid to how these technologies can coexist under a single architecture that enhances transparency, regulatory assurance, and strategic cyber resilience.

Aim and Objectives

This doctoral research aims to develop a multidisciplinary cybersecurity framework that strengthens the integrity, confidentiality, and resilience of accounting and finance information systems. It integrates four transformative technologies: the first is Blockchain, the next is Quantum Computing, the third is Machine Learning, and the last is Game Theory, into a cohesive model termed the BQMG-AIS Framework (Blockchain, Quantum, Machine Learning, and Game Theory integrated with Accounting Information Systems).

Methodology

A multi-method approach combining systematic literature review, conceptual modelling, and empirical analysis was adopted. Empirically, three benchmark datasets, the first one European Credit Card Fraud, the second is the IEEE-CIS Fraud Detection, and the third the PaySim Mobile Money, were analysed using Logistic Regression, Random Forest, and XGBoost. Evaluation metrics, including AUC-ROC, precision, recall, F1-score, and SHAP interpretability, ensured transparency and auditability, which are critical to accounting governance.

Findings

The empirical results demonstrated high detection accuracy and interpretability, confirming the effectiveness of machine-learning models in identifying financial fraud within imbalanced datasets. The conceptual model establishes Blockchain for immutable audit trails, Quantum Computing for post-quantum cryptography, and Game Theory for strategic attacker–defender optimisation. Together, these layers form a comprehensive, multi-tiered cybersecurity framework that is validated both conceptually and empirically.

Contributions

This research contributes a novel, interdisciplinary cybersecurity architecture that unites technical innovation with accounting governance principles. It bridges quantitative (machine learning–based testing) and qualitative (conceptual synthesis) methodologies, offering auditors, regulators, and financial institutions a transparent, scalable, and future-ready cybersecurity solution aligned with Accounting Information Systems.

Conclusion

Future accounting systems must be both technologically advanced and strategically intelligent, capable of defending against evolving cyber threats while maintaining transparency, compliance, and trust. The BQMG-AIS Framework advances the domain of accounting cybersecurity by uniting Blockchain, Quantum Computing, Machine Learning, and Game Theory into a cohesive, auditable, and post-quantum-ready cybersecurity model for the digital finance era.

Student Declaration

“I, Huma Habib Shadan, declare that the Doctor of Philosophy thesis entitled “Cybersecurity in the era of emerging technologies in accounting and finance: Towards an innovative integrated strategic framework” is no more than 85,000 in length, including quotes and exclusive of tables, figures, appendices, bibliography, references and footnotes. This thesis contains no material that has been submitted previously, in whole or in part, for the award of any other academic degree or diploma. Except where otherwise indicated, this thesis is my own work”.

I have conducted my research in alignment with the Australian Code for the Responsible Conduct of Research and Victoria University’s Higher Degree by Research Policy and Procedures.

This thesis has been edited for clarity of expression, punctuation and grammar using the Grammarly tool. This use complies with VU guidelines on use of editors in HDR theses and overall, VU policy on use of AI in research.

Signature

A solid black rectangular box used to redact the student's signature.

Date

08 December 2025

Dedications

This thesis is dedicated to my beloved family, whose unwavering love, encouragement, and patience have been my greatest strength throughout this journey. To my parents, for instilling in me the values of perseverance and integrity that have guided every step of my academic and professional life. To my close friends and loved ones, thank you for your constant belief in me during the most challenging moments of this research.

This work is also dedicated to all researchers striving to make accounting and finance systems safer and more transparent through innovation and ethical inquiry.

Acknowledgements

I would like to express my deepest gratitude to my Principal Supervisor, Professor Sardar Islam, for his invaluable guidance, continuous support, and profound insights throughout the development of this thesis. His expertise, mentorship, and encouragement have been instrumental in shaping both the conceptual and empirical aspects of my research.

My sincere thanks also go to my Associate Supervisors, Dr Sheeba Armoogum and Dr Azadeh Alavi, for their thoughtful feedback, technical advice, and intellectual encouragement. Their perspectives have enriched this work and strengthened its contribution to the field of accounting, cybersecurity and emerging technologies.

I am especially grateful to Victoria University, the VU Business School, and the Graduate Research Office for providing the resources, facilities, and an intellectually stimulating environment that made this research possible.

Special thanks are due to my fellow doctoral colleagues and research peers for their companionship, discussions, and support throughout this journey.

Finally, I extend heartfelt appreciation to my family and friends for their patience, understanding, and belief in me. Their encouragement gave me the strength to persevere through the most demanding stages of this research.

Table of Contents

ABSTRACT.....	II
BACKGROUND.....	II
PRESENT LITERATURE REVIEW RESEARCH	II
LIMITATIONS OF THE EXISTING LITERATURE REVIEW	II
AIM AND OBJECTIVES	II
METHODOLOGY	III
FINDINGS	III
CONTRIBUTIONS	III
CONCLUSION.....	III
STUDENT DECLARATION	IV
DEDICATIONS.....	V
ACKNOWLEDGEMENTS	VI
LIST OF FIGURES.....	14
LIST OF TABLES	16
LIST OF ABBREVIATIONS.....	17
CHAPTER 1	19
1. INTRODUCTION & BRIEF BACKGROUND.....	19
1.1. INTRODUCTION	19
1.1.1. Cybersecurity	20
1.1.2. Artificial Intelligence.....	21
1.1.3. Accounting & Information Technology.....	21
1.1.4. Internal Auditing	24
1.1.5. Cybersecurity, Accounting and Finance	25
1.1.6. Blockchain (BC) & BC Technology	26
1.1.7. Game Theory	27
1.1.8. Social Engineering.....	28
1.1.9. Quantum Computing.....	30
1.1.10. Machine Learning (ML)	31
a. Levels of Machine Learning (ML).....	31
i. Supervised learning (task-driven).....	32
ii. Unsupervised learning (data-driven)	32
iii. Reinforcement learning (algorithms learn to react to an environment).....	32
1.2. CYBERSECURITY THREATS IN ACCOUNTING AND FINANCE	32
1.2.1. Deepfake-Enabled Executive Impersonation (CFO Fraud)	32
1.2.2. Large-scale Voice Phishing and Social Engineering	32
1.2.3. Phishing, Ransomware, and Insider Threats (General Trends).....	32
1.2.4. Wire Transfer Fraud via Cyber Manipulation	33
1.3. PRESENT RESEARCH REVIEW	33
1.3.1. Research Problem	34
1.3.2. Research Question	36
1.3.3. Conceptual Positioning of BQMG-AIS.....	36
1.3.4. Statement of Original Contribution	36
a. Development of the BQMG-AIS Integrated Cybersecurity Architecture.....	37
b. An Empirical Multi-Dataset Assessment of Fraud Detection Models in AIS Contexts	37
c. Integration of Explainability and Governance into AI-Driven Cybersecurity	37

d.	Strategic Modelling of Cyber Threats in Accounting Through Game Theory	38
e.	Reframing Emerging Technologies Through an AIS Centred Lens	38
1.4.	STRUCTURE OF THE THESIS	38
CHAPTER 2		41
2. LITERATURE REVIEW ON ADVANCED CYBERSECURITY FRAMEWORKS FOR ACCOUNTING BLOCKCHAIN, QUANTUM COMPUTING, GAME THEORY, AND MACHINE LEARNING		41
2.1	CONCEPTUAL FOUNDATIONS OF AIS CYBERSECURITY	41
2.1.1	<i>Cybersecurity in Accounting: Governance & Audit Perspective</i>	41
2.1.2	<i>Technology-Specific Research Streams in AIS Cybersecurity</i>	41
a.	Blockchain-Based Security in Accounting and Cybersecurity	42
b.	Machine Learning and AI-Based Cyber-Threat Detection	43
c.	Quantum Computing and Post-Quantum Cybersecurity	44
d.	Game-Theoretic Approaches to Cybersecurity and Decision-Making	45
2.1.3	<i>Cross-Stream Research Gap</i>	46
2.1.4	<i>Integrated Literature Gap Map</i>	46
a.	Introduction to the Literature Gap Map	46
1.	Technology-Siloed Development	48
2.	Insufficient AIS Alignment	48
3.	Limited Empirical Integration Across Technologies	48
4.	Weak Governance and Explainability Positioning	48
5.	Absence of a Unified AIS-Centred Cybersecurity Architecture	49
2.1.5	<i>How the Literature Gaps Shape the Direction of This Thesis</i>	49
2.1.6	<i>Integrated Literature Gap for Advanced Cybersecurity Frameworks in AIS</i>	49
a.	Cross-Cutting Literature Gaps Aligned with Thesis Aim	49
b.	Positioning of the Present Research	50
CHAPTER 3		52
3. BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY IN ACCOUNTING AND FINANCE SYSTEMS: ADOPTION, CHALLENGES, AND OPPORTUNITIES		52
3.1	OVERVIEW OF BLOCKCHAIN	52
3.1.1	<i>Introduction</i>	52
3.1.2	<i>Conceptual Boundary of Blockchain</i>	53
3.1.3	<i>What is Blockchain?</i>	53
3.1.4	<i>Blockchain Technology (BCT) & Its Suitability</i>	54
3.1.5	<i>Generations of Blockchain</i>	55
3.1.6	<i>Mining of Blockchain</i>	56
3.1.7	<i>Cybersecurity goals</i>	57
a.	Availability	57
b.	Integrity	57
c.	Authentication	57
d.	Confidentiality	57
e.	Non-repudiation	57
3.2	THEORETICAL BACKGROUND, RESEARCH AIM AND RESEARCH QUESTIONS	57
3.2.1	<i>Introduction</i>	57
3.2.2	<i>Main Research Question Alignment</i>	58
3.2.3	<i>Conceptual Model of Finance and Accounting System Exploiting Blockchain-based Cybersecurity Strategies</i>	58
a.	Job fit	59
b.	Complexity	59
c.	Perceived Consequences	59

d.	Affect towards use	59
e.	Relationship	60
f.	Culture	60
3.2.4	<i>Research Aim and Research Question</i>	60
a.	Research Aim	60
b.	Research Question	60
3.3	BLOCKCHAIN-BASED CYBERSECURITY	61
3.3.1	<i>Blockchain and Accounting</i>	63
3.3.2	<i>Cybercrimes</i>	63
3.4	CHANGES BROUGHT BY BLOCKCHAIN-BASED CYBERSECURITY IN ACCOUNTING	63
3.4.1	<i>Blockchain technology & AI in Finance</i>	63
a.	Distributed Ledger Technology	64
b.	Smart contract	64
3.4.2	<i>Blockchain as a cybersecurity framework</i>	65
3.4.3	<i>Blockchain Relevance to Accounting Information Systems (AIS)</i>	66
3.4.4	<i>Blockchain's use in financial accounting- an in-depth look</i>	66
a.	Blockchain and Big data in accounting	67
b.	Blockchain and auditing	68
3.4.5	<i>Limitations of Blockchain-based Cybersecurity in Accounting Information Systems</i> 68	
3.5	RESEARCH METHODOLOGY	69
3.5.1	<i>Introduction</i>	69
3.5.2	<i>Research Methodology</i>	70
3.5.3	<i>Research Methodology Adopted</i>	71
a.	What is a Systematic Literature Review?	71
b.	Systematic Literature Review adopted	72
c.	Systematic Literature Review Process	73
d.	Bibliometric mapping/visualisation	77
3.6	FINDINGS & DISCUSSIONS	77
3.6.1	<i>Findings</i>	77
a.	Job-fit	77
b.	Complexities	78
c.	Perceived Consequences	79
i.	<i>Selfish Mining</i>	79
ii.	<i>Scalability</i>	79
iii.	<i>Privacy Leakage</i>	80
d.	Affect towards Use	80
e.	Relationship	80
f.	Cybersecurity Culture	81
3.6.2	<i>Adoption of AI & Blockchain-based Cybersecurity Impacting the Role of Accountant & Auditor</i>	82
3.7	CONTRIBUTION TO KNOWLEDGE	83
3.7.1	<i>Adoption of the Model</i>	83
a.	Adoption Model with Multiple Dimensions	83
b.	Blockchain Adoption Behaviour Anchoring	84
c.	Game-Theoretic Blockchain Governance	84
d.	Industry 4.0 Contextualisation	84
3.7.2	<i>Job-Fit</i>	84
3.7.3	<i>Complexity</i>	84
3.7.4	<i>Perceived Consequences</i>	84
3.7.5	<i>Affect Toward Use</i>	85
3.7.6	<i>Relationship</i>	85
3.7.7	<i>Cybersecurity Culture</i>	85
3.7.8	<i>Policy Implications</i>	85

3.8	INTEGRATION OF BLOCKCHAIN INTO THE BQMG-AIS FRAMEWORK	86
3.9	CONCLUSION	86
3.10	FUTURE RESEARCH	88
CHAPTER 4		89
4. SECURING ACCOUNTING AND FINANCE INFORMATION SYSTEMS: AI-DRIVEN CYBERSECURITY INNOVATIONS AND CHALLENGES.....		89
4.1	AN INTRODUCTION TO SECURE ACCOUNTING AND FINANCE INFORMATION SYSTEMS (IS)	89
4.1.1	<i>Brief Background of the Study.....</i>	89
4.1.2	<i>Overview of Accounting and Finance Information Systems.....</i>	90
a.	Cloud-Based Solutions.....	90
b.	Role of AI in AFIS.....	90
c.	Cybersecurity Considerations	90
d.	Compliance and Risk Management.....	90
4.1.3	<i>AI Innovations in Cybersecurity.....</i>	91
4.1.4	<i>Challenges of AI-Driven Cybersecurity</i>	91
a.	Third-Party Risks	91
b.	Technical Hurdles	91
c.	Ethical Concerns	91
d.	Regulatory Complexities.....	92
e.	Collaboration and Knowledge Gaps.....	92
4.1.5	<i>Research Aim.....</i>	92
4.1.6	<i>Research Questions</i>	92
4.1.7	<i>Best Practices for Implementation.....</i>	92
a.	Compliance as a Foundation.....	92
b.	Robust Compliance Frameworks	93
c.	Regular Audits and Continuous Monitoring	93
d.	Employee Training and Security Awareness	94
e.	Investment in Cybersecurity Technologies	94
f.	Third-Party Vendor Management	95
4.1.8	<i>Case Studies.....</i>	95
a.	Enhancing Cybersecurity in Financial Institutions	95
b.	Challenges and Risk Management	95
c.	The Role of AI in Financial Applications.....	96
d.	Lessons Learned.....	96
4.2	LITERATURE REVIEW.....	96
4.2.1	<i>The Evolving Threat Landscape.....</i>	96
4.2.2	<i>AI-Driven Innovations in Cybersecurity</i>	97
a.	Anomaly Detection	97
b.	Incident Response Automation	97
c.	Behavioural Analytics	98
d.	Continuous Learning.....	98
4.2.3	<i>Learning-Based Anomaly Detection in AIS</i>	98
4.2.4	<i>Adversarial Machine Learning Defences.....</i>	98
a.	Adversarial Training.....	99
b.	Generative Adversarial Networks (GANs)	99
c.	Threat Simulation Platforms	99
4.2.5	<i>Explainable AI (XAI) for Financial Compliance</i>	99
4.2.6	<i>Conceptual Boundaries</i>	99
4.3	CONCEPTUAL FRAMEWORK	99
4.3.1	<i>AI Technologies</i>	100
4.3.2	<i>Organisational Environment</i>	100
4.3.3	<i>External Factors</i>	100

4.4	RESEARCH METHODOLOGY.....	100
4.4.1	Identification/search strategy.....	101
4.4.2	Screening.....	101
4.4.3	Eligibility.....	101
4.4.4	Inclusion	101
4.5	RESULTS AND FINDINGS.....	102
4.5.1	<i>RQ1: AI's Role in Enhancing AIS Cybersecurity</i>	102
4.5.2	<i>RQ2: Technical, Ethical, and Regulatory Challenges</i>	103
a.	Technical	103
b.	Ethical	103
c.	Regulatory	103
4.5.3	<i>RQ3: Best Practices for Risk-Balanced AI Adoption</i>	103
a.	Human-AI Collaboration.....	103
b.	Continuous Model Evaluation	103
c.	Governance Frameworks.....	103
d.	Vendor Management.....	103
4.6	DISCUSSION AND ANALYSIS	103
4.7	FUTURE TRENDS	104
4.7.1	<i>Cloud Computing in Finance</i>	104
4.7.2	<i>Blockchain Technology Applications</i>	104
4.7.3	<i>AI Innovations in Cybersecurity</i>	104
4.7.4	<i>Ongoing Assessment of Technology Relevance</i>	105
4.8	LIMITATIONS	105
4.8.1	<i>SLR Limitations</i>	105
a.	Publication Bias	105
b.	Domain Specificity	105
c.	Study Heterogeneity	105
4.8.2	<i>Organisational and Cost Barriers</i>	105
a.	Skill Shortage.....	105
b.	Explainability Tool Maturity	105
c.	Computational Expenditure	105
d.	Legacy Dependencies.....	105
4.8.3	<i>Stakeholder Roles and Operational Challenges</i>	106
a.	Financial Institutions.....	106
b.	Regulators.....	106
c.	Vendors	106
d.	National Security Entities	106
4.9	INTEGRATION WITH THE FINAL FRAMEWORK	106
4.10	BEST PRACTICES FOR IMPLEMENTATION	106
4.10.1	<i>Governance & Compliance</i>	106
4.10.2	<i>Vendor & Data Management</i>	106
4.10.3	<i>AI Usage Policies</i>	106
4.10.4	<i>Continuous Improvement</i>	107
4.11	CONCLUSION	107
CHAPTER 5.....		108
5. QUANTUM COMPUTING AND CYBERSECURITY IN ACCOUNTING AND FINANCE: THE PRESENT AND THE FUTURE CHALLENGES AND OPPORTUNITIES FOR SECURING ACCOUNTING AND FINANCE SYSTEMS.....		108
5.1. AN INTRODUCTION: QUANTUM COMPUTING AND ACCOUNTING AND FINANCE SYSTEM CYBERSECURITY CHALLENGES		108
5.1.1.	<i>Background of the Study</i>	108
5.1.2.	<i>Motivation and Relevance</i>	108

5.1.3.	Research Aim, Research Questions and Research Objectives	109
a.	Research Aim	109
b.	Research Question	110
c.	Research Objectives	110
❖	Objective 1	110
❖	Objective 2	111
❖	Objective 3	111
5.1.4.	Significance of the Study	111
5.1.5.	Scope and Delimitations	111
5.2.	LITERATURE REVIEW AND THEORETICAL FOUNDATIONS	112
5.2.1.	Fundamentals of Quantum Computing	112
a.	Quantum Computing	113
b.	Basic Building Blocks of Quantum Computing	113
i.	Qubit	113
ii.	Superposition	113
iii.	Entanglement	113
c.	Cryptography	114
5.2.2.	Prior Year Research	115
a.	Cybersecurity in Accounting Research [357]	115
b.	Innovative accounting methodology for ensuring the interaction of economic and cybersecurity enterprises [47]	116
c.	Cybersecurity and Prevention in the Quantum Era [359]	116
d.	Quantum computing for finance: Overview and prospects [140]	116
5.2.3.	Critical Cybersecurity Threats in Current Accounting & Finance Systems	118
i.	Data Breaches and Unauthorised Access	118
ii.	Weak or Outdated Cryptography	118
iii.	Fraud and Anomaly Detection Limitations	119
iv.	Third-Party and Supply Chain Risks	119
v.	Insider Threats and Human Factors	119
5.2.4.	Limitations of the Existing Literature Reviews	120
5.2.5.	Cybersecurity Frameworks and Quantum Threat Landscape	121
a.	Classical Cybersecurity Frameworks in Accounting and Finance	121
b.	Quantum Threat Landscape	121
i.	Grover's concept	121
ii.	Peter Shor's concept:	122
5.3.	CONCEPTUAL FRAMEWORK AND RESEARCH PROPOSITIONS	123
5.3.1.	Justification for the Theoretical Lens	123
5.3.2.	Integrated Conceptual Framework of Finance and Accounting System Leveraging Quantum Computing-based Cybersecurity Strategies	123
a.	User-Level Constructs: Technology Adoption Models	123
i.	Job Fit/Job Performance	124
ii.	Complexity	124
iii.	Perceived Consequences	125
iv.	Affect Towards Use	125
v.	Relationship/Social Factor	125
vi.	Culture	126
b.	Organisational Constructs: IS/Contingency Theory Foundations	126
c.	Quantum-Specific Constructs: Emergent from Empirical Synthesis	127
5.3.3.	Mapping the Integrated Conceptual Framework Factors to Research Objectives and Questions	130
5.3.4.	Research Propositions	130
a.	Proposition 1	130
b.	Proposition 2	130
c.	Proposition 3	130
d.	Proposition 4	131

5.4.	RESEARCH METHODOLOGY	131
5.4.1.	<i>Introduction</i>	131
a.	Systematic review	131
b.	Meta-Analysis	132
5.4.2.	<i>Research Methodology adopted</i>	132
5.4.3.	<i>PSALSAR Research Methodology</i>	133
5.5.	RESULTS & FINDINGS	137
5.5.1.	<i>Results and Findings – Testing of Propositions</i>	137
a.	Proposition 1	138
b.	Proposition 2	141
c.	Proposition 3	143
d.	Proposition 4.....	146
5.5.2.	<i>Discussion – Answers to Research Questions</i>	148
5.6.	CONTRIBUTIONS OF THE STUDY	149
5.6.1.	<i>Academic Contributions</i>	149
5.6.2.	<i>Methodological Contributions</i>	149
5.6.3.	<i>Practical Contributions to Financial Institutions</i>	149
5.6.4.	<i>Policy Contributions to Technology Regulations in Accounting</i>	149
5.7.	FUTURE RESEARCH.....	150
5.8.	CONCLUSION.....	151
CHAPTER 6		154
6.	STRATEGIC CYBERSECURITY IN ACCOUNTING: A GAME-THEORETIC FRAMEWORK FOR MITIGATING SOCIAL ENGINEERING	154
6.1.	INTRODUCTION	154
6.1.1.	<i>Brief Background</i>	154
6.1.2.	<i>Motivation & Relevance</i>	154
6.1.3.	<i>Related Research</i>	155
6.1.4.	<i>Research Aim, Objective and Questions</i>	155
a.	Research Aim and Objectives	155
b.	Research Questions	156
6.1.5.	<i>Contribution to Knowledge and Statement of Significance</i>	156
a.	Academic Contribution	156
b.	Statement of Significance.....	157
•	Practical Contribution	157
6.1.6.	<i>Scope & Delimitations</i>	158
a.	Scope	158
b.	Delimitations.....	158
6.2.	LITERATURE REVIEW AND THEORETICAL FOUNDATION.....	159
6.2.1.	<i>Overview of Cybersecurity in Accounting Based on Game Theory:</i>	159
a.	Game Theory in Cybersecurity.....	159
b.	Zero-Sum Game.....	159
c.	Stackelberg Game	159
d.	Nash Equilibrium.....	160
e.	Relevance to this Thesis	160
6.2.2.	<i>Prior Research</i>	160
a.	Game theory in network security for digital twins in the industry	160
b.	Cybersecurity Threat Assessment Integrating Qualitative Differential and Evolutionary Game	161
c.	Applications of Game Theory in Finance and Managerial Accounting	162
d.	Cyber Security Risk Modelling in Distributed Information Systems	162
6.3.	CONCEPTUAL FRAMEWORK	163
6.3.1.	<i>Introduction</i>	163
6.3.2.	<i>Core Components of the Conceptual Model</i>	163

a.	Actors and Roles	163
b.	Game Model.....	163
c.	GTM Framework.....	164
d.	Equilibrium Mechanism	164
e.	Social Engineering Layer.....	164
f.	Core Components of Conceptual Model.....	164
6.3.3.	Game Theory Model	166
6.3.4.	Game Theory Models and Cybersecurity	167
6.3.5.	Game Theory Model and Social Engineering Attack	167
6.3.6.	Game Theory and Accounting Cybersecurity	168
6.4.	RESEARCH METHODOLOGY	169
6.4.1.	Overview	169
6.4.2.	Research Design	169
6.4.3.	Application of Game-Theoretic Methodology	169
6.4.4.	Game Theory Model Structures	171
6.4.5.	Data Collection Method	172
6.4.6.	Payoff and calibration	173
6.5.	RESULTS, FINDINGS AND GENERAL DISCUSSIONS	174
6.5.1.	Discussion – Testing the Game Theory Matrix Model	174
6.5.2.	General Observations	186
6.5.3.	Discussion– Based on Research Questions	186
a.	RQ1	186
b.	RQ2	187
c.	RQ3	187
d.	RQ4	188
6.6.	CONTRIBUTIONS OF THE STUDY	188
6.6.1.	Interdisciplinary Integration of Game Theory in Accounting Cybersecurity	189
6.6.2.	Matrix-Based GTM Framework Development	189
6.6.3.	Strategic Defence Prioritisation based on Equilibrium Outcomes	189
6.6.4.	Adaptation and Extension for Future Threats	189
6.7.	CONCLUSIONS	189
6.7.1.	Game Theory and BQMG-AIS Integration	190
6.8.	FUTURE RESEARCH	190
6.8.1.	Real-Time Matrix Adaptation using Threat Intelligence Feeds	191
6.8.2.	Behavioural Game Theory for Social Engineering	191
6.8.3.	Post-Quantum Game-Theoretic Security	191
6.8.4.	Automated Cyber Defence with Machine Learning and GTM	191
6.8.5.	Sectoral Adaptation and Empirical Case Studies	191
6.8.6.	Quantitative ROI Models for Cyber Investment	191
CHAPTER 7		193
7.	ARTIFICIAL INTELLIGENCE DRIVEN CYBERSECURITY IN ACCOUNTING: A MULTI-STREAM FRAUD DETECTION FRAMEWORK USING ML	193
7.1.	INTRODUCTION	193
7.1.1	Background	193
a.	Overview of cybersecurity in accounting and finance	193
b.	Introduction to Machine Learning	195
c.	The role of machine learning in enhancing cybersecurity measures	195
d.	The need for advanced cybersecurity solutions tailored to accounting and finance systems	195
7.1.2	Theoretical Framing of Machine Learning in Accounting Cybersecurity	196
7.2.	EXPERIMENTAL DESIGN	197
7.2.1	Research Aim	197

7.2.2	<i>Research Objectives</i>	197
a.	To analyse the current state of cybersecurity in accounting and finance systems	197
b.	To explore the application of machine learning in accounting and finance cybersecurity..	197
c.	To develop machine learning models for detecting and preventing cyber threats in accounting and finance	198
d.	To integrate explainability techniques into fraud detection systems for improved auditability and compliance	198
e.	To establish methodological best practices for transparent, reproducible, and reliable ML workflows in accounting cybersecurity	198
7.2.3	<i>Research Questions</i>	198
7.2.4	<i>Hypotheses and Alignment with Research Questions</i>	199
i.	Hypotheses	199
ii.	Mapping Research Questions and Hypotheses	199
7.2.5	<i>Significance of the Study</i>	199
a.	Benefits of ML Integration in Financial Cybersecurity in Practice.....	199
b.	From a practical standpoint.....	200
c.	From an academic and theoretical standpoint	200
7.2.6	<i>Scope and Limitations</i>	200
a.	Focus on machine learning techniques applicable to cybersecurity in accounting and finance. 201	
b.	Exclusion of non-machine learning cybersecurity measures.....	202
7.3.	PRIOR RESEARCH	202
7.3.1.	<i>Cybersecurity in Accounting and Finance</i>	203
a.	Historical perspective	203
b.	Current trends and practices	203
i.	AI-Driven Fraud Detection	203
ii.	Biometric and Behavioural Authentication	203
iii.	AI in Intrusion Detection & Prevention (IDPS).....	204
iv.	Zero Trust and Adaptive Security	204
c.	Current practices and standards.....	204
7.3.2.	<i>Machine Learning</i>	204
a.	Principles and basics of machine learning	204
b.	Overview of machine learning concepts and algorithms	205
c.	Applications of machine learning in various domains	205
7.3.3.	<i>Synthesis of Prior Research in ML-Based Accounting Cybersecurity</i>	206
7.3.4.	<i>The intersection of Cybersecurity and Machine Learning</i>	206
a.	Potential impacts of machine learning on cybersecurity	206
b.	Existing research and gaps	207
7.4.	RESEARCH METHODOLOGY	209
7.4.1	<i>Research Design and Rationale</i>	210
7.4.2	<i>Justification of Methodological Scope</i>	210
7.4.3	<i>Integration into Accounting and Finance Systems</i>	212
7.4.4	<i>Proposed Solution</i>	212
7.5.	DATASET COLLECTION METHODS	213
7.5.1	<i>Data Sources:</i>	213
i.	Primary Data	213
ii.	Secondary Data	213
7.5.2	<i>Experimental Setup and Rationale</i>	214
i.	Experimental Setup	214
ii.	Critical Analysis of Data Collection Strategy.....	214
iii.	Link to Research Questions and Objectives.....	214
7.5.3	<i>Dataset Selection</i>	215
7.5.4	<i>Data Source and Ethics</i>	215
7.5.5	<i>Key Features and Data Quality</i>	215
7.6.	DATA PREPROCESSING	216

7.6.1	<i>Missing Data and Outlier Handling</i>	216
7.6.2	<i>Feature Engineering and Selection</i>	216
7.6.3	<i>Normalisation and Scaling</i>	217
7.6.4	<i>Class Imbalance Remedies</i>	217
7.6.5	<i>Model Development and Performance Evaluation Framework</i>	218
a.	Model Training, Validation and Algorithm	218
i.	Logistic Regression	218
ii.	Random Forest	219
iii.	XGBoost (Extreme Gradient Boosting)	219
b.	Model Validation and Cross-Validation Strategies	220
i.	K-Fold Stratified Cross-Validation	220
ii.	Overfitting Checks and Tuning	220
c.	Model Evaluation Metrics and Mathematical Formulas	220
i.	Confusion Matrix	221
ii.	Core Evaluation Metrics	221
iii.	ROC-AUC and PR-AUC	222
iv.	Metric Selection Justification	222
7.6.6	<i>Interpretability and SHAP Feature Importance</i>	222
a.	SHAP Fundamentals	222
b.	Application and Benefits	222
c.	Feature Importance in Empirical Results	223
7.6.7	<i>Explainability, Auditability, and Model Governance</i>	223
7.6.8	<i>Explainability and Model Validation</i>	224
7.7.	INTERACTIVE VALIDATION VIA STREAMLIT APPLICATION	224
7.7.1	<i>Dataset – Credit Card Fraud Data</i>	225
7.7.2	<i>Dataset – IEEE-CIS Fraud Data</i>	225
7.7.3	<i>Dataset – PaySim Mobile Money Data</i>	226
7.7.4	<i>Integrating the results from the three Datasets</i>	226
a.	Cross-Dataset Synthesis of Results	226
b.	Linking Findings to Research Questions	227
c.	Hypothesis Validation	227
d.	Theoretical Contributions	227
e.	Practical Implications for Accounting	228
f.	Comparison with Prior Literature	228
g.	Limitations and Risks	228
h.	Summary of Discussion	228
7.8.	EVALUATION OF FRAUD DETECTION DATASETS	228
7.8.1	<i>Credit Card Fraud Dataset [560]</i>	228
a.	Introduction	228
b.	Dashboard Outputs and Visual Results	229
c.	Model Evaluation and Interpretation	236
d.	Connection to Research Aim, Objectives, and Hypotheses	237
e.	Discussion in Context of Research Questions	238
f.	Accounting and Finance Implications	238
g.	Summary of Findings	239
7.8.2	<i>IEEE-CIS Fraud Data [579]</i>	239
a.	Introduction	239
b.	Dashboard Outputs and Visual Results	240
c.	Model Evaluation and Interpretation	246
d.	Linkage to Research Aim, Objectives, and Hypotheses	247
e.	Discussion in Context of Research Questions	247
f.	Accounting and Finance Implications	248
g.	Summary of Findings	248
7.8.3	<i>PaySim Fraud Data [582]</i>	249
a.	Introduction	249

b.	Dashboard Outputs and Visual Results	249
c.	Model Evaluation and Interpretation	256
d.	Linkage to Research Aim, Objectives, and Hypotheses	257
e.	Discussion in Context of Research Questions	258
f.	Accounting and Finance Implications	258
g.	Summary of Findings	259
7.9.	DISCUSSION BASED ON RESEARCH QUESTIONS	259
7.9.1	<i>RQ1 (Detection Effectiveness in Highly Imbalanced Datasets)</i>	259
7.9.2	<i>RQ2 (Performance Trade-offs Across Models)</i>	260
7.9.3	<i>RQ3 (Explainability and Compliance)</i>	260
7.9.4	<i>RQ4 (Methodological Best Practices for ML Workflows)</i>	260
7.9.5	<i>Experimental Validity and Organisational Applicability</i>	261
7.10.	CONCLUSIONS AND RECOMMENDATIONS	262
7.10.1	<i>Cross-Stream Integration within the BQMG-AIS Framework</i>	262
7.10.2	<i>Summary of Findings</i>	264
7.10.3	<i>Contributions to Knowledge</i>	264
a.	Methodological Contribution	264
b.	Theoretical Contribution	265
c.	Technical Contribution	265
d.	Applied Contribution	265
e.	Knowledge Integration	265
7.10.4	<i>Recommendations for Practice</i>	265
a.	Adopt a Hybrid Model Strategy	265
b.	Embed Dashboards into Accounting Systems	265
c.	Enhance Auditor Training	265
d.	Continuous Model Retraining	265
e.	Threshold Customisation	266
f.	Regulatory Compliance	266
g.	Pilot Deployment	266
7.10.5	<i>Future Research Directions</i>	266
CHAPTER 8		268
8.	TOWARDS A NEW, IMPROVED FRAMEWORK AND A SET OF STRATEGIES FOR CS IN ACCOUNTING AND FINANCE IN THE CURRENT WORLD	268
8.1.	INTRODUCTION	268
8.2.	CONCEPTUAL FOUNDATION	269
8.2.1	<i>Machine Learning for Anomaly Detection</i>	269
8.2.2	<i>Blockchain for Data Integrity and Audit Assurance</i>	269
8.2.3	<i>Quantum Computing for Encryption and Secure Communication</i>	270
8.2.4	<i>Game Theory for Strategic Defence and Threat Modelling</i>	270
8.2.5	<i>Applications in accounting include</i>	270
8.3.	THE DEVELOPMENT OF THE BQMG-AIS+ INTEGRATED CYBERSECURITY FRAMEWORK 271	
8.3.1	<i>Core Components</i>	271
8.3.2	<i>Architectural Boundaries, Data Governance, and System Constraints:</i>	272
a.	Conceptual versus Operational Components	273
b.	On-Chain versus Off-Chain Data Architecture	273
c.	Governance and Access Control Mechanisms	273
d.	System Constraints and Assumptions	274
8.3.3	<i>Framework Layers</i>	274
8.3.4	<i>Framework Flow</i>	275
8.4.	INTEGRATION WITH EMPIRICAL FINDINGS	275
8.4.1	<i>Blockchain Layer (Immutable Integrity Layer)</i>	275

8.4.2	<i>Quantum Computing Layer (Future-proof Cryptography Layer)</i>	276
8.4.3	<i>Machine Learning Layer (Adaptive Detection Layer)</i>	276
8.4.4	<i>Game Theory Layer (Strategic Defence Layer)</i>	276
8.4.5	<i>Formalisation of the Game-Theoretic Decision Layer</i>	276
8.5.	FRAMEWORK COMPONENTS AND DATA FLOW	278
8.5.1	<i>Data Ingestion and Preprocessing</i>	278
8.5.2	<i>Blockchain and Quantum Integration</i>	279
8.5.3	<i>Game-Theoretic Policy Engine</i>	279
8.5.4	<i>Systemic Benefits</i>	279
8.6.	FRAMEWORK VALIDATION AND THEORETICAL IMPLICATIONS	279
8.6.1	<i>Empirical Validation through Multi-Stream Machine Learning</i>	280
8.6.2	<i>Conceptual Validation across the Four Technology Streams</i>	280
8.6.3	<i>Theoretical Integration and Paradigmatic Alignment</i>	280
8.6.4	<i>Validation Scope and Limitations</i>	281
8.7.	PRACTICAL IMPLICATIONS FOR ACCOUNTING AND FINANCE	281
8.7.1	<i>Enhancing Fraud Detection and Audit Assurance</i>	281
8.7.2	<i>Strengthening Cryptographic Security through Quantum-Resistant Methods</i>	282
8.7.3	<i>Strategic Defence and Social Engineering Mitigation</i>	282
8.7.4	<i>The Need for a Unified Framework</i>	282
8.7.5	<i>Compliance, Governance, and Explainability</i>	283
8.7.6	<i>Real-Time Cybersecurity Dashboards and Monitoring</i>	284
8.8.	TECHNOLOGICAL BUILDING BLOCKS OF THE UNIFIED FRAMEWORK	284
8.8.1	<i>Classical Digital Accounting Infrastructure</i>	284
8.8.2	<i>AI Technologies for Cybersecurity</i>	284
8.8.3	<i>Quantum Computing Components</i>	285
8.8.4	<i>Cybersecurity Controls</i>	285
8.9.	INTEGRATED OPERATIONAL MODEL FOR SECURING ACCOUNTING AND FINANCE SYSTEMS	285
8.9.1	<i>Quantum-Secured Data Pipeline for Financial Information</i>	286
8.9.2	<i>AI-Driven Real-Time Data Management and Decision Systems</i>	286
8.9.3	<i>Integration of Post-Quantum Cryptography into AIS</i>	287
8.9.4	<i>Securing Accounting Records and Ledgers</i>	288
8.10.	STRATEGIC BENEFITS AND ORGANISATIONAL CONTRIBUTION OF THE UNIFIED FRAMEWORK	288
8.11.	IMPLEMENTATION STRATEGY FOR ORGANISATIONS (CFO-LEVEL ROADMAP)	289
8.11.1	<i>Vision and Motivation for Adoption</i>	289
8.11.2	<i>AI Adoption Areas in Accounting and Finance</i>	289
8.11.3	<i>Strategy for Quantum Adoption</i>	289
8.11.4	<i>Cybersecurity Strategies in the Quantum–AI Era</i>	290
8.11.5	<i>Human Capital and Skills Development</i>	290
8.11.6	<i>Governance, Regulatory, and Compliance Alignment</i>	290
8.12.	CONTRIBUTIONS TO THE THEORY OF CS FOR ACCOUNTING AND FINANCE	291
8.13.	USE CASES IN ACCOUNTING AND FINANCE	292
8.13.1	<i>Use Case 1: Real-Time Fraud Monitoring in Accounts Payable</i>	292
8.13.2	<i>Use Case 2: Financial Statement Integrity and Audit Trail Strengthening</i>	292
8.13.3	<i>Use Case 3: Internal Controls Against Social Engineering and Insider Threats</i>	293
8.13.4	<i>Strategic Risk Management Using Game Theory</i>	293
8.13.5	<i>Use Case 4: Post-Quantum Security Transition Planning</i>	293
8.14.	VALIDATION OF RESEARCH HYPOTHESES (H1–H4)	293
8.14.1	<i>Hypothesis: H1</i>	293
8.14.2	<i>Hypothesis: H2</i>	294
8.14.3	<i>Hypothesis: H3</i>	295

8.14.4	<i>Hypothesis: H4</i>	295
8.15.	SUMMARY OF IMPLICATIONS	296
CHAPTER 9		297
9.	CONTRIBUTIONS, SUMMARY AND CONCLUSIONS	297
9.1.	THEORETICAL, METHODOLOGICAL, AND PRACTICAL CONTRIBUTIONS	297
9.1.1	<i>Theoretical Contributions</i>	297
9.1.2	<i>Contribution to Accounting Information Systems Theory</i>	298
9.1.3	<i>Contribution to Machine Learning and Cybersecurity Theory</i>	298
9.1.4	<i>Integration of Game Theory in Financial Cyber Defence</i>	298
9.1.5	<i>Cross-Disciplinary Contribution</i>	299
9.1.6	<i>Streamlit-Based Prototype Integration</i>	299
9.1.7	<i>Regulatory and Compliance Integration</i>	299
9.1.8	<i>Methodological Contributions</i>	299
9.1.9	<i>Practical and Policy Contributions</i>	299
9.2.	INTEGRATION OF RESEARCH QUESTIONS (RQ1–RQ4) AND CROSS-CHAPTER SYNTHESIS	300
9.3.	IMPACT AND IMPLICATIONS OF THE INTEGRATED BQMG-AIS FRAMEWORK	300
9.3.1	<i>Overall Impact of the Integrated Framework</i>	300
9.3.2	<i>Implications for CFOs and Finance Leaders</i>	301
9.4.	LIMITATIONS AND FUTURE WORK	301
9.4.1	<i>Data Availability and Generalizability</i>	301
9.4.2	<i>Computational Complexity</i>	301
9.4.3	<i>Model Explainability and Auditor Adoption</i>	301
9.4.4	<i>Quantum Readiness and Interoperability</i>	301
9.4.5	<i>Ethical and Governance Considerations</i>	301
9.4.6	<i>Scope-Related Limitations (Doctoral Constraints)</i>	302
9.4.7	<i>Field-Level Research Challenges</i>	302
9.5.	CONCLUSION	302
10.	REFERENCES:	304

List of Figures

Figure 1.1 Accounting Challenges and Information Technology Response.....	19
Figure 1.2 Five Vs of Big Data	19
Figure 1.3 Basic Data Flow Diagram.....	21
Figure 1.4 Data Flow Diagram of Customer Payment Process.....	22
Figure 1.5 Flow Diagram of Payroll Processing	22
Figure 1.6 Flow Chart of Payroll Processing	23
Figure 1.7 Data Flow Diagram of Payroll Processing	23
Figure 1.8 Flow Chart of Payroll Processing	24
Figure 1.9 Various types of machine learning techniques	31
Figure 1.10 A general structure of an ML-based predictive model, considering both the training and testing phases	33
Figure 3.1 The key features of Blockchain Technology	53
Figure 3.2 Different security threats in edge networks	54
Figure 3.3 Schematic Diagrams explaining How Blockchain Works.....	55
Figure 3.4 The basic features of Blockchain Technology.....	62
Figure 3.5 Transaction in the supply chain using blockchain	65
Figure 3.6 PRISMA Flow Diagram	70
Figure 3.7 Process of Systematic Literature Review	72
Figure 3.8 Systematic Literature Review Approach	73
Figure 3.9 Summary of Methodology.....	74
Figure 3.10 PRISMA Flow Diagram	76
Figure 3.11 Co-occurrence analysis of the Author's keyword.....	77
Figure 5.1 Process of Encryption and Decryption	114
Figure 5.2 Classification of encryption and decryption algorithms	115
Figure 5.3 Integrated Conceptual Quantum Resilient Cybersecurity Model	129
Figure 5.4 Prisma Flow Diagram	136
Figure 6.1 Conceptual Model (Cybersecurity for accounting based on Game Theory and Social Engineering).....	165
Figure 6.2 A classification of game models.....	166
Figure 6.3 A conceptual model to describe how social engineering attacks work and take effect	168
Figure 6.4 General Structure of GTM.....	170
Figure 7.1 Essential elements of cybersecurity in financial management	195
Figure 7.2 Confusion Matrix-Logistic Regression.....	230
Figure 7.3 Confusion Matrix-Random Forest.....	230
Figure 7.4 Confusion Matrix-XGBoost	230
Figure 7.5 Precision-Recall Curve-Logistic Regression.....	231
Figure 7.6 ROC Curve-Logistic Regression	232
Figure 7.7 Precision-Recall Curve-Random Forest	232
Figure 7.8 ROC Curve-Random Forest	232
Figure 7.9 Precision-Recall Curve-XGBoost.....	233
Figure 7.10 ROC Curve-XGBoost.....	233

Figure 7.11 Precision-Recall Comparison	233
Figure 7.12 ROC Comparison	234
Figure 7.13 Calibration - Reliability	234
Figure 7.14 BAR Chart side-by-side Metric Test	235
Figure 7.15 SHAP values.....	236
Figure 7.16 Feature importances-model-based	236
Figure 7.17 Confusion Matrix-Logistic Regression.....	240
Figure 7.18 Confusion Matrix-Random Forest.....	241
Figure 7.19 Confusion Matrix-XGBoost	241
Figure 7.20 Precision-Recall Curve-Logistic Regression	242
Figure 7.21 ROC Curve-Logistic Regression	242
Figure 7.22 Precision-Recall Curve-Random Forest	242
Figure 7.23 ROC Curve-Random Forest	243
Figure 7.24 Precision-Recall Curve-XGBoost.....	243
Figure 7.25 ROC Curve-XGBoost.....	243
Figure 7.26 Precision-Recall Comparison	244
Figure 7.27 ROC Comparison	244
Figure 7.28 Calibration - Reliability	245
Figure 7.29 BAR Chart side-by-side Metric Test	245
Figure 7.30 Feature Importances-Model-Based.....	246
Figure 7.31 Paysim Confusion Matrix-Logistic Regression.....	250
Figure 7.32 Paysim Confusion Matrix-Random Forest	250
Figure 7.33 Paysim Confusion Matrix- XGBoost.....	251
Figure 7.34 Paysim Precision-Recall Curve	251
Figure 7.35 Paysim ROC Curve-Logistic Regression	252
Figure 7.36 Paysim Precision-Recall Curve-Random Forest.....	252
Figure 7.37 Paysim ROC Curve Random Forest.....	252
Figure 7.38 Paysim Precision Recall Curve-XGBoost	253
Figure 7.39 Paysim ROC Curve-XGBoost	253
Figure 7.40 Paysim Precision-Recall Comparison.....	254
Figure 7.41 ROC Comparison	254
Figure 7.42 BAR Chart side-by-side Metric Test	255
Figure 7.43 Calibration - Reliability	255
Figure 7.44 SHAP Calibration Reliability	256
Figure 7.45 SHAP Model-Based Importance	256
Figure 8.1 Integrated Framework: The BQMG-AIS Architecture for CS in Accounting and Finance.....	272
Figure 8.2 Integrated BQMG-AIS Conceptual Framework for Cybersecurity in AIS	278

List of Tables

Table 2.1 Literature Gap Map	47
Table 3.1 Comparison of different mining techniques.....	56
Table 3.2 Factors for Applying Blockchain-Based Cybersecurity Measures in an Organisation.	58
Table 5.1 Identified Research Gaps Mapped to Research Questions and Propositions	117
Table 5.2 PSALSAR framework for systematic literature reviews	133
Table 5.3 SLR research scope based on the application of the PICOC framework to the determined objectives	134
Table 5.4 SLR study selection of literature using inclusion and exclusion criteria	135
Table 6.1 Game Matrix 1	174
Table 6.2 Game Matrix 2	177
Table 6.3 Game Matrix 3	178
Table 6.4 Game Matrix 4	180
Table 6.5 Game Matrix 5	182
Table 7.1 Selected Datasets.....	216
Table 7.2 Confusion Matrix	221
Table 7.3 Model performance across the three datasets.....	227
Table 7.4 Model Comparison.....	233
Table 7.5 Model Comparison.....	237
Table 7.6 Model Comparison-Sorted by Test PR-AUC	244
Table 7.7 Model Comparison.....	246
Table 7.8 Model Comparison.....	253
Table 7.9 Model-Based comparison	257
Table 8.1: Distinct insights contribution	271
Table 8.2 Mapping Framework Components to Research Questions and Hypotheses.....	275
Table 8.3 Cross-Chapter Mapping of Research Questions & Contributions	283
Table 8.4 The Integrated Framework And Accounting Activities.....	294
Table 9.1 Cross-disciplinary contribution.....	299
Table 9.2 Cross-Chapter Synthesis	300

List of Abbreviations

AI	Artificial Intelligence
AIS	Accounting Information System
AICPA	American Institute of Certified Public Accountants
API	Application Programming Interface
AQF	Australian Qualifications Framework
BC	Blockchain
BQMG	Blockchain–Quantum–Machine Learning–Game Theory Framework
BQMG-AIS	Extended BQMG Framework integrated with Accounting Information Systems
CS	Cybersecurity
DL	Deep Learning
DLT	Distributed Ledger Technology
ERP	Enterprise Resource Planning
GAAP	Generally Accepted Accounting Principles
GDP	Gross Domestic Product
GRC	Governance, Risk, and Compliance
GT	Game Theory
GTM	Game-Theoretic Model
H1 – H4	Research Hypotheses 1 to 4
IIA	Institute of Internal Auditors
IFAC	International Federation of Accountants
IFRS	International Financial Reporting Standards
IoT	Internet of Things
IT	Information Technology
ML	Machine Learning
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
PICOC	Population–Intervention–Comparison–Outcome–Context (SLR framework element)
PoW	Proof of Work
PR-AUC	Precision–Recall Area Under Curve

PSALSAR	Protocol–Search–Appraisal–Literature–Synthesis–Analysis–Reporting (systematic review framework)
QKD	Quantum Key Distribution
QML	Quantum Machine Learning
RQ1 – RQ4	Research Questions 1 to 4
SHAP	SHapley Additive exPlanations
SLR	Systematic Literature Review
XAI	Explainable Artificial Intelligence
XGBoost	Extreme Gradient Boosting (machine-learning algorithm)

Chapter 1

1. Introduction & Brief Background

1.1. Introduction

Historically, accounting processes were predominantly manual, relying on paper-based ledgers and human recording before the introduction of computerised systems and digital automation [1]. Although Information and Communication Technologies (ICT) have been established, technologies such as Artificial Intelligence (AI), Cloud Computing, and Big Data are commonly and actively used in accounting processes [2].

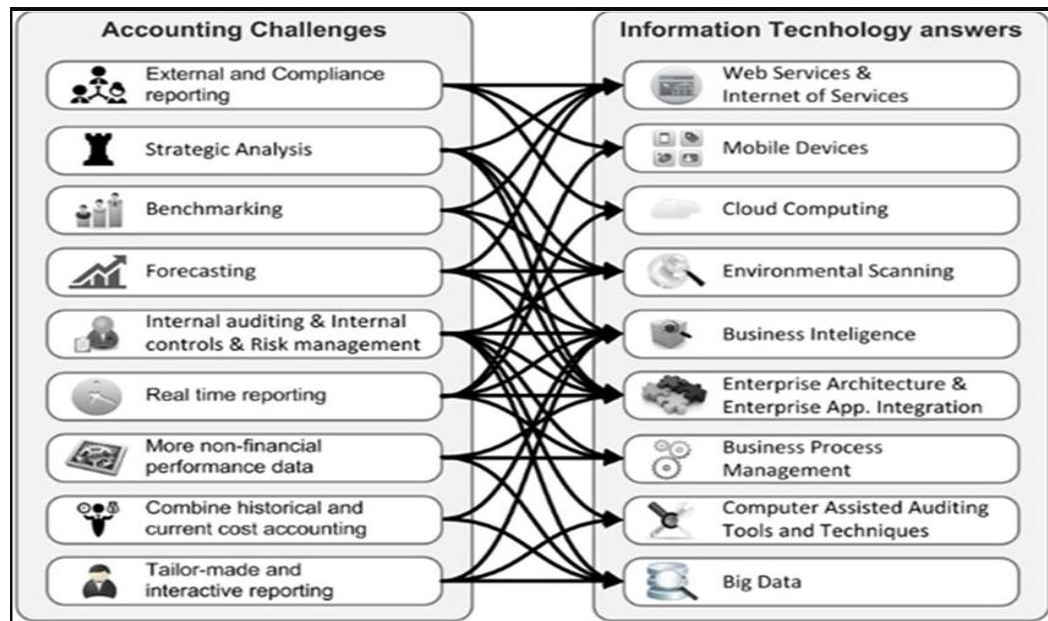


FIGURE 1.1 Accounting Challenges and Information Technology Response

SOURCE: [3]

Figure 1.1 illustrates the accounting challenges resolved using Information Technology (IT), specifically the use of Artificial Intelligence (AI) as a solution.

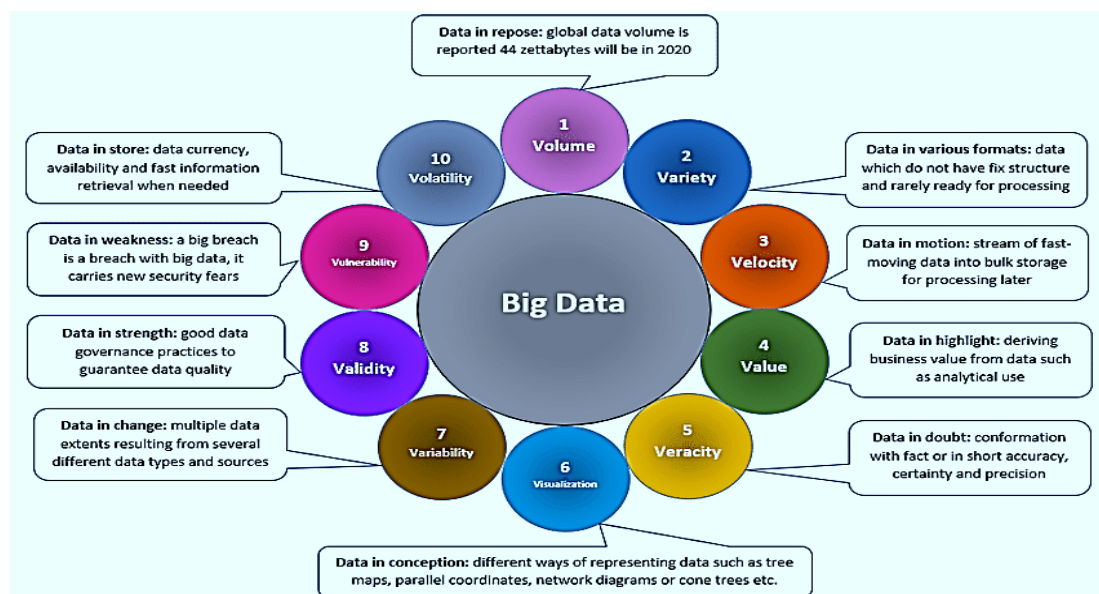


FIGURE 1.2 Five Vs of Big Data

SOURCE: [4]

Figure 1.2 briefly details the IT-based solutions to the organisation's accounting challenges.

[4] Big Data in accounting is often described through the “Five Vs,” each representing a distinct characteristic of modern digital information flows. Volume captures the sheer scale of transactional and financial records produced by contemporary accounting platforms [5]. Velocity reflects the rapid pace at which these data are generated, transmitted, and processed, particularly in real-time reporting and payment systems. Variety refers to the heterogeneity of data sources and formats, ranging from structured ledger entries to unstructured documents and communications [6]. Veracity concerns the reliability, accuracy, and integrity of these data streams, which are essential for audit assurance and regulatory compliance. Value relates to the ability to derive meaningful insights from large datasets to support fraud detection, risk assessment, and financial decision-making [5]. Together, these dimensions highlight the cybersecurity demands placed on Accounting Information Systems, where vast, fast-moving, and diverse financial data must be safeguarded and processed with high levels of trust and resilience.

1.1.1. Cybersecurity

Cybersecurity safeguards critical systems and sensitive data from digital attacks [4]. Cybersecurity strategies and measures, also known as Information Technology (IT) security, are designed to combat threats to networked systems and applications, including cyber espionage, whether originating from within or outside an organisation. It has been argued that cybersecurity should be focused on the organisational level [7]. Cybersecurity at this level covers three key areas. The first is technical (e.g., intrusion detection systems, intrusion prevention systems), the second is organisational (e.g., policies, procedures, processes), and the last is socio-psychological (e.g., adherence to guidelines, motivation for workplace behaviour). Rapid technological growth is intensifying competition and reshaping the global financial services landscape [7].

Cybersecurity encompasses the technologies, processes, and governance mechanisms designed to protect digital systems, networks, and data from unauthorised access, manipulation, or disruption [7]. It operates across technical, organisational, and human-centred dimensions, including intrusion detection systems, access control policies, incident response procedures, and employee behavioural compliance [4]. Within accounting and finance environments, cybersecurity has become foundational to safeguarding the confidentiality, integrity, and availability of financial information, particularly as organisations increasingly rely on interconnected Accounting Information Systems (AIS) [8, 9].

Cyberattacks targeting accounting systems can compromise audit trails, distort financial reporting, and undermine regulatory compliance, making AIS a high-value target for threat actors [10, 11]. The complexity of modern digital infrastructures—cloud platforms, mobile

access, and real-time data flows—further expands the attack surface and increases the risk of data breaches, ransomware, and insider threats [12-15]. Recent studies emphasise that cybersecurity failures in financial systems have cascading consequences, including operational disruption, reputational damage, and erosion of stakeholder trust [16, 17]. As AIS evolve toward automation and integration with emerging technologies, robust cybersecurity frameworks are essential to ensuring the resilience and trustworthiness of financial data ecosystems [18].

1.1.2. Artificial Intelligence

Artificial intelligence is a transformative innovation that offers numerous benefits to businesses [19]. With the advent of big data and a significant increase in computational power in recent years, organisations have embraced AI to create value and drive efficiency in their operations. [20] Notably, there has been a surge of interest in AI in recent years, with companies increasingly adopting AI applications to enhance their business operations and drive growth. [21] Businesses are increasingly turning to AI applications as a strategic tool to enhance corporate wealth. The potential benefits include increased sales revenue, improved business efficiency, and cost reduction.[22] According to recent research from the MIT Sloan Management Review, AI is not just a tool but a potential game-changer. Eighty per cent of companies perceive AI as an excellent strategic prospect, with nearly 85% considering it a tool to gain a competitive advantage. [23], which is why many organisations compete to overcome organisational obstacles and achieve sustainable revenue growth by investing heavily in AI technology. In contrast, some are still trying to understand the worth of AI investment [24].

1.1.3. Accounting & Information Technology

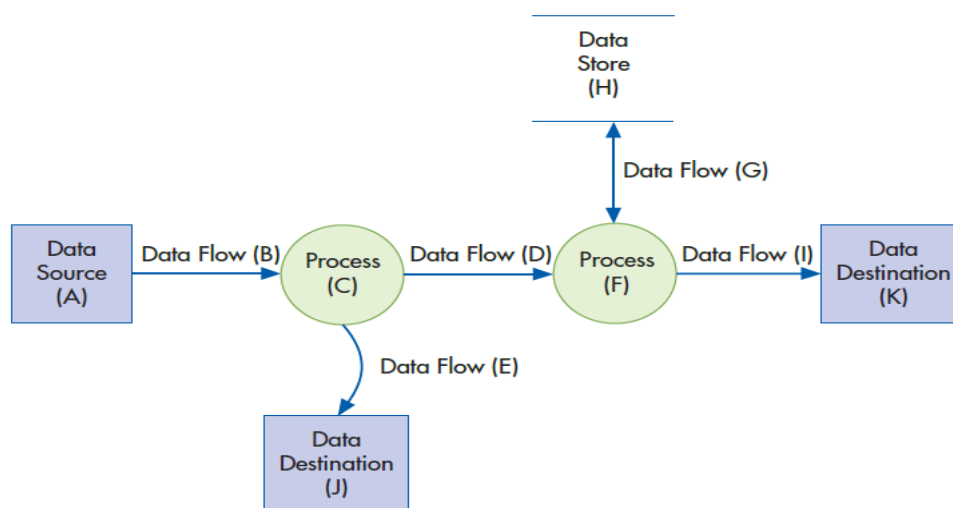


FIGURE 1.3 Basic Data Flow Diagram

SOURCE:[25]

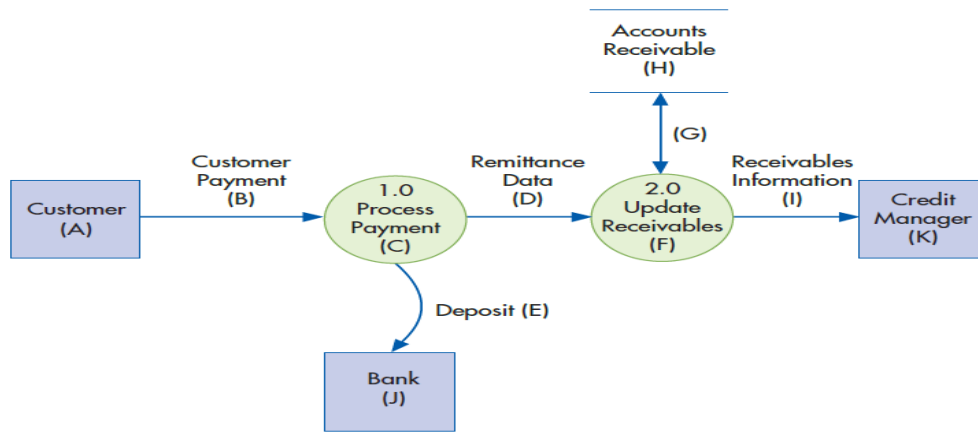


FIGURE 1.4 Data Flow Diagram of Customer Payment Process

SOURCE: [25]

Figure 1.3 and Figure 1.4 show the basic data flow diagram and the data flow diagram of the customer payment process, respectively. Another accounting transaction processing cycle is illustrated in the payroll flow chart shown in Figure 1.5 and continued in Figure 1.6. Figure 1.7 details the data flow diagram of payroll processing.

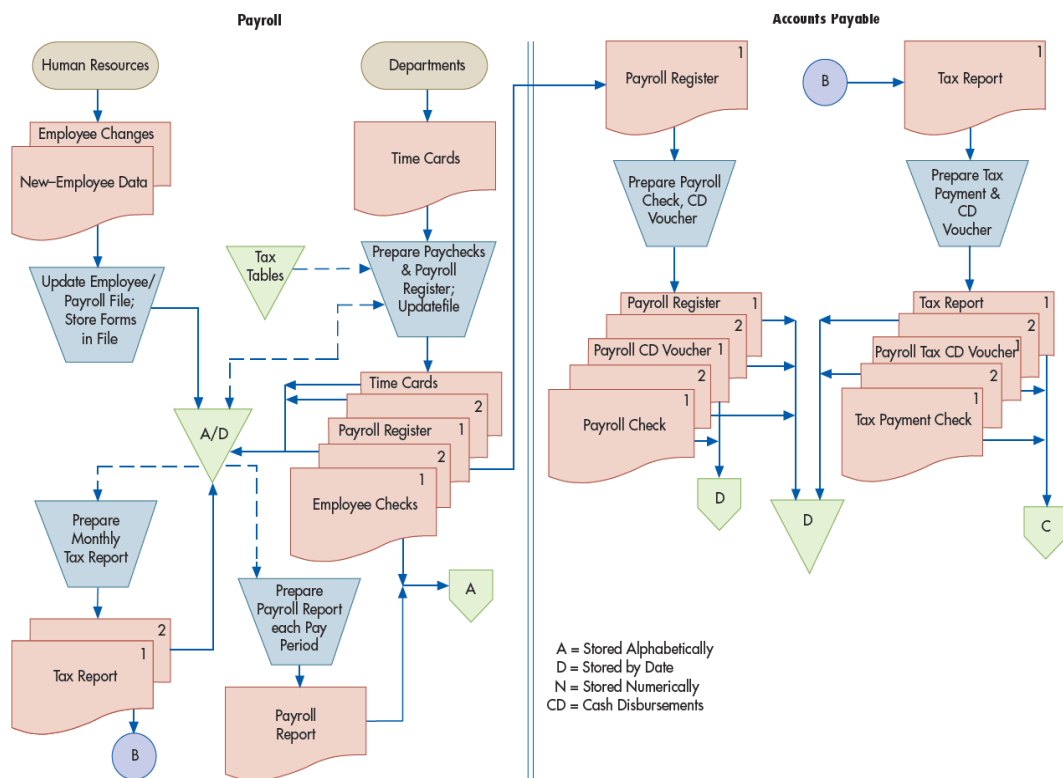


FIGURE 1.5 Flow Diagram of Payroll Processing

SOURCE: [25]

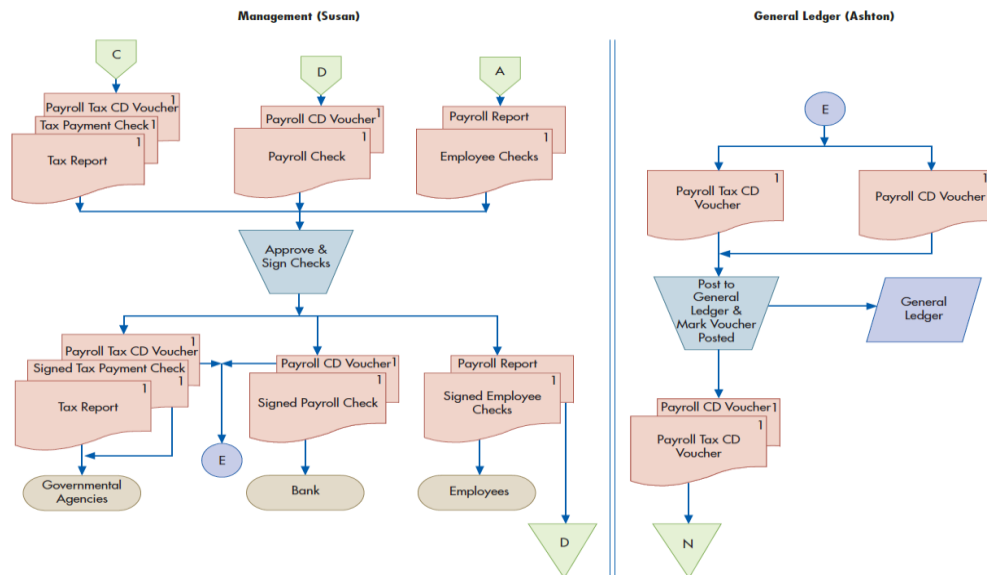


FIGURE 1.6 Flow Chart of Payroll Processing

SOURCE: [25]

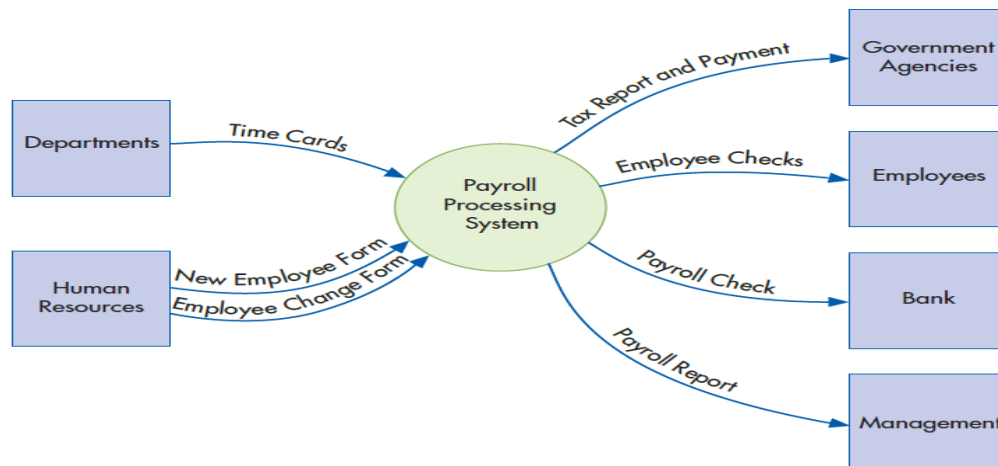


FIGURE 1.7 DATA FLOW DIAGRAM OF PAYROLL PROCESSING

SOURCE: [25]

An Accounting Information System (AIS) integrates people, processes, data, and IT infrastructure to collect, store, process, and distribute financial information [25]. Figures 1.3 to 1.7 illustrate foundational data-flow concepts within accounting processes, including the movement of information between data sources, processing activities, storage points, and destinations. These diagrams demonstrate how accounting transactions—such as customer payments or payroll activities—are structured into logical flows that ensure data completeness, accuracy, and traceability. While the operational details of these flows vary across organisations, the underlying principle remains consistent: AIS depend on well-designed information pathways to support transaction processing, financial reporting, auditing, and compliance [26],[27],[28],[29]. Modern AIS environments further enhance these processes

through databases, cloud platforms, automated controls, and real-time data exchanges, improving accuracy, reducing processing time, and strengthening internal controls [30].

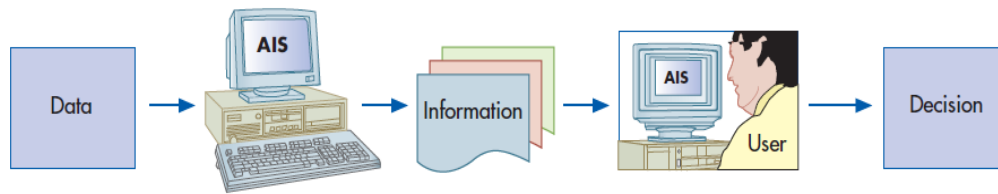


FIGURE 1.8 Flow Chart of Payroll Processing

SOURCE: [25]

Information technology also reshapes how accounting data moves through organisational processes. As depicted in Figure 1.8, AIS functions as an integrated system that transforms raw data into decision-useful information for internal and external stakeholders. This transformation relies on secure, reliable, and well-governed information pathways. As organisations increasingly adopt digital workflows, the integrity and confidentiality of accounting data become more vulnerable to cyber threats, system failures, and unauthorised access [8-11],[30],[31]. These vulnerabilities are amplified by the interconnected nature of modern enterprise systems, where a single compromised node can affect multiple financial processes.

The integration of IT into accounting, therefore, creates both opportunities and risks. Digital systems improve efficiency, accuracy, and analytical capability, but they also expand the attack surface for cyber threats, making AIS a critical target for fraud, manipulation, and data breaches [8], [9], [32], [33]. This intersection between accounting processes and technological infrastructure forms a central motivation for this research, which examines how advanced technologies—such as blockchain, machine learning, quantum-resistant cryptography, and game-theoretic modelling—can strengthen the security, resilience, and trustworthiness of accounting and finance information systems [1],[34] [29],[30], [31].

1.1.4. Internal Auditing

The study explains Audit [35] as a professional process that systematically examines and verifies a company's financial records and supporting data. The primary objective is to assess their accuracy, consistency, and compliance with Generally Accepted Accounting Principles (GAAP) or International Financial Reporting Standards (IFRS), ultimately providing an informed opinion on the organisation's financial integrity. The study points out that the internal audit function in the public sector differs from that in the private sector in terms of its status and the extent of outsourcing [36]. While audit committees play a pivotal role in supervising the activities of internal and external auditors, this oversight can sometimes result in conflicts of interest.

As mentioned in the article [35], the Institute of Internal Auditors (IIA) states that internal auditing is an independent and objective assurance and advisory function [35]. It aims to add

value by systematically evaluating and enhancing an organisation's risk management, internal control mechanisms, and governance processes. Internal auditing improves decision-making, regulatory compliance, and organisational effectiveness through a disciplined and strategic approach. [37] The rapid advancement of digital technologies is reshaping the internal auditing landscape, offering new opportunities for increased efficiency, security, and automation. One of the most transformative innovations is blockchain technology, a decentralised, distributed ledger system that enhances data security through its immutable, chain-based storage and asymmetric encryption [38, 39]. Additionally, Turing-complete smart contracts enable automated auditing, enabling real-time verification and continuous monitoring [40]. This automation reduces manual intervention, enhances accuracy, and streamlines audit workflows. [36] Beyond automation, cybersecurity and data privacy have become critical concerns for internal auditors. As the article points out, a study highlights the growing role of internal audits in mitigating cyber risks and ensuring compliance with data protection regulations. As organisations navigate the complexities of digital transformation, internal auditing must evolve to incorporate advanced technologies, reinforcing its role in safeguarding organisational integrity and resilience.

1.1.5. Cybersecurity, Accounting and Finance

[8] The study addresses the threat of cyberattacks, which pose a significant challenge to accounting information systems and necessitate robust cybersecurity measures to safeguard sensitive financial data. The dynamic and evolving nature of cyber threats demands continuous monitoring and adaptation of security protocols to mitigate potential risks effectively [9]. The quality and reliability of accounting information have become increasingly critical in the face of rising cyber threats, as the complexity of accounting processes and technological advancements have amplified these systems' vulnerability [9]. In accounting information systems, cyber threats can lead to unauthorised access, data loss, or the destruction of vital accounting information, underscoring the need for comprehensive protection mechanisms [10]. The study analysed the literature on the impacts of cyberattacks, which shows that they pose significant risks to organisations, especially in accounting information systems [8]. A growing body of literature indexed in Scopus highlights that the impacts of cyberattacks extend far beyond direct financial losses. Empirical and industry-based studies consistently demonstrate that cyber incidents can lead to significant operational disruptions, reputational damage, and erosion of stakeholder trust, particularly in accounting and financial systems where data integrity and reliability are critical [41-43]. These multidimensional consequences underscore the systemic nature of cybersecurity risks and reinforce the need for integrated and resilient security frameworks within accounting information systems. The prior year's research explains that the organisation, the custodian of vast amounts of sensitive financial data, is responsible for ensuring the confidentiality and integrity of the information it manages [11]. Integrating traditional accounting practices with modern cybersecurity controls is essential to

addressing the complex challenges of data security in an ever-evolving digital landscape [12-14, 44].

Furthermore, the theft of sensitive data can also lead to legal and regulatory violations, resulting in fines and lawsuits. The long-term impacts of a cyberattack include poor business performance and higher costs for recovery and upgrading security systems. The research highlighted that the shift of financial transactions to digital platforms is increasing rapidly, and safeguarding financial data has become crucial for maintaining trust, complying with regulatory requirements, and ensuring the financial stability of individuals who rely on accounting systems [11]. Data confidentiality and integrity are inherently interconnected: confidentiality prevents unauthorised access to sensitive information, while integrity ensures that the data remains accurate and reliable. One breach often compromises the other [45]. Achieving a balance between stringent confidentiality measures and authorised access to maintain data integrity requires robust access controls, encryption, and continuous monitoring mechanisms [15, 46]. The study has also identified that the rapidly evolving threat landscape, including phishing, ransomware, and social engineering, poses significant challenges to maintaining data security [11].

Additionally, malicious or inadvertent actions by employees within an organisation further exacerbate risks to data confidentiality and integrity. Innovative approaches are being developed to address these challenges and enhance the integration of economic and cybersecurity aspects within enterprises, focusing on identifying and mitigating financial losses caused by cyber threats [47]. Additionally, adopting hybrid threat models for innovative systems highlights the growing emphasis on threat analysis and cybersecurity across diverse technological domains [48]. These advancements reinforce the importance of proactive cybersecurity measures in maintaining the integrity and trustworthiness of accounting information systems, which are essential for organisational resilience in an increasingly digitised environment.

1.1.6. Blockchain (BC) & BC Technology

What is Blockchain: Satoshi Nakamoto is the inventor of the blockchain, the underlying technology he explained in his 2008 paper entitled “Bitcoin: A Peer-to-Peer Electronic Cash System[49]. The paper's abstract explains how blockchain enables direct online payments between two parties without a third party. Nakamoto’s contribution was to solve the double-spending problem, allowing a digital currency to be copied and spent more than once. Today, there are hundreds of other cryptocurrencies, such as Litecoin and Dogecoin, but Bitcoin still dominates the market and is the most popular cryptocurrency. These can be exchanged for real money, goods, or services. The user can electronically send bitcoins to another person using wallet software on a computer, mobile device, or a web application [49]. Recent studies explain that Blockchain is a revolutionary technology, a decentralised, distributed, and immutable ledger designed to record transactions and track assets seamlessly within a business

network [50]. Virtually anything of value can be tracked and traded on a blockchain platform, making it a versatile tool for modern commerce. By securely capturing transactional data in a nearly tamper-proof manner, blockchain minimises risks and cuts costs, offering a robust foundation for trust and efficiency in digital transactions.

It has been established that Blockchain technology is a decentralised and distributed ledger system that enables multiple participants to securely and transparently record and verify transactions[51]. Initially introduced in 2008 as the foundational technology for the cryptocurrency Bitcoin, its potential uses go well beyond digital currencies [52].

Blockchain comprises three components. [50]:

- * **Blocks:** The building blocks which store the information. These blocks are linked up sequentially in a chain. Each block contains data, a hash, and the hash of the previous block. Data refers to the information stored in a block. A hash is a unique code of the block, like a digital fingerprint. The previous block's hash serves as a link to the previous block, which contributes to the chain's security.

- * **Miners:** The individuals who add new blocks to the chain through mining. A process where they need to solve a complex problem to find the nonce that generates a valid hash. Once they successfully do this, the block is validated and added to the chain, and the miner receives a reward for their work.

- * **Nodes:** Any electronic device storing and maintaining a copy of the blockchain. They are responsible for verifying the chain's validity and ensuring the network operates efficiently. Every node stores its copy of the chain and updates it independently of others. These components work together to maintain the blockchain's security, transparency, and integrity. Existing evidence highlights the widely accepted game-changing technology, the Blockchain, revolutionising diverse fields like finance [1], supply chain management, insurance, voting, healthcare, and government services [53-55]. Blockchain technology enhances cybersecurity through its decentralised, immutable, and transparent nature. Distributing data across multiple nodes reduces the risk of single points of failure and minimises the likelihood of data manipulation. Applications include identity management, data privacy, and securing IoT devices. However, scalability, regulatory issues, and energy consumption persist. Solutions like advanced consensus algorithms and integration with AI can address these challenges, making blockchain a promising tool for improving cybersecurity measures across various sectors. Organisations across multiple industries are eagerly exploring their potential to create innovative solutions that are immutable, traceable, transparent, and trustworthy [56]. By leveraging blockchain, businesses can redefine processes and build systems that inspire confidence and efficiency on an unprecedented scale.

1.1.7. Game Theory

Research in this domain shows that Game theory, a fascinating branch of applied mathematics, is the exploration of how rational decision-makers, or "players," strategise to achieve the best

possible outcomes in competitive or cooperative scenarios [57]. Each player's decisions are fluid, influenced by the moves of others, creating a ripple effect that shapes the game's outcome. With games involving any number of players, their interests may align, conflict, or combine in complex ways [57]. Game theory dives into the art of optimal decision-making in these interconnected settings, unravelling how strategic interactions drive the dynamics of winning and collaboration.

Studies in accounting information systems reveal the four components of the game theory, i.e. players, strategies, actions, and the last one, payoffs [57]. Initially developed in economics, game theory has been utilised to analyse the behaviours of cyber attackers and defenders [58]. The game theory addresses cybersecurity challenges by modelling the strategic interactions between attackers and defenders. It provides frameworks for understanding decision-making processes in dynamic environments where parties adapt strategies based on anticipated actions. Techniques such as the Nash equilibrium help identify optimal responses to cyber threats, thereby enhancing defence mechanisms. By integrating artificial intelligence, game theory can predict potential attacks and improve resource allocation, fortifying digital infrastructures against evolving cyber risks. This synergy is essential for developing robust cybersecurity strategies in an increasingly interconnected world.

Furthermore, studies in accounting information systems reveal the widespread use of game theory in the security domain, giving rise to the concept of security games [59]. Beyond cybersecurity, game theory finds applications across diverse fields, including politics, science, economics, auctions, and finance. This paper explores how game theory is explicitly applied to address cybersecurity challenges.

In accounting and finance, game theory provides a structured analytical lens for modelling adversarial behaviour targeting AIS. Attackers may seek to manipulate financial records, compromise audit trails, or exploit system vulnerabilities, while defenders must prioritise controls such as authentication, monitoring, and encryption. Game-theoretic approaches enable organisations to evaluate trade-offs, anticipate attacker incentives, and design more resilient accounting security architectures [60]. Recent research demonstrates the value of game-theoretic modelling in enhancing data privacy, fraud prevention, and cyber-risk governance within financial systems [61].

1.1.8. Social Engineering

Prior research literature explains what social engineering is and the related attacks, indicating that organisations and governments have a substantial stake in protecting sensitive information, as it directly impacts the trust of clients and citizens [62]. However, technology alone cannot fully guard against information theft; employees often represent the weakest link in any security system. Through manipulation, staff members can be coerced into revealing confidential information, granting unauthorised individuals access to secure systems. This craft of manipulating people into disclosing sensitive information is called social engineering,

while the act itself is referred to as a social engineering attack. The literature identifies that social engineering attacks are among the most potent threats, exploiting human interactions and targeting any system or network [63]. Unlike technical vulnerabilities, these attacks cannot be stopped with software or hardware solutions alone; prevention relies on properly training individuals to recognise and avoid such threats. Cybercriminals often resort to social engineering when technical vulnerabilities are absent, using manipulation as their key to bypass otherwise secure systems [64]. Social engineers manipulate their victims to extract sensitive information used for specific purposes or sold on the black market and dark web [63]. With the rise of Big Data, attackers now leverage massive datasets to capitalise on valuable information for business-related gains [65]. They often bundle large volumes of stolen data to sell in bulk, treating it as a commodity in today's markets [66]. While social engineering attacks may vary in execution, they typically follow a four-phase pattern: (1) gathering information about the target, (2) building a relationship with the target, (3) exploiting the information to carry out the attack, and (4) making a clean exit, leaving no traces behind [62]. Social-based attacks exploit relationships with victims by manipulating their psychology and emotions, making them some of the most dangerous and effective methods due to their reliance on human interaction [67]. Common examples include baiting and spear phishing.[63] In contrast, technical-based attacks are carried out online through social networks and websites to harvest sensitive information, such as passwords, credit card details, and answers to security questions [68]. Physical-based attacks involve direct, hands-on actions, such as rummaging through dumpsters to uncover valuable documents [69]. Often, social engineering attacks blend these approaches, creating a powerful combination of psychological, technical, and physical tactics to achieve their goals.

Social engineering involves manipulating individuals into divulging confidential information or granting unauthorised access to systems. Unlike purely technical attacks, social engineering exploits human psychology, trust, and organisational routines, making it one of the most effective and pervasive forms of cyberattack [62, 63]. Common techniques include phishing, baiting, impersonation, and pretexting, often executed through email, messaging platforms, or direct interaction [64-68].

Accounting and finance functions are particularly vulnerable to social engineering because they involve high-value transactions, privileged system access, and sensitive financial data. Attackers frequently target finance personnel with fraudulent payment requests, invoice manipulation schemes, or credential harvesting attempts designed to compromise AIS [62]. Successful social engineering attacks can lead to unauthorised fund transfers, falsified financial records, and significant regulatory and reputational consequences [70]. Strengthening human-centred controls—such as awareness training, behavioural monitoring, and multi-factor authentication—is therefore essential for safeguarding AIS against social engineering threats [71].

1.1.9. Quantum Computing

Quantum theory provides a mathematical framework for describing the behaviour of microscopic particles, such as electrons and photons, which differs significantly from classical physics [72]. While classical theories are sufficient for understanding macroscopic electric properties, quantum theory is essential for understanding small-scale information processing. Developed in the early 20th century, it remains the most comprehensive description of microscopic physics. A computer that operates based on quantum theory is known as a quantum computer. Further in their research, they clarified that "quantum machine learning" gained traction in 2013. In their 2013 manuscript, Lloyd, Mohseni, and Rebentrost introduced the expression, marking its early usage [73]. A year later, in 2014, Peter Wittek expanded on the concept with an influential monograph titled **Quantum Machine Learning, What Quantum Computing Means to Data Mining**, helping to solidify the term's place in the emerging field [74]. While the digital computer has dramatically changed how we process information, quantum computers fundamentally change the nature of computing itself [75]. Quantum computers employ a fundamentally different approach to computing, utilising the physics of quantum mechanics to solve problems that are astronomically complex for traditional computers. They are not likely to replace conventional computers. However, they promise to solve intractable statistical issues that far exceed today's technology's capabilities and to open new frontiers.

The literature explained that traditional computers, conventional computational processors, process information using binary bits (0s and 1s) and rely on logic gates built from switching transistors [76]. In contrast, quantum computers operate on quantum bits, or qubits, not limited to just two states. Qubits can exist as either 0 or 1, or both simultaneously, through a phenomenon known as superposition. This unique capability allows quantum computers to process and store multiple states simultaneously, potentially millions of times more potent than today's most advanced supercomputers. Additionally, quantum computers promise unparalleled advantages, including ultra-secure data transmission, lightning-fast processing speeds, and the capacity to store vast amounts of information far beyond the limits of classical computing systems.

Quantum computing leverages principles of quantum mechanics—such as superposition and entanglement—to perform computations that are infeasible for classical computers. Quantum algorithms, including Shor's and Grover's, have the potential to break widely used cryptographic schemes by rapidly factoring large integers or accelerating search processes [72-75]. As research advances, quantum computing is expected to reshape the security landscape of digital systems.

For accounting and finance, the implications are profound. AIS rely heavily on cryptographic mechanisms to secure financial records, protect audit trails, authenticate users, and safeguard data transmitted across networks. Quantum-capable adversaries could compromise these

protections, exposing sensitive financial information and undermining regulatory compliance [77]. Preparing AIS for a post-quantum environment requires adopting quantum-resistant cryptographic algorithms, enhancing key-management practices, and strengthening governance frameworks [78]. Recent studies emphasise that quantum-safe security is essential for ensuring the long-term confidentiality and integrity of financial data [79].

1.1.10. Machine Learning (ML)

The last technological advancement humanity ever needs to make is machine intelligence [80]. In 1959, Arthur Samuel coined the term "Machine Learning (ML)". According to him, "Machine learning is the discipline of study which involves computers 'ability but without being explicitly programmed to learn [76]. This captures the core idea." [81] ML is a branch of computer science and AI in which data and algorithms are trained to imitate human actions and gradually become more accurate. We are in a digital era where cybersecurity breaches are happening daily and growing more complex, and ML and AI are used to address cybersecurity concerns. We usually see three prominent figures in cyberattacks: cybercriminals, Hackers, and cyberterrorists. Cybercriminals targeting organisations are stealing their money or confidential data. It results in them being left with long-term financial and reputational loss. AI systems require advanced and innovative tools and methods for cybersecurity to enhance their resilience and reliability. Similarly, AI must be applied to improve cybersecurity, increasing awareness and implementing high-tech measures, improvements, and ultimately enhancing overall efficiency and effectiveness. AI systems based on ML algorithms are used to identify, detect, and mitigate these threats; plans must be analysed regularly, and human intervention monitoring is required on a daily basis.

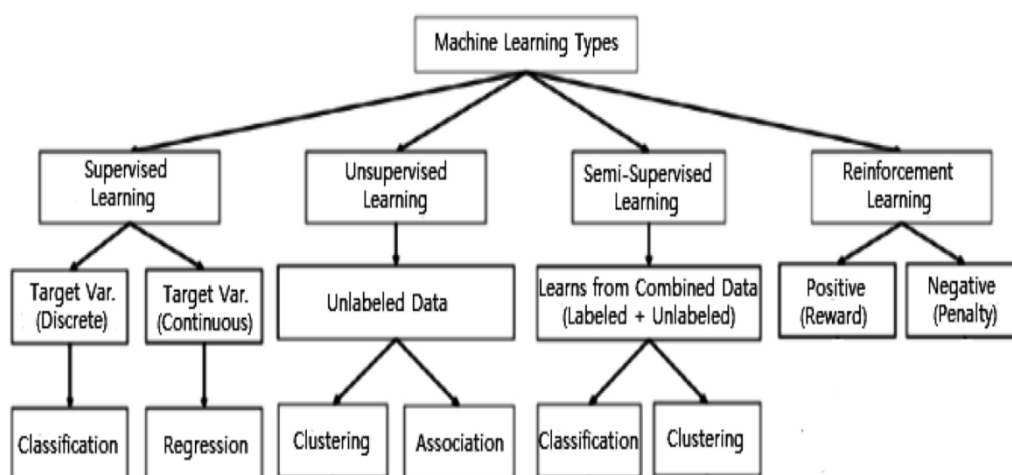


FIGURE 1.9 Various types of machine learning techniques

SOURCE: [82]

Figure 1.9 and Figure 1.10 illustrate the Machine learning algorithms used for the training and testing phases of the machine learning model.

a. Levels of Machine Learning (ML)

ML algorithms, part of AI, can be classified into supervised, unsupervised, semi-supervised, and reinforcement learning. [83] Previous research indicates the three classes of ML as follows:

i.Supervised learning (task-driven)

The methods are given inputs, labelled with corresponding outputs, as training examples, and are applied to solve classification and regression problems.

ii.Unsupervised learning (data-driven)

The methods are given unlabeled inputs and applied to solving clustering and association problems.

iii.Reinforcement learning (algorithms learn to react to an environment)

Data is a sequence of observations, actions, and rewards, and is used in the gaming industry to build games and train robots to perform tasks that mimic human actions.

1.2. Cybersecurity Threats in Accounting and Finance

Organisations' accounting and finance departments are becoming increasingly susceptible to complex cyberattacks that exploit both human and technological flaws. To commit fraud, alter records, or interfere with vital operations, these attacks usually target sensitive financial data, payment systems, and reporting procedures:

Considering examples recently confronted due to the cybersecurity attacks:

1.2.1. Deepfake-Enabled Executive Impersonation (CFO Fraud)

- **Arup Case (Feb 2024):** AI-generated deepfake executives deceived an Arup finance employee during a video call. This manipulation resulted in £20 million (approximately AUD 41 million) being transferred across 15 fraudulent transactions [84].
- **UAE Bank Case (2021):** A UAE director was impersonated by fraudsters using AI voice cloning and fake emails to request urgent fund transfers. The branch manager complied, resulting in US\$35 million (≈ approximately AUD \$ 53 million) being fraudulently transferred [85].

AI deepfakes to exploit finance staff's trust in executive authority are prime examples of social engineering.

1.2.2. Large-scale Voice Phishing and Social Engineering

- **2025 Qantas Attack:** Hackers bypassed multi-factor authentication and accessed data of up to 6 million customers by exploiting human and third-party vulnerabilities at a Manila Qantas call centre, using vishing (voice phishing) and possibly AI-assisted impersonation [86]. These incidents demonstrate how voice-based deception targets individuals, often the weakest link.

1.2.3. Phishing, Ransomware, and Insider Threats (General Trends)

Common cyber threats to finance include:

- **Phishing and Spear Phishing**

Targeted emails impersonating banks or executives, aiming to extract credentials or initiate unauthorised transactions [87].

- **Ransomware Attacks**

Malicious encryption of financial systems or data is particularly acute for accounting firms handling sensitive data.

- **Insider Threats**

Employees or contractors may cause breaches or fraud due to negligence ($\approx 55\%$) or malicious intent ($\approx 25\%$). Another $\sim 20\%$ is due to credentials theft [88].

- **Data Breaches and Reporting Integrity**

Misconfigured cloud storage or outdated systems can lead to data breaches, affecting the accuracy and trust in financial reporting [89].

1.2.4. Wire Transfer Fraud via Cyber Manipulation

Swift and Wire Transfers: Fraudsters employ cyber manipulation to commit wire transfer fraud, capitalising on the irreversibility of high-value transfers. Phishing or compromised credentials are used to initiate fraudulent fund transfers, especially offshore, making detection and reversal difficult [90].

1.3. Present Research Review

Scholarly work on cybersecurity emphasises Blockchain as an emerging technology for cybersecurity that is more reliable and robust. It was also further identified that BC has always provided privacy and protection [34]. Further, it also clarified and discussed, in detail, analysing an industry for the proper use of blockchain technology. Our research project aims to address and resolve the questions identified. The study noted that the focus of cybersecurity has shifted to AI paradigms, particularly in network inconsistency detection, including neural networks, genetic algorithms, fuzzy logic, support vector machines, finite automata, and other diverse data mining-based approaches [91]. The study identified the problem of evaluating the AI paradigms to be implemented in the Cybersecurity System [91].

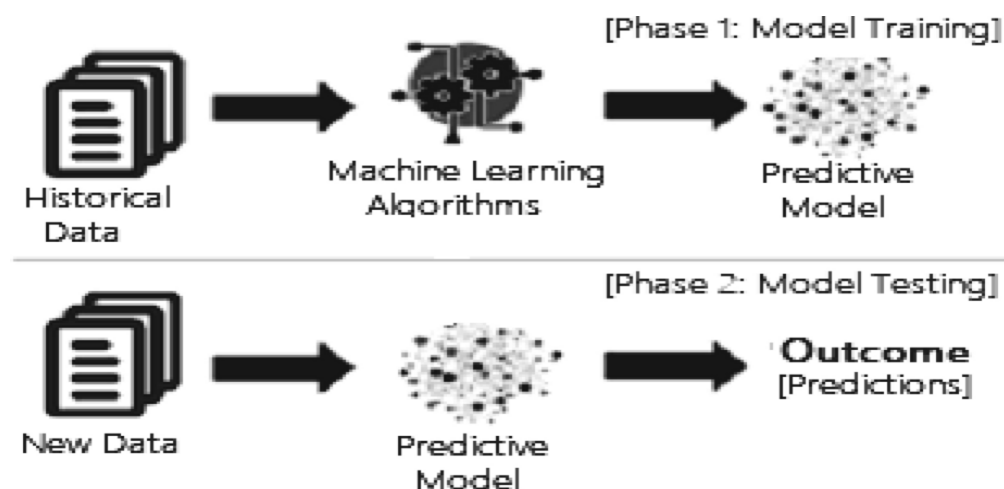


FIGURE 1.10 A general structure of an ML-based predictive model, considering both the training and testing phases

SOURCE: [82]

1.3.1. Research Problem

The rapid digitalisation of accounting and finance systems has increased productivity, but it has also made them much more vulnerable to sophisticated, constantly evolving cyber threats. Current accounting cybersecurity strategies often rely on discrete technological solutions, such as employing blockchain exclusively for audit trails, machine learning exclusively for fraud detection, or quantum cryptography exclusively for potential encryption threats. The entire accounting information cycle is not adequately protected by this technology-by-technology approach, leading to fragmented protection.

The main challenge in this research is the gap between rapidly evolving cybersecurity tools and the rules required for Accounting Information Systems (AIS). As organisations adopt more technologies, such as blockchain, machine learning, quantum computing, and game theory, they are often used in isolation, without a clear connection to accounting, auditing, or the law. This causes control issues, makes auditing more difficult, and reduces trust in financial data. So, current cybersecurity methods are technically advanced but not well-organised. This thesis offers the BQMG-AIS framework, which combines new technologies into a single, organisation-focused cybersecurity system designed for accounting and finance.

Three significant gaps in current academic and business practices are highlighted by recent evidence:

1. Deepfake-enabled impersonation, AI-driven phishing, synthetic identities, automated transaction manipulation, and quick multi-channel intrusions are all contributing to the increasing sophistication of fraud and cyberattacks.
2. As of right now, there is not an integrated cybersecurity architecture for Accounting Information Systems (AIS) that combines Blockchain, Quantum Computing, Machine Learning, and Game Theory.
3. The lack of transparency, auditability, and cross-dataset validation in machine-learning models used in accounting restricts their application in regulated settings where explainability is required.

The lack of an empirically verified, conceptually based, and AIS-aligned cybersecurity framework that combines Blockchain, Quantum Computing, Machine Learning, and Game Theory to improve fraud detection, auditability, governance, and cyber resilience across digital accounting ecosystems is thus the main research issue this thesis attempts to address.

The rapid digital transformation of accounting and finance systems has significantly increased organisational dependence on complex digital infrastructures, cloud platforms, and automated financial processing environments. While these developments enhance efficiency and analytical capabilities, they simultaneously expose Accounting Information Systems(AIS) to increasingly sophisticated cyber threats, including ransomware, phishing, data manipulation, and insider attacks [92, 93]. As financial transactions and reporting processes become

increasingly digitised, protecting the confidentiality, integrity, and availability of financial information has become a central concern for organisations and regulators [41].

Despite the growing body of research on cybersecurity technologies, existing studies frequently examine emerging technologies such as blockchain, artificial intelligence, quantum computing, and behavioural defence mechanisms independently rather than as part of a unified security architecture [94, 95]. This technological fragmentation limits the ability of organisations to implement comprehensive cybersecurity strategies capable of addressing the multi-layered threat environment facing modern accounting information systems. In particular, the absence of integrated cybersecurity architectures creates vulnerabilities in financial ecosystems where multiple digital platforms, data sources, and automated decision systems interact simultaneously[96].

At the same time, regulatory bodies and professional accounting organisations increasingly emphasise the importance of governance, transparency, and explainability in digital financial systems. Cybersecurity controls must not only protect financial data but must also support auditability, regulatory compliance, and organisational accountability [97, 98]. However, many advanced technological solutions remain technically sophisticated but insufficiently aligned with accounting governance frameworks, creating challenges for auditors and regulators seeking to evaluate the reliability and transparency of automated financial systems [99].

Accordingly, a key research gap exists in the absence of an integrated and AIS-aligned cybersecurity framework capable of combining technological innovation with accounting governance principles. This thesis addresses this gap by proposing the BQMG-AIS framework, which integrates four complementary components: Blockchain for immutable financial records, Quantum-resilient cryptographic approaches for future security threats, Machine Learning for adaptive fraud detection, and Game Theory for strategic modelling of attacker-defender behaviour. Importantly, the framework operates at a conceptual and governance-oriented level, rather than representing a fully deployable enterprise cybersecurity system. Empirical analysis using financial fraud datasets is used to validate the machine learning component and demonstrate the feasibility of integrating data-driven cybersecurity techniques within accounting environments, thereby bridging conceptual framework development with empirical validation.

Given the increasing sophistication of cyber threats and the fragmented nature of existing cybersecurity solutions in Accounting Information Systems (AIS), there is a growing need for integrated cybersecurity architectures that combine technological innovation with governance, transparency, and auditability requirements. Recent research highlights that financial information systems face increasingly complex cyber risks as digital transformation expands the attack surface of financial infrastructures, while many cybersecurity solutions remain technologically fragmented across independent security mechanisms [41, 94]. Consequently,

scholars have emphasised the importance of developing integrated frameworks capable of combining advanced technologies and organisational governance mechanisms to ensure the resilience, transparency, and trustworthiness of accounting information systems [100]. Therefore, this research investigates how emerging technologies such as Blockchain, Quantum Computing, Machine Learning, and Game Theory can be integrated into a unified cybersecurity architecture capable of enhancing the resilience and transparency of accounting and financial systems.

1.3.2. Research Question

To address this problem, the thesis is structured around the following research questions:

RQ1: What are the current cybersecurity challenges facing accounting and finance systems in the era of emerging technologies?

RQ2: How can emerging technologies such as Blockchain, Quantum Computing, and Game Theory be conceptually integrated into a unified cybersecurity architecture for accounting and finance?

RQ3: How can machine-learning models be designed, evaluated, and validated to detect financial fraud effectively in highly imbalanced and high-volume accounting datasets?

RQ4: How does the proposed BQMG-AIS framework enhance auditability, governance, transparency, and fraud detection across digital accounting systems?

These questions establish the foundation for the thesis, guiding the literature review, the multi-method research design, the empirical analyses, and the development of the integrated cybersecurity framework.

1.3.3. Conceptual Positioning of BQMG-AIS

Specifically for Accounting Information Systems, this thesis creates the BQMG-AIS Framework, a novel integrated cybersecurity architecture that combines Blockchain, Quantum Computing, Machine Learning, and Game Theory. This framework is purposefully situated at the nexus of empirical and conceptual research.

❖ **Conceptual:** From a conceptual standpoint, it fills gaps in the literature regarding disjointed cybersecurity tactics, a lack of auditor-focused explainability, and a lack of standardised methods for linking emerging technologies with AIS governance.

❖ **Empirical:** To inform the ML detection layer and provide evidence-based insights into the reliability and auditability of fraud detection, it uses empirical data from three machine-learning fraud detection experiments (Credit Card Fraud, IEEE-CIS, and PaySim datasets).

❖ **Strategic:** From a strategic perspective, it links emerging technologies to governance requirements, accounting controls, audit procedures, and actual cyber risk exposures.

This positioning ensures that the remainder of the thesis logically builds into the final integrated framework presented in Chapter 8.

1.3.4. Statement of Original Contribution

This thesis makes a substantive and integrative contribution to the fields of accounting information systems, cybersecurity architecture, and AI-enabled fraud detection by addressing a structural gap in the existing literature: the absence of a unified, governance-aligned cybersecurity framework tailored specifically to Accounting Information Systems (AIS).

While prior studies have examined Blockchain, Machine Learning, Quantum Computing, and Game Theory in isolation, no research to date has synthesised these technologies into a cohesive, empirically grounded architecture explicitly designed for accounting and finance environments. This thesis advances the field through five principal contributions.:

a. Development of the BQMG-AIS Integrated Cybersecurity Architecture

This study introduces the BQMG-AIS Framework, a novel multi-layer cybersecurity architecture that integrates:

- Blockchain for immutable transaction verification and audit trails,
- Machine Learning for adaptive anomaly detection and fraud identification,
- Quantum-resilient cryptographic principles for forward-looking security,
- Game-Theoretic modelling for strategic attacker–defender interaction analysis.

Unlike existing technology-specific models, BQMG-AIS is explicitly aligned with AIS governance structures, internal control frameworks, and auditability requirements. It represents the first integrated framework that conceptualises these four technological domains as interdependent security layers within accounting systems.

b. An Empirical Multi-Dataset Assessment of Fraud Detection Models in AIS Contexts

This thesis improves empirical research by conducting a multi-dataset machine learning evaluation using three widely recognised fraud-related datasets (Credit Card, IEEE-CIS, and PaySim). Unlike prior studies that rely on single datasets or generic financial contexts, this research:

- Evaluates model robustness across heterogeneous fraud environments,
- Employs precision-recall metrics suitable for highly imbalanced accounting data,
- Incorporates calibration analysis and SHAP-based interpretability mechanisms.

This empirical layer strengthens the credibility of ML-based fraud detection within regulated accounting environments and directly addresses concerns regarding generalisability and audit defensibility.

c. Integration of Explainability and Governance into AI-Driven Cybersecurity

A critical limitation in existing ML-based cybersecurity research is the insufficient consideration of explainability and governance. This thesis embeds interpretability (e.g., SHAP analysis), calibration reliability, and audit transparency into the fraud detection layer, ensuring that AI outputs are defensible before auditors, regulators, and oversight committees.

By explicitly linking technical performance metrics to accounting governance requirements, the research bridges the gap between algorithmic sophistication and institutional accountability.

d. Strategic Modelling of Cyber Threats in Accounting Through Game Theory

The study extends cybersecurity modelling in accounting by incorporating Game-Theoretic attacker–defender dynamics, particularly in relation to social engineering and financial manipulation. Rather than treating fraud detection as a purely technical classification problem, the thesis conceptualises cyber threats as strategic interactions influenced by incentives, information asymmetry, and behavioural adaptation.

This strategic layer enhances the theoretical robustness of the proposed architecture and situates accounting cybersecurity within a dynamic adversarial framework.

e. Reframing Emerging Technologies Through an AIS Centred Lens

Finally, the thesis reframes emerging technologies not as generic digital innovations, but as components of an integrated accounting-specific cybersecurity ecosystem. By mapping each technological layer to transaction processing cycles, internal controls, audit functions, and governance mechanisms, the research provides a practical roadmap for auditors, CFOs, financial institutions, and regulators preparing for increasingly complex cyber risk environments.

Overall Scholarly Contribution

Collectively, these contributions move beyond incremental technological enhancement. The thesis advances a structural reconceptualisation of cybersecurity in Accounting Information Systems, from fragmented tool deployment toward an integrated, multi-layered, governance-aligned architecture. In doing so, it bridges conceptual theory, empirical validation, and professional practice, offering both academic advancement and policy-relevant guidance for securing digital accounting ecosystems.

This research combines ideas from Accounting Information Systems (AIS), cybersecurity governance, and socio-technical systems theory. From an AIS perspective, the study focuses on data accuracy, traceability, internal controls, and adherence to regulations. Cybersecurity governance helps align technical security measures with organisational risk management and responsibilities. Additionally, a socio-technical approach recognises that cybersecurity outcomes result from the interaction among technology, human behaviour, and organisational practices. By bringing these together, the study sees cybersecurity not just as a technical issue, but as an important part of managing financial information systems.

1.4. Structure of the Thesis

This thesis is organised into eight chapters, each building on the previous one to establish a comprehensive framework for strengthening cybersecurity in accounting and finance systems through the adoption of emerging technologies.

- **Chapter 1** introduces the research context, rationale, and the significance of cybersecurity in accounting and finance. It delineates the technological foundations of Artificial Intelligence, Blockchain, Quantum Computing, and Game Theory, and presents the research background, objectives, and contributions.
- **Chapter 2** offers a thorough literature review focused on advanced cybersecurity frameworks that incorporate Blockchain, Quantum Computing, Game Theory, and Machine Learning. It critically examines existing studies, identifies pertinent research gaps, and lays the theoretical groundwork for the subsequent chapters.
- **Chapter 3** investigates the applications of Blockchain and Artificial Intelligence in securing accounting systems, addresses adoption challenges, examines theoretical frameworks, and considers implications for auditors and accountants.
- **Chapter 4** explores innovations in cybersecurity for accounting and finance information systems (AFIS) driven by Artificial Intelligence, emphasising the challenges of implementation, ethical considerations, and best practices.
- **Chapter 5** evaluates the transformative potential of Quantum Computing to enhance cybersecurity in accounting and finance. This chapter analyses encryption techniques, quantum-resilient algorithms, and proposes a conceptual framework for Quantum-based cybersecurity.
- **Chapter 6** develops a Game-Theoretic model to address cyber threats arising from social engineering within accounting systems. It formulates strategic defence mechanisms based on equilibrium principles and validates the proposed Game-Theoretic Model (GTM) framework.
- **Chapter 7** empirically implements fraud detection models driven by Artificial Intelligence, utilising diverse datasets including Credit Card, IEEE-CIS, and PaySim. This chapter evaluates the model's performance, interpretability, and practical integration into accounting workflows.
- **Chapter 8** synthesises findings from the preceding chapters and proposes the integrated Blockchain, Quantum Machine Learning, Game Theory (BQMG) Framework, extending it into the BQMG-AIS architecture tailored for cybersecurity in accounting.
- **Chapter 9**, the last chapter, concludes with an overview of theoretical, methodological, and practical contributions, as well as limitations and future research directions.

This thesis uses a combined approach across multiple studies, with Chapters 3 to 8 related but able to stand alone. Each chapter examines a different aspect of cybersecurity in accounting systems, such as blockchain for data security, machine learning for detecting unusual activity, quantum computing for future encryption, and game theory for understanding attacker and defender strategies. Although each chapter can be read on its own, together they form the

BQMG-AIS framework. This structure allows for detailed analysis in each area while keeping the overall flow of the thesis clear. It helps to bring all the parts together into a single, organisation-focused cybersecurity model.

Collectively, these chapters provide both theoretical insights and practical avenues for harnessing emerging technologies to enhance cybersecurity resilience, ensure audit assurance, and foster trust within contemporary accounting and finance ecosystems.

The foundational discussion of this chapter emphasises the changing cybersecurity requirements in accounting and finance systems. It is essential to look ahead and examine the broader body of scholarly and professional literature that addresses these challenges. The following chapter presents an extensive literature review of cutting-edge cybersecurity paradigms, with a focus on Blockchain, Quantum Computing, Game Theory, and Machine Learning.

Chapter 2

2. Literature Review on Advanced Cybersecurity Frameworks for Accounting Blockchain, Quantum Computing, Game Theory, and Machine Learning

2.1 Conceptual Foundations of AIS Cybersecurity

2.1.1 Cybersecurity in Accounting: Governance & Audit Perspective

This research project evaluates the overall performance, efficiency, and effectiveness of ML/AI tools within blockchain-based cybersecurity strategies integrated into an organisation's management and reporting system.

The rapid digital transformation of accounting and finance systems has fundamentally altered the cybersecurity risk landscape within Accounting Information Systems (AIS) [101]. Financial data is increasingly processed through cloud infrastructures, enterprise platforms, real-time reporting systems, and algorithmic decision-support tools. While these technologies enhance operational efficiency and data analytics capability, they simultaneously expand the attack surface and introduce complex interdependencies across technological, organisational, and behavioural layers [102].

Existing cybersecurity research in accounting and finance has largely evolved along technology-specific trajectories. Blockchain research emphasises data immutability and decentralised trust mechanisms; machine learning studies prioritise anomaly detection and fraud classification performance; quantum computing literature addresses cryptographic resilience and computational acceleration; and game-theoretic models explore strategic attacker-defender dynamics. However, these streams often operate in isolation, resulting in fragmented protection architectures that do not fully address the integrated nature of AIS environments[103].

Moreover, accounting systems operate within highly regulated frameworks requiring auditability, explainability, internal control validation, and governance transparency. Many technically advanced cybersecurity models fail to align explicitly with these governance requirements, limiting their practical adoption in accounting contexts.

Accordingly, this chapter critically reviews existing literature across blockchain security, machine-learning-driven fraud detection, post-quantum cryptography, and game-theoretic cybersecurity models, with a specific focus on their applicability to Accounting Information Systems. The review moves beyond descriptive summarisation to identify structural gaps, conceptual fragmentation, and areas of underdeveloped integration. These identified gaps provide the analytical foundation for the BQMG-AIS framework presented in later chapters.

2.1.2 Technology-Specific Research Streams in AIS Cybersecurity

Building on the multidisciplinary foundation established in the previous chapter, this literature review examines the major research streams that inform contemporary cybersecurity strategies in Accounting Information Systems (AIS). Existing literature examining cybersecurity technologies in finance and accounting can broadly be synthesised into four dominant streams:

blockchain-based security frameworks, machine-learning-driven cyber-threat detection, quantum computing and post-quantum resilience, and game-theoretic security modelling [47, 104-107]. Although these technological domains have produced significant advancements, much of the existing research remains fragmented, with limited integration across technologies within accounting governance environments [47, 108].

The growing adoption of Artificial Intelligence (AI) and Machine Learning (ML) in organisational networks reflects a broader shift toward automated cybersecurity mechanisms capable of detecting and responding to evolving threats [105],[109]. However, identifying and mitigating security risks within complex digital infrastructures remains a major challenge for researchers and practitioners alike [110]. Much of the early cybersecurity research has relied on systematic literature review (SLR) methodologies to synthesise existing findings, identify knowledge gaps, and guide future investigations [111].

Existing cybersecurity research relevant to Accounting Information Systems can be categorised into four major technological streams: blockchain-based security frameworks, machine learning-driven cyber-threat detection, quantum computing and cryptographic resilience, and game-theoretic security modelling. While each stream contributes valuable insights, the literature demonstrates limited integration across these domains, creating challenges for developing comprehensive cybersecurity architectures within accounting systems. The following sections analyse key contributions across the four technology streams most relevant to this research.

a. Blockchain-Based Security in Accounting and Cybersecurity

Blockchain technology has emerged as a significant technological innovation in cybersecurity and accounting research due to its decentralised architecture, cryptographic security mechanisms, and immutable transaction records [104, 108]. In financial information systems, blockchain enables distributed verification of transactions, reducing reliance on central authorities while enhancing data transparency and auditability [47],[112]. Because accounting systems rely heavily on trustworthy and tamper-resistant financial records, blockchain has attracted considerable attention as a potential mechanism for improving cybersecurity governance in Accounting Information Systems (AIS) [108].

One of the earliest comprehensive studies examining cybersecurity in the accounting domain is the systematic review conducted by [47], which analysed 39 peer-reviewed studies published between 2000 and 2018. The study highlights the increasing importance of cybersecurity investment in financial organisations and emphasises the role of internal auditing in monitoring and controlling cyber risks. Empirical regression analysis was identified as the most commonly used methodology in accounting cybersecurity research. The authors also observed that investors tend to lose confidence in organisations that experience cyberattacks, highlighting the need for stronger cybersecurity governance and risk-mitigation

strategies [47] [113]. The study further identifies a critical research gap regarding the training and competence of auditors in addressing cybersecurity threats.

Additional systematic reviews have examined the role of blockchain in cybersecurity applications. The review conducted by [114] investigates blockchain as a cryptographic distributed ledger technology capable of facilitating secure and trusted transactions among untrusted network participants. Following the introduction of the Bitcoin blockchain in 2008, numerous platforms such as Ethereum [115] and Hyperledger Fabric [108] have expanded blockchain's applicability across diverse domains, including IoT security, data storage, and network protection. Using databases such as IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, and Google Scholar, the authors identified a growing body of research focusing on blockchain-enabled cybersecurity mechanisms. However, the study concludes that systematic investigations specifically addressing blockchain applications in cybersecurity remain limited, particularly in business and financial environments.

Similarly, [112] explores the role of blockchain in protecting critical infrastructure systems. Through a survey of 314 scientific publications, conference proceedings, and research reports, the authors analyse blockchain's potential to secure energy infrastructure and industrial control systems. The study emphasises blockchain's ability to provide distributed data storage, encryption-based verification, and peer-to-peer communication mechanisms. Despite these advantages, the authors acknowledge that blockchain also introduces new vulnerabilities, particularly at the interface between users and systems, where identity-based attacks and implementation weaknesses may occur. These findings highlight the importance of integrating blockchain with complementary cybersecurity technologies.

Within accounting practice, [108] conducted a systematic literature review examining blockchain's impact on accounting research and practice. Using the Scopus database and following the PRISMA protocol, the study analysed 346 publications related to blockchain applications in accounting, auditing, and business innovation. The results indicate that blockchain can significantly enhance transparency, automate reconciliation processes, and improve the traceability of financial transactions. However, the authors highlight several limitations, including the restricted scope of database coverage and the limited empirical analysis of blockchain-based accounting systems. They further emphasise the need for future research to examine accountability, governance implications, and the integration of blockchain with other digital technologies.

Collectively, these studies demonstrate that blockchain technology can strengthen data integrity and transparency in accounting systems. However, blockchain-focused research often examines the technology in isolation and rarely integrates adaptive threat-detection mechanisms such as machine learning or strategic security modelling approaches.

b. Machine Learning and AI-Based Cyber-Threat Detection

Machine Learning (ML) and Artificial Intelligence (AI) techniques have become increasingly important in cybersecurity research because of their ability to analyse large datasets, identify anomalous patterns, and detect cyber threats in real time [116], [113]. As digital infrastructures expand across organisational networks, traditional rule-based security mechanisms often struggle to identify complex attack patterns, creating the need for adaptive and automated threat detection systems [116]. Consequently, ML-based cybersecurity frameworks have gained prominence in areas such as fraud detection, intrusion detection systems, malware analysis, and phishing identification [117, 118],[119],[120, 121],[122, 123].

The study conducted by [116] provides a comprehensive evaluation of machine learning techniques used in cybersecurity applications. The authors analysed six ML classifiers—Artificial Neural Networks, Deep Belief Networks, Naïve Bayes, Decision Trees, Random Forests, and Support Vector Machines—across multiple cybersecurity domains including intrusion detection systems [117, 118], malware detection [119], phishing detection [120, 121], spam filtering [122, 123], and fraud detection [124]. Using databases such as Scopus, ACM Digital Library, IEEE Xplore, ScienceDirect, SpringerLink, and Web of Science, the study reviewed 143 research articles to compare the performance of different ML models across commonly used datasets.

The findings demonstrate that machine learning algorithms significantly improve detection accuracy in cybersecurity environments. However, the study identifies several challenges, including adversarial attacks on ML models, dataset limitations, and the computational complexity associated with advanced algorithms. Future research directions include developing robust ML models capable of handling adversarial inputs, improving dataset benchmarking techniques, and exploring deep learning approaches in emerging domains such as IoT and smart cities.

Similarly, [113] examines the integration of machine learning and cybersecurity to enhance threat detection and system resilience. The study highlights the increasing prevalence of cyber threats such as eavesdropping, traffic analysis, and denial-of-service attacks in modern digital infrastructures. Machine learning techniques are widely used to detect anomalies, classify malicious activities, and automate security responses. However, the authors emphasise that implementing ML algorithms in large-scale computing environments requires significant computational resources, which may create performance challenges for organisational systems.

Although machine learning offers powerful detection capabilities, existing studies often focus primarily on algorithmic performance metrics rather than governance considerations or integration with other cybersecurity technologies, such as blockchain. As a result, ML-based cybersecurity solutions may lack the transparency and auditability required in accounting environments.

c. Quantum Computing and Post-Quantum Cybersecurity

Quantum Computing represents an emerging technological paradigm with the potential to transform both financial analytics and cybersecurity practices. Unlike classical computing systems, which process information using binary bits, quantum computing uses quantum bits (qubits) capable of representing multiple states simultaneously through quantum superposition and entanglement [104]. These capabilities enable quantum computers to solve complex optimisation and cryptographic problems significantly faster than classical systems, creating both opportunities and risks for financial cybersecurity infrastructures [104],[115].

The study by [104] explores the application of quantum computing within the financial services sector through the case of Intesa Sanpaolo's Quantum Competence Centre (QCC). The research highlights the potential of quantum technologies to enhance financial applications such as credit risk analysis, fraud detection, portfolio optimisation, and financial modelling. By leveraging quantum algorithms, financial institutions may achieve computational efficiencies that are currently unattainable using classical computing systems. However, the adoption of quantum computing in finance remains at an early stage. Hardware limitations, the shortage of quantum software engineers, and the lack of practical financial applications currently restrict large-scale deployment. Additionally, current quantum systems are unable to process large-scale financial datasets efficiently. Despite these limitations, ongoing research aims to develop proof-of-concept models demonstrating the potential advantages of quantum technologies in financial decision-making and cybersecurity protection.

Further advances in this field are illustrated by [115], who investigate the use of Quantum Graph Neural Networks (QGNNs) for financial fraud detection. The study integrates quantum computing with graph neural networks through Variational Quantum Circuits (VQC) to improve fraud detection accuracy. The authors demonstrate that QGNNs may outperform classical machine learning models in detecting complex fraud patterns in financial transaction networks. Nevertheless, the research remains largely experimental, and the practical implementation of quantum-based fraud detection systems in real-world financial environments requires further investigation.

d. Game-Theoretic Approaches to Cybersecurity and Decision-Making

Game Theory has been widely used in cybersecurity research to model strategic interactions between attackers and defenders in digital systems. By analysing decision-making behaviour under conditions of uncertainty and conflict, game-theoretic models provide valuable insights into how organisations can optimise defensive strategies against cyber threats [108], [105, 112, 125, 126],[127-129],[109, 130, 131],[106]. In financial and organisational contexts, such models are particularly useful for evaluating security investments, modelling adversarial behaviour, and understanding incentive structures that influence malicious activities within complex digital ecosystems [105, 112, 125, 126].

[108]The study applies evolutionary game theory to secure supply chain management systems. The authors propose a Game-Theory-Based Secured Supply Chain Architecture (GBSSCA) designed to enhance trust, transparency, and security within multi-factory supply chain environments. The model integrates reinforcement learning techniques, replication dynamic equations, and Q-learning algorithms to simulate interactions among manufacturers, platform users, and potential attackers. Experimental results demonstrate that the proposed architecture improves detection accuracy and strengthens supply chain security mechanisms.

These findings are particularly relevant for accounting systems, which often operate as integral components of digital supply chains. Secure data exchanges and trust-building mechanisms are essential for protecting financial transactions and maintaining organisational accountability. The study also highlights the importance of addressing behavioural and psychological aspects of cybersecurity threats, including social engineering attacks.

Another significant contribution is presented by [106], who investigate the application of game-theoretic techniques to improve the accuracy of tree-based classification models in financial decision-making. The authors propose a two-stage methodology combining machine learning classification algorithms with game-theoretic analysis to reduce misclassification errors in financial credit evaluation. Using the German Credit dataset from the UCI Machine Learning Repository, the study demonstrates that incorporating payoff structures and strategic decision frameworks can significantly improve prediction accuracy.

Game-theoretic approaches, therefore, offer valuable insights into decision-making under uncertainty and strategic threat modelling. However, many existing models rely on simplified assumptions and lack direct integration with real-world cybersecurity infrastructures or accounting information systems.

2.1.3 Cross-Stream Research Gap

The reviewed literature highlights significant advancements in blockchain security mechanisms, machine learning-based threat detection, quantum computing applications, and game-theoretic security modelling. However, these technological developments are largely investigated independently. Few studies attempt to integrate these technologies within a unified cybersecurity architecture aligned with accounting governance requirements.

Accounting Information Systems require cybersecurity solutions that simultaneously ensure data integrity, real-time threat detection, strategic risk modelling, and long-term cryptographic resilience. The absence of an integrated framework combining blockchain verification, machine learning detection, quantum-resilient cryptography, and game-theoretic decision modelling represents a significant gap in existing research. Addressing this gap forms the foundation for the integrated cybersecurity framework proposed in this thesis.

2.1.4 Integrated Literature Gap Map

a. Introduction to the Literature Gap Map

The preceding analysis demonstrates that while the literature on Blockchain, Machine Learning, Quantum Computing, and Game-Theoretic cybersecurity has expanded significantly, it remains structurally fragmented when examined through the lens of Accounting Information Systems (AIS). Technological innovation has progressed rapidly within individual domains; however, integration across domains remains underdeveloped[100, 132, 133].

Theme/ Chapter	Literature	Key Gaps	Gaps Addressed
Blockchain Security in Accounting Systems	Blockchain for immutable ledgers, smart contracts, and real-time audit trails; conceptual models for blockchain-enabled assurance. [32],[134, 135]	1. Studied in isolation (no ML/QC/GT integration). 2. Weak linkage to AIS controls, audit workflows, and fraud analytics. 3. Limited empirical grounding using real datasets.	1. Chapter 3 develops a blockchain-centred AIS cybersecurity model. 2. Chapter 7 provides empirical fraud-detection results supporting integration. 3. Chapter 8 embeds blockchain as the AIS integrity layer in BQMG-AIS.
Post-Quantum Cryptography & Quantum Risks	QC threats to classical cryptography; overview of PQC, QKD, quantum-safe security for finance.[32, 104],[115]	1. Technology-focused literature; little AIS/audit application. 2. PQC/QKD not linked to accounting controls or compliance. 3. No integration with ML or blockchain systems.	1. Chapter 5 develops a quantum-resilient AIS cybersecurity model. 2. Chapter 8 incorporates PQC as the dedicated cryptographic layer in BQMG-AIS.
Game-Theoretic Cybersecurity Approaches	Attacker–defender modelling; security investment; social-engineering games; equilibrium analysis.[32],[108],[112]	1. Too abstract; limited AIS/internal-control context. 2. Rarely combined with ML or blockchain audit trails. 3. Minimal focus on accounting-specific social engineering risks.	1. Chapter 6 develops a GT-based defence model for accounting scenarios. 2. Chapter 8 integrates GT as the strategic/policy engine interacting with ML & BC layers.
ML & Deep Learning for Fraud Detection	Fraud detection using supervised/ensemble/deep learning; high ROC/PR-AUC results; imbalance-handling strategies.[32],[116],[115]	1. Mostly single-dataset studies → poor generalisability. 2. Limited calibration/interpretability for audit needs. 3. Weak linkage to AIS, governance, and auditability. 4. No multi-layer security integration.	1. Chapter 7 evaluates LR/RF/XGBoost across three datasets. 2. Calibration & SHAP used to support audit explainability. 3. Chapter 8 defines ML as the anomaly-detection layer in BQMG-AIS.
Auditability, Explainability & Governance of Accounting AI	Importance of XAI, model governance, internal controls, and regulatory compliance (SOX/IFRS/ethics).[32, 33]	1. Governance/XAI discussions are generic; not AIS-specific. 2. Limited empirical demonstration of SHAP calibration in accounting workflows. 3. No framework integrating AI governance with BC/PQC/GT.	1. Chapter 1 identifies governance and XAI needs for AIS. 2. Chapter 7 operationalises SHAP & calibration for auditors. 3. Chapter 8 embeds cross-cutting governance integration across all layers.

TABLE 2.1 LITERATURE GAP MAP

The literature gap map presented in Table 2.1 synthesises these deficiencies into five interrelated categories:

- (1) blockchain-based accounting security,
- (2) post-quantum cryptographic resilience,
- (3) game-theoretic attacker–defender modelling,
- (4) machine learning-driven fraud detection, and
- (5) governance and explainability in AI-enabled accounting systems.

1. Technology-Siloed Development

A dominant pattern across the literature is the siloed treatment of emerging technologies. Blockchain studies emphasise immutability and distributed verification, yet rarely incorporate adaptive fraud detection models [132, 136]. Machine learning research focuses on performance optimisation but often neglects strategic adversarial modelling or integration with immutable ledgers [133, 137]. Quantum computing literature addresses encryption resilience but remains disconnected from operational AIS control systems [138, 139]. Game-theoretic models analyse attacker–defender interactions but frequently lack empirical validation within real accounting datasets [140].

This siloed development results in isolated security enhancements rather than a systemic cybersecurity architecture.

2. Insufficient AIS Alignment

Much of the cybersecurity literature is developed at a generic organisational or network-security level, with limited explicit mapping to Accounting Information Systems processes such as transaction processing cycles, audit trails, internal controls, and financial reporting integrity [100, 141].

In regulated financial environments, cybersecurity mechanisms must align with:

- Internal control frameworks
- Auditability requirements
- Governance transparency
- Regulatory compliance standards

However, few studies explicitly demonstrate how their proposed models integrate into AIS workflows or support audit committee oversight [132].

3. Limited Empirical Integration Across Technologies

Although machine learning fraud detection research often includes empirical evaluation, it is rarely combined with:

- Blockchain verification layers
- Game-theoretic strategic modelling
- Post-quantum cryptographic considerations

Empirical evidence tends to validate individual algorithms rather than integrated security ecosystems [137, 142]. Consequently, the literature lacks multi-layer empirical validation within AIS contexts.

4. Weak Governance and Explainability Positioning

Explainability and governance considerations remain secondary in many ML-based cybersecurity studies. Performance metrics such as accuracy, recall, and precision are frequently prioritised over interpretability, transparency, and audit defensibility [143], [144].

In accounting environments, however, model decisions must withstand scrutiny from auditors, regulators, and financial oversight bodies [141]. The absence of explicit governance alignment creates a gap between technical performance and institutional trust.

5. Absence of a Unified AIS-Centred Cybersecurity Architecture

Most critically, no existing research proposes a comprehensive framework that simultaneously integrates:

- Immutable transaction verification (Blockchain)
- Adaptive fraud detection (Machine Learning)
- Forward-looking cryptographic resilience (Quantum Computing)
- Strategic adversarial modelling (Game Theory)

within a governance-aligned Accounting Information Systems architecture [132, 140, 145].

The absence of such a unified model represents the central structural gap in the literature.

2.1.5 How the Literature Gaps Shape the Direction of This Thesis

The integrated gaps identified above directly inform the design logic of this thesis.

First, Chapters 3–6 examine each technological stream through systematic and conceptual analysis, ensuring that each domain is grounded in accounting-specific contexts rather than generic cybersecurity discourse.

Second, Chapter 7 provides empirical validation through multi-dataset machine-learning-based fraud-detection experiments, explicitly incorporating performance calibration and SHAP-based interpretability to address governance and auditability deficiencies [144].

Third, Chapter 8 synthesises conceptual and empirical insights into the BQMG-AIS framework, a unified cybersecurity architecture that integrates Blockchain, Quantum Computing, Machine Learning, and Game Theory within an Accounting Information Systems governance structure.

The Literature Gap Map, as detailed in Table 2.1, therefore serves as the analytical bridge between this chapter and the subsequent development of the BQMG-AIS Framework, ensuring that the thesis remains tightly aligned with identified scholarly deficiencies, accounting governance needs, and emerging technological challenges. Thus, it is not merely descriptive; it serves as the analytical bridge between fragmented prior research and the integrative contribution advanced in this thesis.

2.1.6 Integrated Literature Gap for Advanced Cybersecurity Frameworks in AIS

The previous section in Chapter 2 reviewed research on blockchain, post-quantum cryptography, game-theoretic cybersecurity, machine-learning-based fraud detection, and AI governance in accounting and finance. Although this body of work is extensive and rapidly developing, it remains fragmented and often focused on specific technologies. Table 2.1 summarises the main thematic areas, the current state of the literature, and the key gaps that drive this thesis and the development of the BQMG-AIS framework.

a. Cross-Cutting Literature Gaps Aligned with Thesis Aim

Building on the thematic analysis above and in line with the Associate Professor's feedback, several overarching gaps in the literature emerge that directly motivate this thesis.

- **No unified model combining Blockchain, Quantum, ML, and Game Theory for AIS cybersecurity**

Existing research studies these technologies primarily in isolation or in limited pairwise combinations (e.g., blockchain + AI, quantum + cryptography). There is no comprehensive, AIS-centred framework that harmonises all four technologies into a single, multi-layer architecture for accounting cybersecurity.

This thesis covers Chapters 3–7, each of which elaborates on technology-specific models and empirical evidence, which are then integrated in Chapter 8 into the BQMG-AIS framework as a unified architecture for AIS security.

- **Insufficient empirical evaluation of fraud detection methods in accounting datasets**

Many fraud-detection studies depend on generic financial or e-commerce data, often without explicitly presenting results in accounting and auditing terms, and typically using only one dataset. This thesis addresses Chapter 7, which conducts a multi-dataset ML evaluation specifically focused on accounting fraud and AIS, utilising three main datasets and reporting metrics (PR-AUC, recall, precision, calibration, SHAP) that are significant to auditors and finance professionals.

- **Weak explainability and limited auditor-centric evaluation of ML models**

Although ML performance metrics are widely reported, fewer studies focus on whether model decisions are interpretable and trustworthy for auditors, audit committees, and regulators. Explainability tools are rarely mapped to auditability and governance requirements.

This thesis discusses the empirical work (Chapter 7), which emphasises SHAP interpretability, calibration, and model transparency, while Chapter 8 incorporates explainability and governance as explicit design criteria within the BQMG-AIS framework.

- **Limited connection between cybersecurity models and AIS governance and control frameworks**

A significant gap exists between technical security research and the governance/control literature in accounting. Many models do not demonstrate how proposed techniques integrate with AIS processes, internal controls, or regulatory frameworks.

Addressed by this thesis: Throughout Chapters 3–6, the conceptual models are consistently framed in terms of accounting controls, AIS processes, and governance. Chapter 8 explicitly links each BQMG-AIS layer (blockchain, quantum, ML, game theory) to AIS integration points, control objectives, and practical use cases (e.g., accounts payable fraud monitoring, financial statement integrity, social-engineering defence).

b. Positioning of the Present Research

Overall, the literature gap map shows that although notable progress has been made in each technology area, there remains a fundamental lack of integrated, AIS-aligned, and empirically grounded cybersecurity frameworks. This thesis addresses that gap by:

- Conducting systematic literature reviews across blockchain, AI-powered cybersecurity, quantum computing, and game theory (Chapters 3–6).
- Performing a multi-dataset empirical machine learning study on financial fraud detection, emphasising auditability and explainability (Chapter 7).
- Integrating these strands into the BQMG-AIS framework, which combines Blockchain, Quantum Computing, Machine Learning, and Game Theory for cybersecurity in accounting and finance (Chapter 8).

This combined gap map thus directly supports the research problem and questions introduced in Chapter 1 and offers a clear conceptual link to the subsequent methodological and empirical chapters.

Chapter 3

3. Blockchain and Artificial Intelligence for Cybersecurity in Accounting and Finance Systems: Adoption, Challenges, and Opportunities

3.1 Overview of Blockchain

3.1.1 Introduction

Adopting artificial intelligence (AI) and blockchain-based cybersecurity strategies in accounting represents a transformative shift in the management and protection of financial data. [33] The study pointed out that the digital era continues to evolve, and accounting systems have become increasingly reliant on advanced technologies, which, while enhancing efficiency, also expose them to significant cybersecurity threats. Integrating AI and blockchain technologies offers a robust solution to these challenges by providing enhanced security measures that protect against unauthorised access and data breaches. Further, the study explains that blockchain technology ensures data integrity and transparency through its decentralised, immutable ledger system, making it particularly beneficial for auditing and compliance processes. Additionally, it clarifies that this technology reduces fraud risk and enables the creation of secure, transparent financial records.

Meanwhile, AI and machine learning algorithms are employed to detect and respond to cyber threats in real-time, thereby augmenting the capacity of accounting firms to safeguard financial data. [146] Despite the promising benefits, integrating these technologies into accounting practices poses significant challenges. High implementation costs, regulatory uncertainties, and the need for continuous updates and training are significant barriers that must be addressed. Moreover, the ethical implications of using AI in cybersecurity, such as data privacy and transparency concerns, require careful consideration.

Despite increasing digitalisation of accounting information systems, traditional centralised architectures remain vulnerable to data manipulation, unauthorised access, and audit trail tampering. Such vulnerabilities raise significant concerns regarding the integrity, transparency, and traceability of financial records in modern digital environments. Centralised databases create single points of failure and increase exposure to cyber threats, fraud, and unauthorised modifications of financial data [147, 148]. Blockchain technology has emerged as a potential solution to these challenges due to its decentralised architecture, cryptographic security mechanisms, and immutable ledger structure [149, 150]. By distributing transaction records across a network of nodes and validating entries through consensus mechanisms, blockchain reduces the risk of data manipulation and enhances trust in financial information [151].

Furthermore, blockchain-enabled systems create tamper-resistant audit trails that allow transactions to be permanently recorded and independently verified, thereby improving the traceability and reliability of accounting data [152, 153]. These characteristics enable continuous auditing and strengthen internal control environments by ensuring that financial

records cannot be altered without detection [154, 155]. As a result, blockchain has been increasingly recognised in the literature as a transformative technology capable of enhancing the security, transparency, and reliability of accounting information systems [156]. Accordingly, this chapter examines how blockchain technology can serve as a cybersecurity mechanism for accounting information systems by providing immutable ledger structures and distributed verification mechanisms. The objective is to evaluate blockchain's potential to strengthen financial data integrity and support the broader cybersecurity architecture proposed in this thesis.

3.1.2 Conceptual Boundary of Blockchain

This chapter focuses exclusively on blockchain as a cybersecurity mechanism that enhances the integrity, transparency, and auditability of accounting information systems. The chapter examines blockchain's immutability, consensus mechanisms, and decentralised structure as tools for protecting financial records from tampering and manipulation. Importantly, this chapter does not examine blockchain token economics, mining efficiency, cryptocurrency market behaviours, or distributed applications unrelated to accounting. These areas fall outside the conceptual boundary of the thesis. The focus remains strictly on blockchain's role as a cybersecurity and assurance layer within AIS.

3.1.3 What is Blockchain?

Blockchain is a distributed ledger technology that records transactions across multiple nodes, ensuring that financial records cannot be altered without network consensus [157, 158]. This immutability makes blockchain particularly relevant for accounting information systems, where transaction integrity and auditability are essential. Instead of providing administrator rights that enable the editing and deletion of data, Blockchain changes transactions through a consensus-based protocol [159].

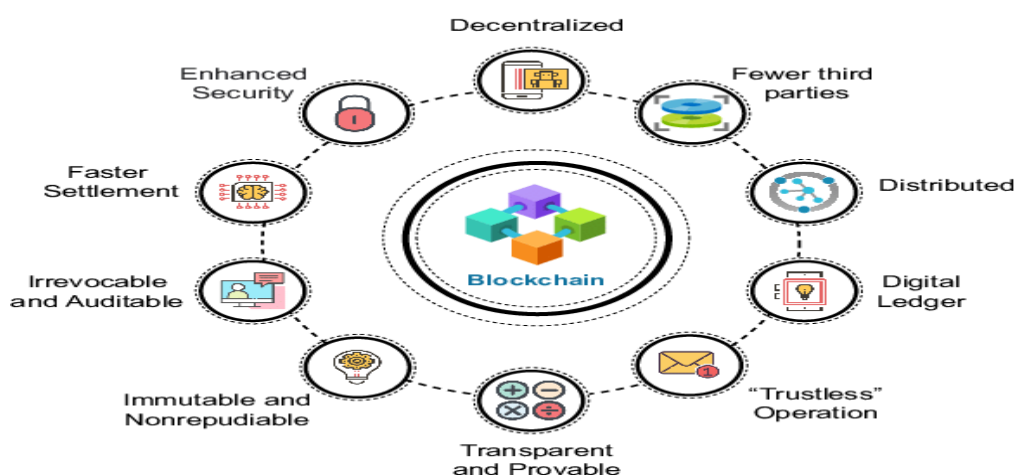


FIGURE 3.1 The key features of Blockchain Technology

SOURCE: [160]

Whether we refer to permission, public, private, or permissionless, any model is supported by Blockchain [100, 161]. We should follow the permission blockchain if we want the best

solution for protecting client privacy and meeting regulatory standards [162]. The literature highlights the technical structure of Blockchain [157, 163], where new entries are added to the end of the ledger, linking the previous block to the new ones via a hash value. The hash value changes with the changes made to the block, resulting in a broken chain [157, 163]. Also, by preventing single-node tampering through each node getting a copy of the ledger [159], we can say that the transaction may be either a trade or a legal contract created using smart contracts [164], so we can say that a significant transformation is required in the economic [165-167], political [165], and social context [165, 168]. It would not be wrong to say that Blockchain has the potential to bring about those changes[169]. Figure 3.1 illustrates the key features of Blockchain Technology. Ultimately, the globally recognised Big Four accountancy firms (Deloitte, PwC, Ernst & Young, and KPMG) showed interest in blockchain technology, launching several new projects.

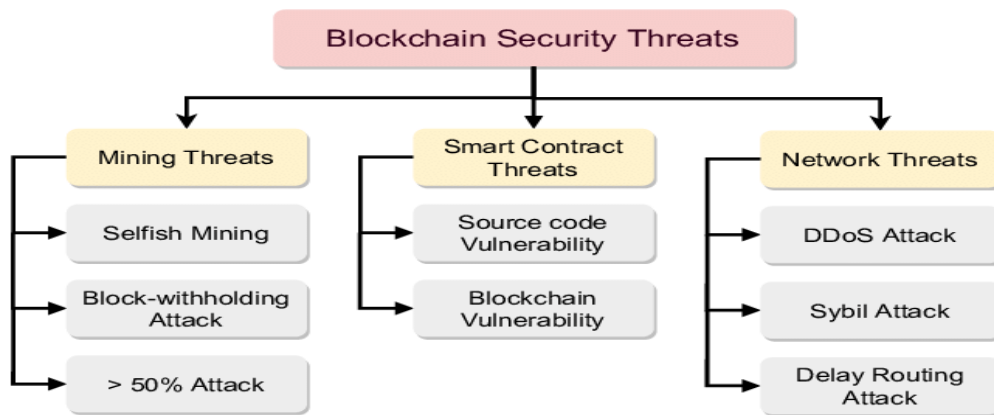


FIGURE 3.2 Different security threats in edge networks

SOURCE: [160]

Financial and professional institutions have collaborated to lead various initiatives in accounting and auditing. It includes exploring the technology's potential, such as Rubix, the first Blockchain-based platform launched by Deloitte, which enables users to build their customised Blockchain and smart contracts [170]. For example, Deloitte has implemented advanced encryption mechanisms and AI-driven cybersecurity tools to enhance the protection of sensitive financial data within accounting systems. Figure 3.2 illustrates the blockchain security threats as identified in edge networks.

3.1.4 Blockchain Technology (BCT) & Its Suitability

[171]Recently, Blockchain Technology has become popular in the financial ecosystem and is considered a critical emerging technology [172]. Another study examined the emergence of BCT as a technology that provides a secure and trustworthy environment for information systems. BCT digitally encodes all the assets, whether tangible or intangible, as a distributed database. It is not wrong to say that BCT is one of the most crucial and evolving technologies in the computation model [173, 174]. At the same time, BCT is facing increasing cyberattack challenges[175]. Blockchain is one of the most widespread technologies, allowing transactions

to be more transparent than traditional centralised systems. Figure 3.3 explains how blockchain technology works. This technology can help organisations manage and distribute digital data using mutually distributed ledgers. Literature shows that blockchain technology has four key components. These components include non-localisation (decentralisation), security, audibility, and intelligent execution [95]. This technology initially focuses on sharing and executing digital events among given blockchains. [176] Blockchain is an emerging technology, and its application has increased rapidly. However, it is quite possible to have unjustifiable use of this technology, and Greenspan, in the article [177], has given us eight criteria that must be met to ensure the suitability of Blockchain Technology application:

- a. The first criterion is the need for a shared database, which also requires a ledger with a set of transactions.
- b. The second criterion is the databases where multiple writers are happy to insert the data.
- c. The third one is the mistrust of the inter-writer, who does not allow any peer to edit routine transactions.
- d. Fourth is disintermediation, where the third party does not, and the writer is unwilling to control the database completely.
- e. Fifth is the transaction interaction, which confirms the undeniable link between the two transactions.
- f. Sixth is transaction verification, where each transaction is automatically verified.
- g. The seventh is that validation of existence means that nodes verify transactions.
- h. The last one stores values representing entries that have real-world value.

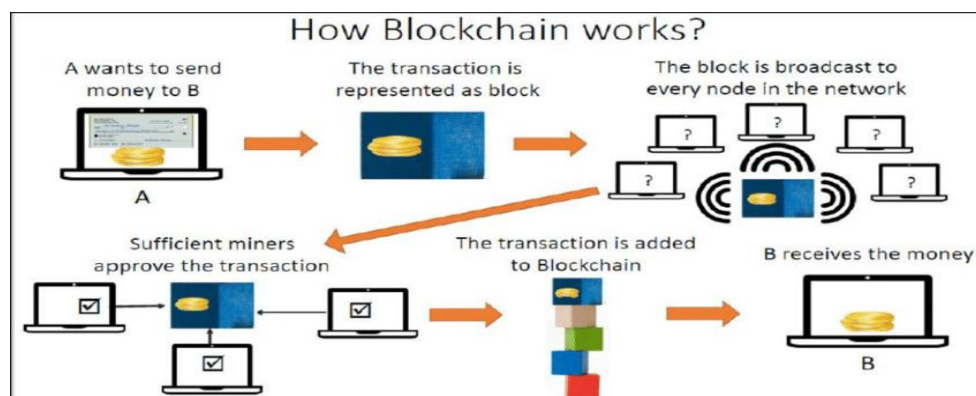


FIGURE 3.3 Schematic Diagrams explaining How Blockchain Works

SOURCE: [178]

3.1.5 Generations of Blockchain

[179] This section provides a brief overview of the three generations of Blockchain Technology that support money transactions, assets, and smart contracts. Satoshi Nakamoto introduced the first generation of Blockchain in 2009 [180].

- a. **(Blockchain 1.0) Bitcoin is the first cryptocurrency to use blockchain technology, specifically designed for money transactions.** The second generation overcame this concern by adding additional cases that made asset exchanges possible, rather than only money. Users who own assets or shares can exchange them for goods and property and participate in voting [181].
- b. **(Blockchain 2.0) Ethereum Rise, a smart contract, is a third-generation blockchain** that is programmed and verified by everyone in the network, compelling both parties to strictly adhere to it. The third generation introduced an application with enhanced Blockchain capabilities, recognised worldwide, and saw increased adoption across other critical services [182], [183].
- c. **(Blockchain 3.0) Next-Generation Technology Without Mining, Distributed Applications (DApps)** need not be prepared. Individuals or corporations that need applications and services do not need to prepare them. They can use decentralised storage and decentralised communication to make this application work. They can work because they are very different from other networks. As the study suggests[183], we can develop this formula: DApp = frontend + contracts (running, i.e., on Ethereum).
- d. **(Blockchain 4.0) Making Blockchain usable in Industry 4.0** is the latest. It is because people's robust changes, driven by the essential requirements of integrity and trust, can be addressed. Industry 4.0 comprises three core components: automated systems, enterprise resource planning, and systems that work together. The core components are trust and protection from the outside world, which are somehow integrated with this new industrial revolution and from anyone who tries to access confidential data or information. Moreover, the author suggested using this to meet the need for more trust and privacy protection in the business world [183].

Mining approach	Resources needed	Randomness	Implementat ions	Reward miner?
Proof of Work (PoW)	High computational power	No randomness	Bitcoin	Yes
Proof of Stake (PoS)	Wealth or stake	Randomised BC selection	Ethereum	No
Proof of Space (PoSpace)	High memory	No randomness	Permacoin	Yes
Proof of Importance (PoI)	Node significance	No randomness	NEM	Yes
Measure of Trust (MoT)	Trustworthiness	No randomness	Not implemented	Yes (trust)
Minimum Block Hash	None	Randomised BC selection	Bitcoin extension	Yes
Practical Byzantine Fault Tolerance (PBFT)	None	No randomness	Hyperledger	No

TABLE 3.1 Comparison of different mining techniques

Source: [184]

3.1.6 Mining of Blockchain

What do we mean by mining? This process creates a block that gradually gets attached to the database. Miners can participate in network transactions to be rewarded for their speed and accuracy. Miners in Bitcoin, a blockchain application, create the first block and receive a reward, typically in the form of money for financial transactions, becoming a critical concept in blockchain technology. Miners may adopt several approaches discussed to win. Major mining approaches have been summarised in Table 3.1. According to the table, Proof of Work (commonly abbreviated as PoW) is used to prevent cyber-attacks 51% of the time. Cryptocurrencies like Bitcoin use double-spending to confirm transactions initiated to create new blocks on the chain. A consensus algorithm is used.

3.1.7 Cybersecurity goals

[176] The US National Institute of Standards and Technology (NIST) states that cybersecurity involves safeguarding, preserving, and protecting computers, electronic communications systems, services, and networks. It also includes information to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.[185]. The definition above clearly helps us to identify the five security dimensions below:

a. Availability

Guarantees access to and use of information on a timely and reliable basis [185].

b. Integrity

It is "a property whereby data has not been altered in an unauthorised manner since it was created, transmitted or stored." [186] However, integrity is an inherent property of blockchain technology, meaning that using it ultimately provides integrity.

c. Authentication

Establishes confidence in the user's or the information system's identity [187]. We can say that the system stakeholders are involved in this process, not the data at stake.

d. Confidentiality

This means that sensitive information is not shared or disclosed to unauthorised entities. [187] The study explained that if we talk about blockchain technologies by design, BC does not provide this feature, as they are designed to provide auditability.

e. Non-repudiation

Means "protection against an individual wrongly refusing to perform a specific action." [187]. Variants of this characteristic, such as sender or receiver non-repudiation, have emerged due to the vast array of possible activities that may be designed into an IT system. Specifically, in specific blockchain use scenarios, sender non-repudiation is also necessary. Considering examples, we can mention cryptocurrencies to avoid the double-spending problem [188].

3.2 Theoretical Background, Research Aim and Research Questions

3.2.1 Introduction

This thesis builds on the work of Priom and his research team [146], examining how AI- and blockchain-based cybersecurity strategies are being adopted in accounting to enhance data

protection, operational efficiency, and regulatory compliance. By analysing current research trends and future implications, it offers a comprehensive perspective on how these technologies can strengthen trust and security in financial data management [189]. This research has been divided into two parts. The first introduces the conceptual model of personal computing utilisation proposed by Thompson [190]. This model has been adapted to incorporate blockchain-based cybersecurity measures used in financial and accounting systems. The second part outlines the research questions and propositions examined in this thesis, as presented in Section 0, and discusses the corresponding findings in detail in Section 3.6 of this chapter. Priom's work is selected due to its strong alignment with technology adoption models and its applicability to evaluating emerging cybersecurity mechanisms in accounting environments [146]. Compared to alternative models, it provides a structured framework for analysing organisational and behavioural factors influencing technology adoption.

3.2.2 Main Research Question Alignment

This chapter contributes to RQ3, which asks how Blockchain, Quantum Computing, Machine Learning, and Game Theory can be integrated into a unified cybersecurity architecture for accounting and finance systems. Blockchain is positioned as the technological foundation for ensuring data integrity and audit trail reliability within this architecture, providing immutable evidence that complements the detection, encryption, and behavioural defence mechanisms discussed in later chapters.

Factors	Explanation
Job-fit	An individual believes that using Blockchain-based Cybersecurity technology will enhance their job performance.
Complexity	Perceived difficulty in understanding and using BC-based cybersecurity technology.
Perceived Consequences	Choices made by organisations for maximum rewards.
Affect towards use	Measurement of the feelings (joy, pleasure, elation, depression, disgust or hate) towards the implementation or usage of Blockchain-based cybersecurity measures.
Social Factors	Influence of BC-based cybersecurity perception among other players and market competitors.
Culture	Represents the organisational cybersecurity culture, including shared values, awareness, and behavioural norms.
Facilitating Conditions	Factors easing the use of BC-based cybersecurity measures in an organisation.

TABLE 3.2 Factors for Applying Blockchain-Based Cybersecurity Measures in an Organisation.

3.2.3 Conceptual Model of Finance and Accounting System Exploiting Blockchain-based Cybersecurity Strategies

This research project focuses on only four factors of the conceptual model, as outlined in Table 3.2, through the propositions developed. The four factors are the first four, and we add two more to consider here: the Relationship and the culture.

We illustrate the four factors of the Finance and Accounting System utilisation models customised for Blockchain-based cybersecurity measures, including job fit, complexity, perceived consequences, and their effect on use. Next, we add two more features of blockchain technology: the relationship and the cultural factor, which we briefly discuss in this section as we respond to the propositions.

a. Job fit

[190] The study explained that job fit helps gauge an individual's confidence in using technology, enhancing their job performance. [169] For example, the administration cost of an insurance claim includes processing, which can become complex and expensive due to differences and misconceptions surrounding the term. However, smart contracts can address these problems by structuring authentic if-then relationships in insurance policies [169]. Agreed-upon procedures can be implemented by executing the terms adopted through the digital protocol, thereby automating these policies. These result in reduced cost and effort previously required, ultimately lowering the cost of their other insurance products and creating a competitive edge in attracting more customers [169].

b. Complexity

The study [190] defines complexity as the apparent impediment to understanding and applying innovative technology, which aligns with this article's focus on cybersecurity measures using Blockchain technology in accounting and finance. [191] The study explained in the report that a local ledger uses blockchain technology to store and monitor control data access using improved validity of wireless internet access points technology. Also, Blockchain technology assists in navigating a web page using the accurate Domain Name System DNS records, enabling secure online applications with highly secure interaction methods.

c. Perceived Consequences

[190] The study explained that choices made by individuals with the perception of getting a maximum reward, while further detailing the consequences, aim to enhance job flexibility and satisfaction. [191] The study explained that the actual data owners get complete control over their data by implementing Blockchain using encryption, which boosts sharing security and data storage on the client side.

d. Affect towards use

[190] The study used "affect" to measure feelings like pleasure, joy, depression, disgust, hate, satisfaction, and trust. Moreover, this study captures these feelings through measurements of the implementation of Blockchain-based cybersecurity measures by professionals, corporations, organisations, or entities. [191] The study points out that the primary benefit of using blockchain technology is the creation of trust between strangers dealing through the Internet of Value. This confidence is built into the system, enabling instant, efficient execution of trades that eliminate middlemen (third parties). The benefits of the Internet of Value are likely to result in significant changes.

e. Relationship

[192] The article explains that game theory provides a set of mathematical tools for analysing interactions among rational decision-makers. This relationship involves a game in which each decision maker chooses a strategy as a player to maximise their utility, considering the strategies of the other players. Considering the essential terms of this game theory, the first one is the Player, a decision-maker in the game who can be a blockchain user, a mining pool, or a miner. The next one is the Utility, which can be a payoff, revenue, or interest. It is the expected outcome of the player.

f. Culture

[193] One can defend their data and themselves from bad actors by raising cybersecurity awareness. [194] People can learn about the risks of cybercrime and the importance of taking precautions to stay safe online through awareness of cybersecurity. Nevertheless, it also complies with organisational rules and deters them from engaging in deviant behaviours. According to a practitioner study, organisations with a security-conscious culture are three times more likely to have comprehensive security programmes and four times less likely to experience an insider data breach.

3.2.4 Research Aim and Research Question

a. Research Aim

As detailed in the first chapter on Information Technology concerns related to accounting (illustrated in Figure 1.1), the relationship between the accounting challenges and the IT response to those challenges is discussed. Figure 1.2 and Figure 1.3 briefly describe IT-related responses to accounting challenges embedded in the accounting system, which makes our accounting and reporting system vulnerable to cybercrime. Due to their ability to identify problems, Artificial Intelligence and Machine Learning are gaining popularity, and the adoption of data science in corporate networks is becoming a trend that automates and offers better solutions. However, the study suggests the researchers' challenge is identifying the security risks that occur on the web [110]. This project evaluates the overall performance, efficiency, and effectiveness of blockchain in cybersecurity strategies, integrated within an organisation's general management and reporting system, using ML/AI tools.

b. Research Question

In this section, we be covering concerns as pointed out in the article of [134], where it was identified the gap for future research required in the area of cybersecurity concerning the implementation of HTTPS encryption and leaving end users to use some forms of encoding for daily communication so now forcing the need to do research for securely managing the surrounding cryptography and certification schemes. [134] Furthermore, a few primary studies have been conducted to find solutions or address security issues using the Ethereum platform and smart contracts. Ultimately, this will drive further research into how Blockchain platforms can be utilised to develop innovative Cybersecurity Solutions. [189] The mutual relationships

among Blockchain-based cybersecurity systems among workers, professionals, corporations, and organisations have been investigated for decision-making across various organisational functions. The research question this artefact explores is: how can Blockchain-based cybersecurity be utilised in organisational accounting? Blockchain-based cybersecurity utilisation in accounting can increase organisational efficiency, safety, security, trustworthiness, return on investment, quality, creativity, customer satisfaction, employee empowerment, and many more. Due to the limitations of this article's length, only four propositions have been explored. Based on the entire research project, the main question is: What factors influence BC-based cybersecurity technology's quicker and faster adoption in an organisation's accounting and finance department? This research aims to design a conceptual framework that future researchers can utilise for further implementation. This article provides a detailed examination of the connection between Blockchain-based cybersecurity measures and strategies implemented through Machine Learning Algorithms in accounting and finance. Building on the secure core that Blockchain provides, this chapter explores how artificial intelligence complements Blockchain-guided cybersecurity policies. It discusses AI's role in empowering accountants and auditors with adaptive, self-aware defences against the widening cyber threats.

3.3 Blockchain-based Cybersecurity

[134] The article discussed how blockchain technology, a cryptographic-based distributed ledger, can enable untrusted participants to conduct trusted transactions within the system. [157, 195] Blockchain applications addressing cybersecurity problems require thorough research to mitigate emerging cyber-related threats through the solutions offered by emerging technologies. Taylor's paper focused on using blockchain technology to address cybersecurity concerns, including business-related security, privacy, accountability, and data integrity across networked devices such as the Internet of Things (IoT) [134].

The study has comprehensively described the basic structure of Blockchain, as shown in Figure 3.4 [196]. The literature [197] notes that Blockchain technology has broad applications across numerous industries. For example, its ledger system can detect financial transaction fraud, facilitate the secure sharing of patient medical records among healthcare providers, and improve the tracking of artists' intellectual property and music rights. Law enforcement agencies, such as metropolitan police, can leverage Blockchain's robust security features to preserve evidence in cyberbullying and cyberstalking cases [198, 199]. It ensures the integrity and reliability of digital forensic evidence [199], enhancing the efficacy of legal proceedings in cybercrime investigations. Blockchain technology is evolving beyond its initial application in cryptocurrency transactions, paving the way for decentralised applications (dApps) that operate without intermediaries. As the literature mentions [134], this shift can redefine digital ecosystems by enhancing security, transparency, and efficiency in various sectors. Moreover, blockchain's decentralised architecture could be a foundational component of next-generation

internet security infrastructures, strengthening data integrity, authentication, and privacy protections. As a result, blockchain is emerging as a transformative technology with far-reaching implications beyond financial transactions.

Layer	Component Type	Component Name
Application Layer	Basic	APIs
Application Layer	Basic	Regulatory Mechanism
Application Layer	Basic	Cross-Chain Heterogeneity
Application Layer	Basic	Cloud Service
Contract Layer	Basic	Smart Contract
Contract Layer	Basic	Programming Language
Contract Layer	Basic	Formal Verification
Contract Layer	Basic	Testing Network
Contract Layer	Basic	Program Analysis Tools
Contract Layer	Basic	Sandbox Environment
Contract Layer	Basic	Script Coding
Incentive Layer	Basic	Incentive Mechanism
Incentive Layer	Basic	Distribution Mode
Incentive Layer	Basic	Mechanism Optimization
Consensus Layer	Basic	PoW
Consensus Layer	Basic	PoS
Consensus Layer	Basic	PBFT
Consensus Layer	Security	Verification Mechanism
Consensus Layer	Security	Trusted Hardware
Network Layer	Basic	Slicing Technology
Network Layer	Basic	Networking Mode
Network Layer	Basic	Extended Network
Network Layer	Basic	ANC Technology
Network Layer	Basic	P2P Network
Network Layer	Security	Verification Mechanism
Network Layer	Security	Intrusion Detection
Data Layer	Basic	Block
Data Layer	Basic	Chained Data Structure
Data Layer	Basic	Data Transaction
Data Layer	Basic	Key Management
Data Layer	Basic	Cryptography

FIGURE 3.4 The basic features of Blockchain Technology

SOURCE: [196]

Prior research on blockchain in accounting can be broadly categorised into three streams. The first examines blockchain's ability to enhance financial transparency and record immutability [100]. The second investigates its role in strengthening cybersecurity resilience through decentralised verification mechanisms [56]. The third focuses on its implications for auditing and automated assurance processes [200]. While these studies highlight important capabilities, they largely examine blockchain in isolation rather than as part of an integrated cybersecurity architecture for accounting systems.

3.3.1 Blockchain and Accounting

As mentioned in the article [201] BC, a dispersed, digitised database capable of conducting official transactions without third-party interference is a potential game-changer for the accounting profession. The literature [33] highlights the relationship between cybersecurity and financial data, emphasising that cybersecurity has become a critical component in safeguarding financial data within the accounting field in today's digital landscape. Financial information's highly sensitive and pivotal nature makes it an attractive target for cybercriminals, underscoring the urgent need for robust cybersecurity measures to ensure its protection. The escalating frequency and sophistication of cyberattacks have further emphasised the imperative for enhanced security protocols to prevent unauthorised access, data breaches, and financial fraud [202].

3.3.2 Cybercrimes

[203]Cybercriminal activity is the biggest threat to Internet networks and all users, becoming humanity's most significant challenge. Intellectual property crimes are committed when someone engages in activities such as manufacturing, distributing, or selling counterfeit or pirated goods, patents, literary works, trademarks, industrial designs, or artistic creations for commercial gain. Most cybercrimes are connected to a lack of protection or ineffective programs or software. Nevertheless, even with a highly protected combination of different software, no one could be completely safe.

[183] It has briefly discussed four types of cybercrimes:

The first one is Malware, the ransomware attack.

The second one is the Web Application Attacks, including the theft of keys,

The third one is the Distributed Denial of Service Attacks, being the attacks on the process and

The last one is the Man-in-the-Middle Attack, which is a form of intellectual property theft.

[183]Cybercriminals use various tools to execute their crimes, which are sent via email attachments or Phishing emails, and Users visiting malicious websites. Further, the article clarifies that many types of software are available to protect computers, but protecting them from professional cybercriminals is becoming increasingly complex. The financial services industry is driving positive change through powerful blockchain innovations, which fall into two categories: public and permissioned Blockchains. Centralised administrators are increasingly delegating their roles to new authentication and authorisation tools enabled by blockchain technology in this intelligent digital world. Consumers also benefit from blockchain applications from a business perspective, underscoring that blockchain technology is a game-changer. It is used in nearly all applications, including finance, banking, and land reform [183].

3.4 Changes brought by Blockchain-based cybersecurity in accounting

3.4.1 Blockchain technology & AI in Finance

[204] Financial technologies are being revolutionised through the advancement of artificial intelligence-based blockchain technology. In practical accounting environments, blockchain mechanisms can support several critical functions. For example, journal entries recorded on a distributed ledger cannot be modified retroactively without consensus, strengthening transaction integrity. Similarly, blockchain-based audit trails allow auditors to verify transaction histories in real time, reducing reliance on periodic reconciliation processes. These capabilities directly support financial reporting accuracy, fraud detection, and regulatory compliance. This new advancement enables the implementation of a standard protocol for the dynamic tracking of assets and agreements among the concerned parties, streamlining the process. It removes the old third-party verification system, including in-house-developed systems. Blockchain technology was initially created for a new kind of digital currency [205]. When artificial intelligence is integrated with the underlying concept of blockchain technology, it has the potential to make a very transparent and secure transaction system. Distributed Ledger Technology (DLT) and the smart contract are the two most essential introductions of advanced blockchain technology [204], as detailed below:

a. Distributed Ledger Technology

[204] A distributed ledger is a system for recording transactions between contracting parties, secured by cryptographic hashing. It gets recorded in a decentralised, replicated, shared and synchronised manner. In distributed databases, nodes verify data independently, not relying solely on other nodes. These nodes verify and independently recheck transactions in accordance with the prevailing legal rules and agreements before applying them. We split the distributed ledgers into two parts: one minimises the responsibilities of the trusted third parties, and the other relies on certain system properties [206]. [207] Integrating distributed ledger technology (DLT) into accounting practices is poised to redefine financial reporting by shifting the paradigm from an enterprise-centred approach to an exchange-centred framework. This transition has the potential to substantially enhance the quality, transparency, and credibility of financial reports, [208] pioneering the incorporation of a shared ledger design leveraging blockchain technology into accounting information systems. This innovation underscores the transformative capacity of blockchain to create more collaborative and reliable financial ecosystems, fostering trust among stakeholders and improving the integrity of economic data.

b. Smart contract

[207] The study defines smart contracts as "agreements" that, whether on-chain or off-chain, are executed, terminated, and enforced by a computer program. These agreements are modelled as computer programs that enable a network of mutually distrustful nodes to execute transactions reliably without relying on an external trusted authority [209]. To ensure the security of such systems, the study clarifies that any code responsible for locking and transferring assets must be meticulously implemented to prevent vulnerabilities, such as bugs or backdoors, that could be exploited for theft or tampering [210]. [204] The participating

parties must specify the rules for verifying and validating records and transactions in the distributed ledger. The distributed ledger technology maintains authoritative records that are consistent in terms of status and existence, including the evolution of legal agreements and protocols. Computer programs designed explicitly for transactions confirm, validate, and verify that these records adhere to the underlying legal protocols and agreements. We can say that these contracts summarise the details of these transactions, along with the legal clauses and protocols they follow during transfers to other nodes. It can also be used by the government and financial institutions to automate their laws and enhance transparency, reducing the movement of illicit black money within the financial market. [207] Moreover, smart contract technology enables rapid verification of transaction records against accounting standards or predefined business rules. Encoding the third accounting entry directly onto the blockchain establishes a transparent, encrypted, and self-verifying accounting information system. This system facilitates secure data sharing among business partners and enables continuous reporting to stakeholders. Additionally, smart contracts can manage "entries" related to the credit terms of payables, which are securely recorded on the blockchain [211].

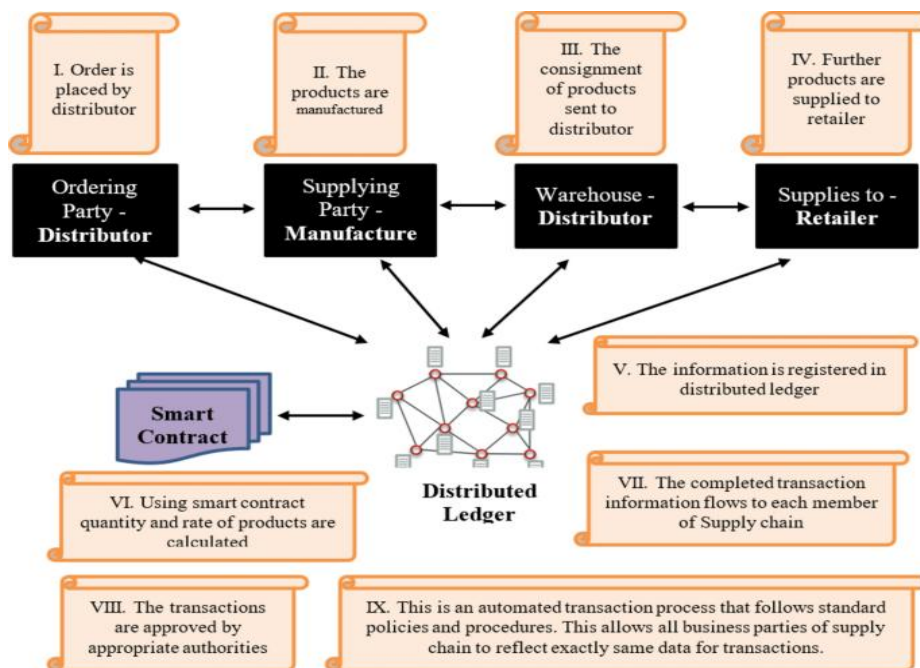


FIGURE 3.5 Transaction in the supply chain using blockchain

SOURCE [212]

Figure 3.5 shows the blockchain process using distributed ledger technology, including a smart contract for the supply chain [212]. Machine learning algorithms are still being developed and are very efficient and complex. If we test these algorithms, their outputs may raise legal, economic, social, or ethical issues. Financial and monetary institutions have previously implemented these algorithms, resulting in storage outputs that are not logical to even the developers, and this has led to either faults or flash crashes.

3.4.2 Blockchain as a cybersecurity framework

[34]The study describes Blockchain as a cybersecurity tool, an emerging technology that is highly reliable and powerful. We have a trusted intermediary responsible for ensuring secure business, addressing any issues that arise during the transaction, and covering security breaches. So, Blockchain, as a reliable, decentralised public ledger, has made this old, straightforward method obsolete by removing the intermediary between the two parties. [213] The study clarifies that Blockchain Technology not only removes the need for a third party and the concern of relying on one, which may involve other dangers or corruption through interaction with the third party, but also ensures the safety of their transactions.

3.4.3 Blockchain Relevance to Accounting Information Systems (AIS)

Blockchain directly strengthens core AIS functions by providing tamper-resistant ledger structures that prevent unauthorised alteration of journal entries, approvals, transactional histories, and reconciliation records. Immutable blocks and hash-linked chains allow auditors, compliance teams, and financial controllers to trace transactions with confidence, reducing the risk of falsified entries, timing fraud, and unauthorised adjustments. For functions such as asset management, tax reporting, procurement, inter-company settlements, and internal control monitoring, blockchain acts as a verification layer. This ensures accuracy and integrity across the financial reporting lifecycle, making it highly relevant to cybersecurity in modern AIS.

From a governance perspective, the adoption of blockchain within Accounting Information Systems (AIS) must align with established financial control frameworks, auditing standards, and regulatory compliance requirements. Accounting systems operate within strict governance environments that emphasise transparency, accountability, and the reliability of financial records. Blockchain-based ledgers can enhance governance by strengthening internal control accountability, improving audit evidence reliability, and ensuring tamper-resistant financial records. Immutable transaction logs provide a secure audit trail that enables auditors and regulators to verify the authenticity, completeness, and chronological integrity of financial transactions, thereby strengthening assurance processes in financial reporting environments [136, 200].

In addition, blockchain-enabled accounting infrastructure can support governance mechanisms for regulatory oversight and financial reporting compliance. Distributed ledger systems enable authorised stakeholders, such as auditors, regulators, and compliance officers, to access verifiable transaction histories in near real time, thereby improving the effectiveness of monitoring and control. These capabilities are consistent with modern governance expectations that emphasise reliable audit evidence, enhanced transparency, and strengthened internal control environments within digitally enabled accounting systems [141, 214]. Consequently, blockchain-based cybersecurity mechanisms contribute not only to technological resilience but also to broader governance objectives in accounting and finance systems.

3.4.4 Blockchain's use in financial accounting- an in-depth look

[34]Accounting is an industry that is being impacted daily by new technologies. Companies begin to have to adjust and adhere to these changes. [215] Blockchain is one of the leading technologies primed to change the accounting industry. Accountants and companies must work to implement this into their daily operations. Blockchain records and validates information in a decentralised manner, and the entire process does not require any intermediary authorities. The technology guarantees that the data is transparent, secure, tamper-proof, and reliable through distributed ledger technology, hash chaining, and the PoW mechanism. As a result, blockchain technology can significantly enhance the trust between market participants. [216] Allowing the Blockchain to be used in this function enables it to make its first crucial changes to accounting by making financial information more "transparent, secure, permanent, and immutable". It is exactly what users of company financial information need to perform their daily tasks and succeed in their jobs. As stated, accountants aim to ensure that their company's financial report is precise and error-free. Therefore, an independent third-party accounting firm audits the data produced and tracked by a company's internal accounting department. Blockchain technology checks off many goals that auditors and other accountants seek to have a successful year in their information and numbers. The reliability of this information is confirmed to an extent after the audit, but it can never be assured that it is impeccably correct, beyond error. Therefore, audits are assigned specific risk grades upon completion, along with an opinion from the independent auditor. Blockchain's process for companies' finance departments would enable companies pursuing these goals to gain public trust, with the aim of providing confirmed, accurate numbers without error or the risk of failure. Blockchain does not stop the recording or publication of financial data for the public. Anyone can become a different node, since the information is stored on the public blockchain. It includes auditors and lawyers, who could further explain the information provided, and other types of investors could conduct further research to make better investment decisions and develop more effective strategies using the Blockchain. Firms would post source documents for the statements and balance sheets, and the information would then be generated into those different statements and ledgers through smart contracts [216].

a. Blockchain and Big data in accounting

The study [217] explains the term "Big Data" and identifies how researchers offer various definitions for Big Data, recognising that both "Big" and "Data" are relative concepts. A dataset may be deemed "Big" when it pushes an information system to its maximum capacity or renders it unable to perform a specific task [218]. Additionally, interpretations of Big Data vary among users. The volume of data considered "Big" for a typical firm might be insignificant for a multinational corporation. Therefore, determining whether data qualify as Big Data depends on "whether these data push the limits of the capabilities of the information systems that process them" [218].

The primary concern with big data is that it is implemented across most of the enterprise's current business practices, which must be incorporated into the future of accounting [34]. Blockchain is becoming increasingly popular across many fields of business, enabling accurate data management and connecting big data to blockchain technology. Accountants can quickly and efficiently organise and review all the latest information available through big data. Big data affects accounting in many ways. It improves managerial and financial accounting factors, other financial reporting practices, and auditing.

b. Blockchain and auditing

[34] The study discussed an organisation's financial audit, which can be time-consuming, expensive, and laborious, and may require a manual review of the entire system, including paper documentation and legal techniques from external sources. Annual audits for companies or organisations are tedious, time-consuming, complex, and expensive. At the same time, manual reviews of the systems include getting external confirmations and obtaining paper documentation. Blockchain comes to the rescue by reducing reliance on manual tasks, including eliminating record duplication. Therefore, it would not be incorrect to say that integrating blockchain into the accounting system would enable auditors to conduct their audits professionally and develop effective audit methods for the system [97].

Although blockchain creates an impenetrable infrastructure, its impact is further enhanced when Artificial Intelligence is incorporated within it. The subsequent chapter discusses in detail how the use of Artificial Intelligence in conjunction with Blockchain-based cybersecurity solutions alters the way accounting is conducted and enhances its resistance to high-level cyberattacks.

3.4.5 Limitations of Blockchain-based Cybersecurity in Accounting Information Systems

Despite its significant potential to enhance cybersecurity in accounting information systems (AIS), blockchain technology is not without limitations. While the distributed ledger architecture strengthens data integrity and transparency, several technical, organisational, and regulatory challenges constrain its widespread adoption in financial and accounting environments.

The major limitation concerns scalability and transaction throughput. Blockchain networks, particularly those based on proof-of-work consensus mechanisms, often process transactions more slowly than traditional centralised databases. This limitation may restrict the ability of blockchain systems to handle the large volumes of financial transactions generated by modern enterprise accounting systems [56]. In large-scale financial systems, such as enterprise resource planning (ERP) systems and banking platforms, the latency associated with blockchain validation mechanisms can lead to operational inefficiencies.

Another important challenge concerns data confidentiality and privacy. While blockchain provides strong immutability and transparency, these same features may conflict with

confidentiality requirements in accounting and financial reporting. Sensitive financial information stored on distributed ledgers may become accessible to multiple nodes within the network, potentially increasing the risk of unauthorised disclosure. As a result, organisations must carefully design permissioned blockchain architectures and encryption mechanisms to ensure that confidential financial data remains protected [219].

A further limitation relates to integration with existing accounting systems and legacy infrastructure. Most organisations currently operate complex accounting information systems integrated with ERP platforms, financial reporting tools, and regulatory compliance frameworks. Integrating blockchain technology into these environments may require substantial system redesign, process reengineering, and significant investment in new infrastructure and expertise [100]. These implementation challenges may delay or discourage adoption in organisations that rely heavily on established accounting technologies.

In addition, governance and regulatory uncertainty present another major constraint. Accounting systems operate within strict regulatory environments governed by financial reporting standards, auditing frameworks, and data protection regulations. However, blockchain technology introduces decentralised governance structures that may conflict with traditional regulatory models. Questions remain regarding legal accountability, audit verification, and compliance with financial reporting regulations when transactions are recorded on distributed networks [200].

Finally, blockchain technology does not eliminate all cybersecurity risks. While it reduces the risk of transaction tampering, vulnerabilities may still arise from smart contract flaws, compromised endpoints, or insider threats. Cyber attackers may exploit weaknesses in application layers or user interfaces even if the underlying blockchain ledger remains secure [210]. Consequently, blockchain should be considered a complementary security mechanism rather than a complete replacement for traditional cybersecurity controls.

Overall, although blockchain offers significant benefits for enhancing data integrity, auditability, and transparency in accounting information systems, these limitations highlight the need for careful governance, regulatory alignment, and technological integration before its full potential can be realised in financial environments.

3.5 Research Methodology

3.5.1 Introduction

[220]Searching through the literature is a meaningful element of a systematic review. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) statement is the most commonly used component of literature searches [221].

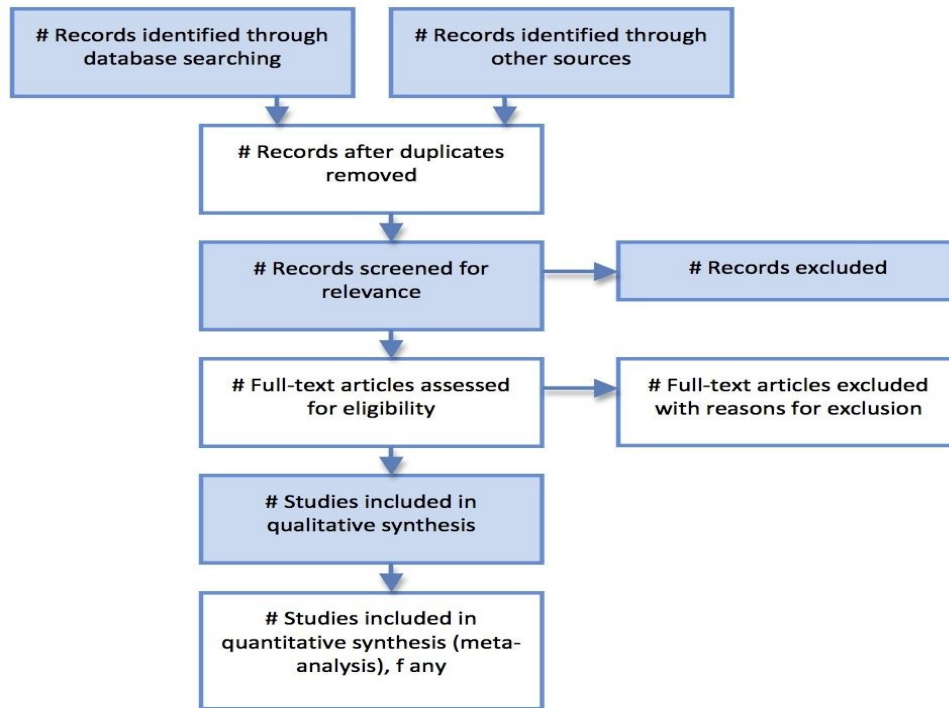


FIGURE 3.6 PRISMA Flow Diagram

SOURCE: [222]

SOURCE: FROM WIKIMEDIA COMMONS, THE FREE MEDIA REPOSITORY

This research project uses the PRISMA statement to filter out most articles. The PRISMA statement guides several steps, starting with understanding what needs to be done, what has been carried out, what has already been found, and what is planned next, which serves as the roadmap for the author [223]. A checklist tool is also available from the PRISMA statement, which can guide systematic review reporting [222]. It is illustrated in Figure 3.6 as a PRISMA flow chart.

3.5.2 Research Methodology

[224] As detailed in the study, this research follows the same approach, which is presented in the next section. Moreover, this is followed by a section that describes the research method adopted; the subsequent section recapitulates the systematic literature review and the social media analytics process.

To ensure methodological clarity and align this chapter with PRISMA expectations, it is important to highlight that Section 3.5.3 presents the formal, detailed systematic literature review (SLR) protocol adopted for the blockchain stream of this research. While the preceding subsections provide essential conceptual foundations and contextual justification for selecting blockchain as the first technological strand of the integrated BQMG-AIS framework, Section 3.5.3 outlines the complete methodological procedure used in this study. This includes the search strategy, databases consulted, keyword formulation, inclusion and exclusion criteria, multi-stage screening, quality appraisal, and thematic coding processes that underpin the rigour, transparency, and replicability of the blockchain SLR. Accordingly, Section 3.5.3

should be regarded as the methodological core of Chapter 3, providing the systematic foundation for the blockchain findings and subsequent cross-technology integration.

3.5.3 Research Methodology Adopted

To address the research questions of this article, the methodology suggested by the study [189] was used. The Author has combined both the systematic literature review and social media analytics; the same method was followed [225]. This research will follow the same process by applying the Systematic Literature Review and performing the research to explore the research questions. The primary reason for conducting an academic literature review is to facilitate the development of theory. Secondly, research areas emerge during this process; next, it helps identify research gaps. Lastly, it guides the tracking of technology from its inception and subsequently helps identify its practical and conceptual implementation [226]. The second method used in this literature is social media analytics, which we use for the following reasons. Firstly, it helps derive user-generated content about technology on social media. Technology frames the users towards technology. [227]. Another reason is that the social media platform features user-generated content that identifies famous technological players. The other one facilitates our acquisition of updated reports directly from the practice of new applications of emerging technologies for domains like technical AI or Blockchain-based cybersecurity. So, we use the systematic literature review (SLR) method for our research.

a. What is a Systematic Literature Review?

[228]A literature review has been defined in this article as a systematic way of accumulating and integrating previous research [229, 230]. Moreover, if the research method is effective and well-conducted, it provides a solid foundation for improving expertise and accelerating concept development [225]. [189] As the study pointed out, one of the primary purposes for choosing this method [19] is that SLR is a well-known method for establishing and assessing research output. It is appropriate for a specific topic or event of interest, aiming to support a stable evaluation of a study issue by retaining a precise, consistent, and auditable process. [19] The fundamental justifications for implementing this method of SLR are as follows:

- Consider technology, probe, and summarise the existing research paper.
- Identifying the gaps in the available study results leads to further research and investigation.

Suppose we say that a systematic review is a research method and process to identify and critically evaluate significant studies, including compilation and assessment of the gathered data of the performed research [231]. Figure 3.7 [224] gives specific steps for performing the systematic literature review, and Figure 3.8 [228] explains the four phases with general questions in detail. [228] Further, the article defined that a systematic review aims to resolve a specific research question or hypothesis by identifying the pragmatic evidence that fits pre-specified inclusion criteria. [232] This article defines SLR as evaluating and interpreting all available research relevant to a particular research question, hypothesis, or event of interest,

using a reliable, thorough, and auditable approach to produce a fair appraisal of a research topic [233].

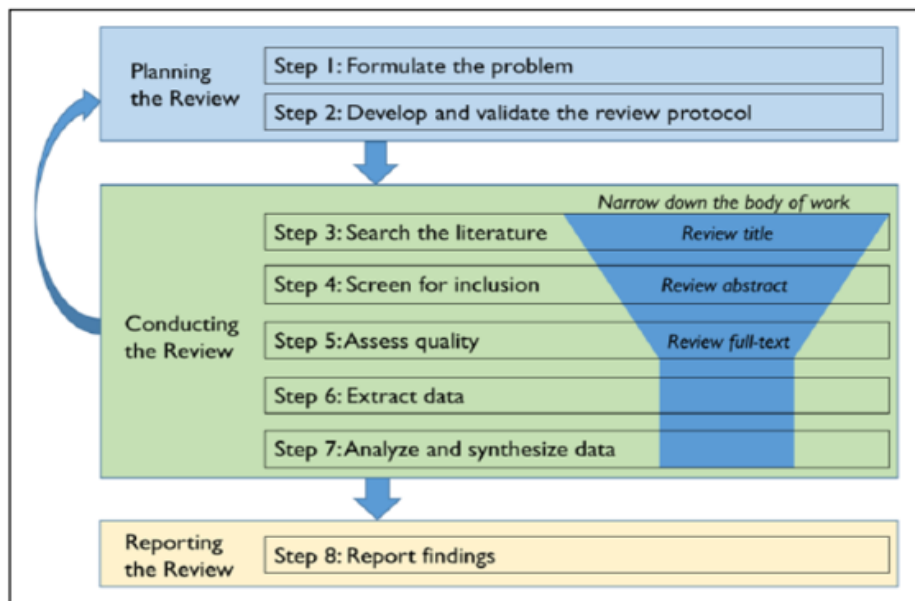


FIGURE 3.7 Process of Systematic Literature Review

SOURCE: [224]

b. Systematic Literature Review adopted

[135] The Literature Review approach was adopted for this study to conduct a comprehensive review of the existing literature and provide systematic significance to its findings. The researcher ensured that to strengthen the protocol, literature reviews on accounting should be considered as a base [234-237] and adhered to [238], providing crystal clear, comprehensive, and instructive information. Examining standards has informed our current research analysis steps, following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) standards [239], which helps researchers report improved systematic reviews [231, 240]. PRISMA delineates robust rules used in security research [241]. A relevant research literature selection has been made through systematic review methods, which are carefully designed and ultimately evaluated based on the emerging results from this research. The reason for trustworthy and effective procedures is that they are used to synthesise the insight [242]. It has already been identified that PRISMA is a protocol for reporting on systematic reviews. It consists of a flow diagram and a checklist, developed for the field of life sciences to increase their accuracy and transparency [243]. Among other existing protocols, PRISMA is selected for its depth, use across different fields worldwide, and its ability to maintain stability across reviews [239]. We have considered the standard guidelines explained by Kitchenham, as shown in Figure 3.8.

Important questions to consider in each step of the review.

Phase 1: design

- Is this review needed and what is the contribution of conducting this review?
- What is the potential audience of this review?
- What is the specific purpose and research question(s) this review will be addressing?
- What is an appropriate method to use of this review's specific purpose?
- What is the search strategy for this specific review? (including search terms, databases, inclusion and exclusion criteria etc.)

Phase 2: conduct

- Does the search plan developed in phase one work to produce an appropriate sample or does it need adjustment?
- What is the practical plan for selecting articles?
- How will the search process and selection be documented?
- How will the quality of the search process and selection be assessed?

Phase 3: analysis

- What type of information needs to be abstracted to fulfill the purpose of the specific review?
- What type of information is needed to conduct the specific analysis?
- How will reviewers be trained to ensure the quality of this process?
- How will this process be documented and reported?

Phase 4: structuring and writing the review

- Are the motivation and the need for this review clearly communicated?
 - What standards of reporting are appropriate for this specific review?
 - What information needs to be included in the review?
 - Is the level of information provided enough and appropriate to allow for transparency so readers can judge the quality of the review?
 - The results clearly presented and explained?
 - Is the contribution of the review clearly communicated?
-

FIGURE 3.8 Systematic Literature Review Approach

SOURCE: [228]

c. Systematic Literature Review Process

[233] A systematic literature review involves several discrete activities, as outlined in the guidelines. [233] Further, the study explains that the medical and sociological textbooks agree on significant process stages and summarise the systematic review into three main phases. The current project is considering these three steps and has been detailed as shown in Figure 3.9.

The summary of the Methodology:

The first is the Planning Review or Designing the Plan.

The next step is defining the research question, and

The last step is to search for the literature, as explained below [135] .

i.Design the plan

Following the protocol of [244], which involves the following steps:

- _ The first step is to define our research question.
- _ The next one is to design a plan.
- _ Third is to search for the literature.
- _ The fourth one is to apply exclusion and inclusion criteria.
- _ Fifth is to perform or conduct a quality assessment, and
- _ the sixth and last step of the planning stage is to discuss the results.

ii.Define the research question and proposition.

The primary step of the systematic literature review is the process led by the

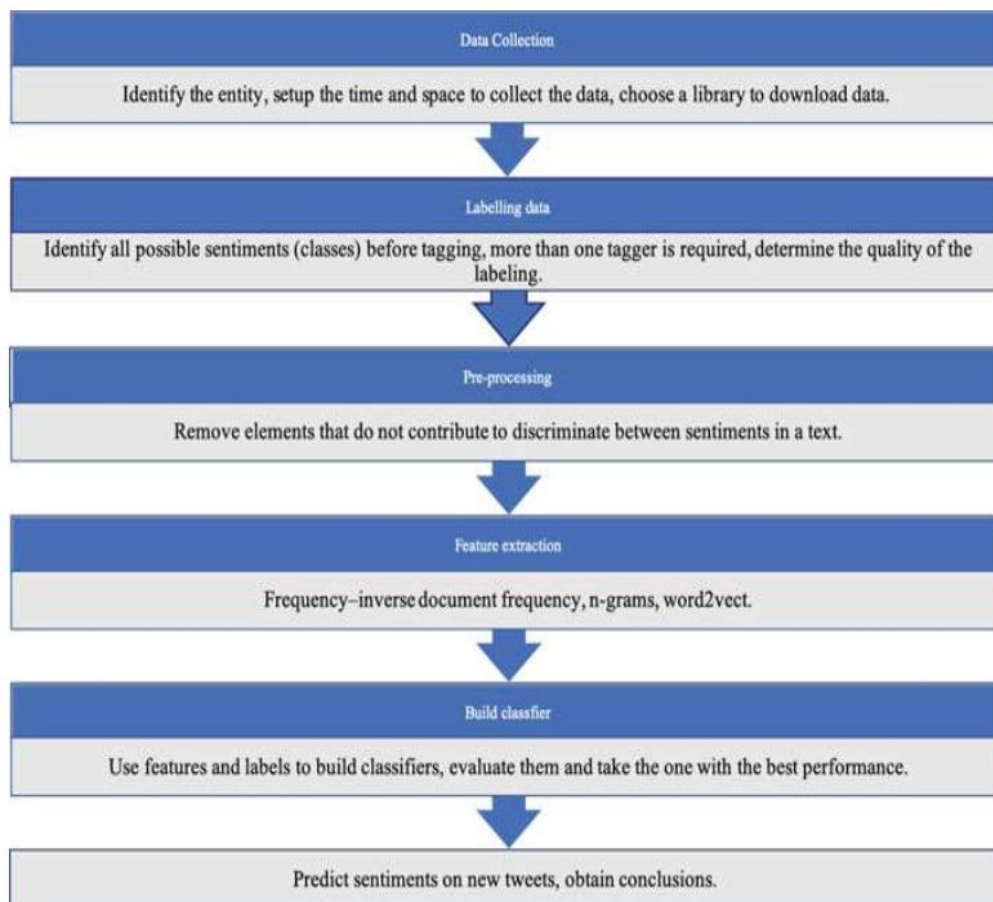


FIGURE 3.9 Summary of Methodology

SOURCE: [245]

research question defining the research subject, the scope and the object [246]. Accordingly, we identified the following research question:

What factors influence BC-based cybersecurity technology's quicker and faster adoption in an organisation's accounting and finance department?

Furthermore, based on this research question, we are responding to the following propositions:

- **Propositions**

Proposition 1: The use of blockchain technology as a distributed ledger enhances the quality of the entire accounting system's processes.

Proposition 2: The report generated through Blockchain Technology is trusted and valuable by the Management of the Enterprise.

Proposition 3: Automating the Blockchain-based cybersecurity system and its execution on an enterprise resource planning system (ERP system). It enables innovation by identifying organisations' core capabilities in real time for their accounting and finance departments. It also includes a discussion of the challenges that need to be addressed.

Proposition 4: Machine learning algorithms and blockchain enable accountants and auditors to produce real-time, trusted, audited, and certified reports.

Proposition 5: The management of AI algorithms for the real-time downstream supply chain process increases the probability of reaching customers and facilitates gathering their needs.

iii. Search for the literature.

[135] Scopus has been considered our primary source for selecting articles and gathering data, ensuring both scientific rigour and inclusivity. Initially, the keywords identified and chosen for our topic were Blockchain, Blockchain Technology, cybersecurity, and Accounting. We selected the article as the source for conducting our research and excluded conference papers or book chapters. We included only those papers in the categories “business, management and accounting, computer science, economics, econometrics and finance, engineering and mathematics.” The time range was also given, covering the period from 2014 to the present. Moreover, only articles written in English were considered, and those in other languages were excluded to ensure clear understanding and improve consistency across the international community. The research string for searching the article on Scopus is as follows:

(TITLE-ABS-KEY (blockchain) OR TITLE-ABS-KEY (cybersecurity) AND TITLE-ABS-KEY (accounting) OR TITLE-ABS-KEY (blockchain AND technology)) AND (LIMIT-TO (PUBYEAR , 2023) OR LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018) OR LIMIT-TO (PUBYEAR , 2017) OR LIMIT-TO (PUBYEAR , 2016) OR LIMIT-TO (PUBYEAR , 2015) OR LIMIT-TO (PUBYEAR , 2014)) AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (SRCTYPE , "j")) AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "ENGI") OR LIMIT-TO (SUBJAREA , "BUSI") OR LIMIT-TO (SUBJAREA , "MATH") OR LIMIT-TO (SUBJAREA , "ECON")) AND (LIMIT-TO (LANGUAGE , "English")).

❖ Application of the criteria of inclusion and exclusion

This research considered the guide [246] to determine which articles to exclude based on their relevance. We have analysed the titles and keywords manually. Figure 3.10 shows the PRISMA flow diagram.

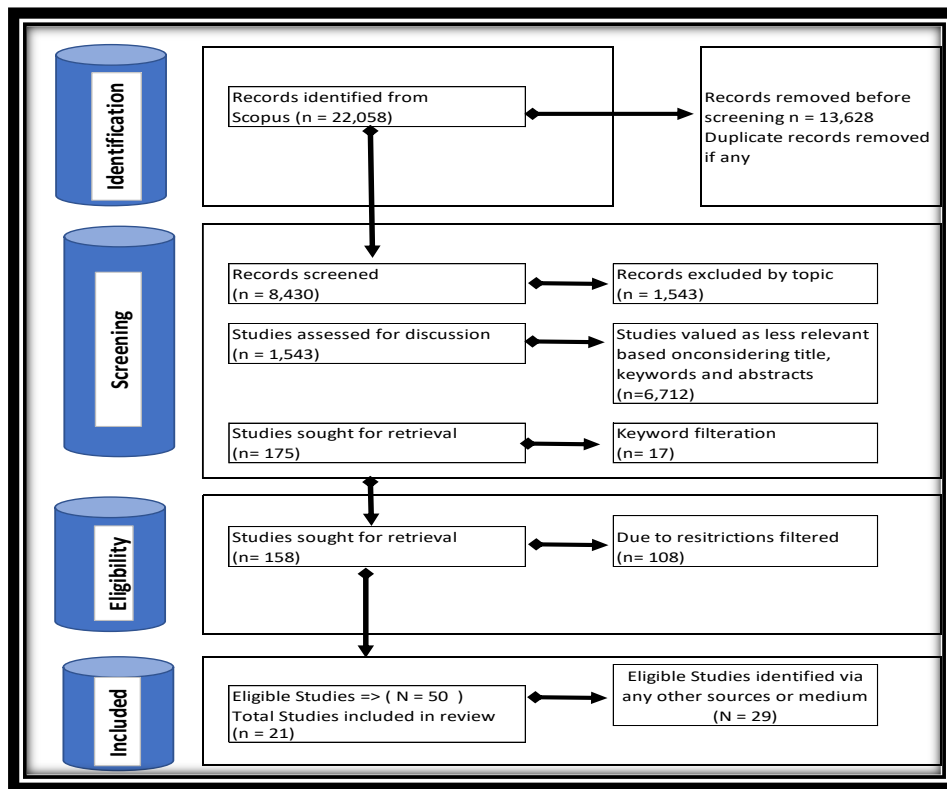


FIGURE 3.10 PRISMA Flow Diagram

❖ Stages for the Selection of the Articles for the Literature Review

▪ Stage 1

The keywords searched in the SCOPUS database are "Cybersecurity," "Blockchain," "Blockchain Technology," and "Accounting."

Selected N = 22,058

▪ Stage 2

The article results had been limited to source type - **Journal Only** & document type - **Article only**.

Selected N = 8,430

▪ Stage 3

The document, published in 2015 and later, was considered for review.

Selected N = 8,430

▪ Stage 4

Only articles published on the subject related to Business, management and accounting and Computer Science, Engineering, Mathematics, Economics and Finance in the English Language

Selected N = 6,887

▪ Stage 5

Inclusion/exclusion criteria- Abstract & Title filtered for Blockchain or cybersecurity, and accounting was applied to the article title and abstract.

Selected N = 158

❖ **Quality assessment:** This research has considered papers published in journals with moderate to low impact factors. We opted not to exclude papers published in journals with moderate-to-low impact factors. Only Articles and journals have been considered for this research since blockchain is a pervasive topic.

d. Bibliometric mapping/visualisation

Figure 3.11 visualises our co-occurrence analysis. The figure shows the relatedness of entries based on the number of documents in which keywords co-occur in a co-occurrence analysis. The keywords were grouped into clusters, or sets of closely related nodes, within a bibliometric network. VOS viewer uses colours to show the cluster assigned to each node with a co-occurrence relationship. The weight of a node is based on the number of occurrences of the corresponding keyword. The weight of a node is based on the number of occurrences of the corresponding keyword. So, VOSviewer has been used to create this form of bibliometric network visualisation; the VOSviewer clustering technique is discussed by [247].

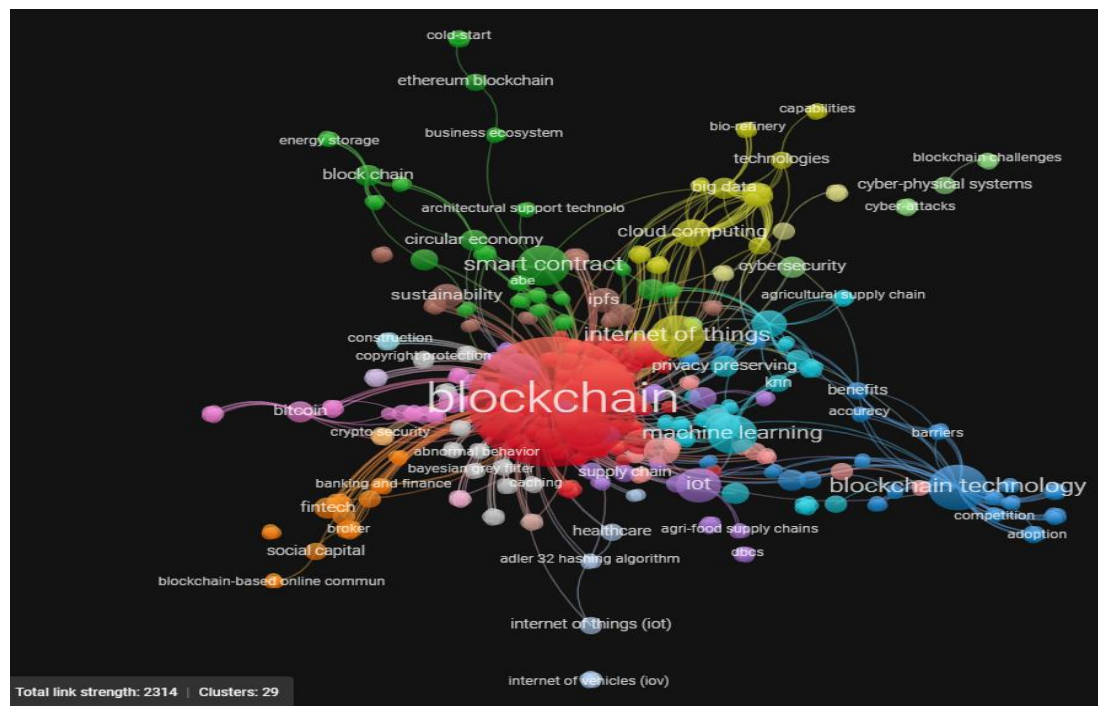


FIGURE 3.11 Co-occurrence analysis of the Author's keyword

3.6 Findings & Discussions

3.6.1 Findings

a. Job-fit

Our proposition no. 1 mentions that the DLT Industry 4.0 application is helping the accounting system to integrate and create transparency and trustworthiness. It builds confidence in the customers. Additionally, employees are confident that they receive a proper and authenticated output, which helps them achieve the organisation's primary objective.

Management is getting reports in real-time, helping them make quality strategic decisions for their company. The second proposition is also being addressed under the umbrella of job fit. The stakeholders need to get a report on time, which is trustworthy. [34] His article explained the blockchain, which is used to record transactions. Not only this, but it also verifies the transaction without a trusted third party, relying on an entirely automated system, thereby eliminating errors caused by intermediary involvement. Removing intermediaries reduced their role and the cost of paying commissions and other secondary transactions involved in this process. The revolution enabled by this new technology makes the output transparent, with transactions visible to everyone and verified by thousands of computers [248]. According to the research, blockchain technology directly improves the performance and confidence of accounting professionals, primarily through Distributed Ledger Technology (DLT) in Industry 4.0. According to Proposition 1, blockchain technology enhances accounting procedures by ensuring transaction traceability and transparency. This is also related to Proposition 2, which states that because blockchain-generated reports are automated and unchangeable, they are intrinsically more reliable.

The extent to which these technologies help professionals achieve their work goals is reflected in the Job-Fit factor. Blockchain speeds up reporting, eliminates middleman validation, and reduces redundancy. Real-time access to reliable records helps management, which enhances planning, compliance, and financial control. Eliminating human intervention in data validation reduces fraud and errors, meeting both strategic and operational requirements.

b. Complexities

Our current research proposition, which involves generating real-time reports, is valuable and trustworthy for decision-making, as illustrated in the scenario below. [54] The author says we can imagine [249] and [250] saying. According to them, the immutability of the information helps multiple stakeholders, such as banks, courts, tax institutions, regulators, accountants, and auditors, verify the consistency of the records, and enables management to make informed corporate decisions. Furthermore, the author notes that this helps track and verify the agent's actions at a particular time. As in the Proof of Existence system, an action operation is traceable, which requires less system complexity. Using this technical method, the risk of employee/agent misbehaviour has been significantly reduced. The agent's responsibility is augmented by the blockchain's ability to enable instant verification of each computable transaction, thereby reducing agency costs. This section covers propositions 2 and 4, discussing the roles of accountants and auditors. Over the years, the accounting profession has evolved in response to environmental changes and undergone several transformations. Accounting practices have undergone significant changes in recent years, driven by the advent of new technologies. Blockchain technology in accounting creates a collaborative digital ecosystem with increased capabilities and features. It extends beyond traditional ledgers [251], which means that real-time accounting has a positive impact on the application of blockchain

technologies [252]. Regarding the value chain, many businesses and competitors are highly interdependent, as they rely on one another. Considering this, businesses are also motivated to improve the operational dependency of these organisations and companies. The most important ones are safe and sound financing and accounting, transparency in processes, minimal risk and resilience against external threats, deepened accountability, and, most of all, efficiency. Market analysts predict a significant rise in the use of blockchain accounting over the next five years; 2016 was a record year, with approximately \$ 1 billion in transactions. Financial service firms and technology-driven organisations are contributing to the exponential growth of blockchain technologies [253]. This growth is primarily due to blockchain technology's ability to provide real-time and reliable updates in decentralised public ledgers. It allows companies to consult the entire history of transactions in the ledger. It hence yields relevant, timely, reliable, and trustworthy updates that minimize human errors when recording complex information from several sources [254-256].

This theme explores how individuals and organisations perceive the impact of utilising blockchain for cybersecurity. Proposition 3 says that automating blockchain security in enterprise resource planning (ERP) systems opens new possibilities. However, this promise is tempered by real-world worries.

The study finds three main problems: (i) Selfish Mining, which breaks consensus protocols; (ii) Scalability, where growing data needs make blockchains hard to use; and (iii) Privacy Leakage, where bad key management puts privacy at risk. Despite these concerns, people still firmly believe that security, operational efficiency, and fraud prevention will all improve. These effects encourage companies to invest in integration, despite the associated technical risks.

c. Perceived Consequences

This section addresses the consequences and challenges of blockchain-based cybersecurity. Under this section, we are covering proposition number three. [257] The article explained the various obstacles encountered due to the enormous potential of blockchain, which, in turn, constrained its path forward. Some of the challenges and contemporary advancements, as detailed by the study, are as follows:

i. Selfish Mining

It is susceptible to attacks from the conspiracy of selfish miners. Only a tiny percentage of the hash power is used for deception, making the whole pattern unprotected and vulnerable. Furthermore, the strategy adopted for this selfish mining considers that the selfish miner never broadcasts or makes public their mining blocks. If we believe the private block, it is notified to the public only when certain conditions are satisfied.

ii. Scalability

Due to the daily growth of its transactions, the blockchain is becoming increasingly significant. It is growing in size bit by bit as the importance of the transaction increases. Furthermore, the

legalisation clause requires every blockchain transaction and proceeding to be connected and accumulated for proper legalisation, so that it can be confirmed through inspection that the root proceedings have been properly depleted. Each junction must accumulate every proceeding to be legal on the blockchain, as they must inspect whether the current source of the proceeding has been adequately exhausted.

iii. Privacy Leakage

Blockchain technology can provide a specific level of confidentiality through the use of public and private keys. End users negotiate based on their public and private keys, confident that there is no substantial identity threat, and thus rely on confidentiality [195]. Blockchain Technology has been a topic of much research. Several applications have also been developed across different fields, building confidence in the robustness of the applied science of blockchain. More analysis is required for large-scale businesses to make blockchain more flexible, including scalability and data-rich research consensus [258]. [259] illustrated that deep learning could be used for visual audit recognition. According to him, deep understanding helps with information detection and supports audit judgment [259]. Therefore, based on the readings, the authors propose a positive relationship between the use of AI for product inspection and the deployment of quality functions.

d. Affect towards Use

We cover proposition no. 2, which states that the report generated in a Blockchain-based environment is trustworthy. [260] The article pointed out that financial statements based on the company's accounting data and on a private blockchain would affect the overall reliability of the accounting data. Since these blocks have digitised current validation processes, holding accounting transactions improves the overall reliability of accounting data. Even though this would mean the accountant is no longer the owner of the enterprise accounting database, they would be involved in the digitised processes and in defining the policies, including validating the entire procedure. They consider financial statements that contain subjective values and balances. These would require exercising the analysis process and are subject to judgment, which blockchain accounting databases cannot yet cover. The dimension examines how people feel and act when using blockchain systems. When people use systems that are clear and can be checked, they report feeling confident, satisfied, and trusting. Proposition 2 states that financial statements supported by private blockchain frameworks are perceived as more trustworthy, even if accountants give up some control over who owns the database.

However, there are emotional issues with subjectivity in data interpretation and the need for professional judgement, which current blockchain systems cannot automate. The accountant's job shifts from handling data to verifying the accuracy of records that have been digitally confirmed.

e. Relationship

Our proposition no. 5 requires AI algorithm management to deliver real-time outputs, increasing the likelihood of reaching out to their customers and meeting their requirements. To address this, we consider the game-theoretic approach used in a blockchain-based environment to address security issues.

They are considering the article by [192], where the authors [261] propose a cyber-insurance scheme [262] to cover the blockchain participants for their losses. Blockchain involves several participants who must choose a provider's service to maximise the utility. It means the involvement of a blockchain provider, and the other is the cyber-insurer. Based on the users' demand, the provider's problem is investing in computing resources to increase its profit. The provider investing heavily in computing resources would want to increase its profit. The blockchain provider purchases the cyber-insurance-related resources to mitigate their losses from cyberattacks. Securing the blockchain accounting system, the users choose the services that the provider and the insurer offer. Cyber insurers set the insurance price depending on the provider's risk level that cyber insurers perceive as acceptable to the provider. The utility here is to obtain equilibrium. In practice, the cyber insurer cannot sense the level of risk accepted by the provider, leading to the adoption of the Bayesian game.

Summarising the strategy and the rationality being considered: Maximising the payoffs means the player is rational and self-interested. Strategy is a set of actions, decisions, or choices the player takes to achieve the desired outcome. It is not wrong to say that the strategies of the leading and other players are based on the utility being considered.

This theme utilises game theory to discuss how individuals in a blockchain network rely on one another. Proposition 5 demonstrates how AI-managed algorithms integrate with blockchain systems to facilitate customer engagement and streamline business processes. Strategically, blockchain service providers, cyber insurers, and end users build relationships with one another.

In this case, participants act as rational agents who strive to maximise their returns by negotiating prices, sharing risks, and setting service levels.

f. Cybersecurity Culture

Proposition No. 3 will be addressed in this section of Cybersecurity Culture. [193] Sanctions are the standard method to deter deviant employee behaviour in information security. The fourth provision suggested that combining machine learning and blockchain in auditing requires a cultural shift towards valuing technological innovation and data-driven decision-making[33]. Moreover, organisations impose sanctions to control community fraud and discourage employees. Proposition No. 5 considers [263] that integrating AI in supply chain management requires a cultural shift towards embracing technological innovation and customer-centric strategies. The Sanctions may include a clause for termination from employment or financial penalties. Although creating a strong cybersecurity culture has many advantages, it is not simple. The author went on to detail the five crucial steps that three

Australian businesses have taken to enhance their own cybersecurity cultures. The five main objectives are to identify critical cybersecurity behaviours, create a network of "cybersecurity champions," develop a brand for the cybersecurity team, establish a cybersecurity hub, and coordinate security awareness campaigns with both internal and external initiatives.

An organisation's culture has a significant impact on the adoption process. Proposition 3 makes it clear that blockchain cannot be added to business systems; it also needs to be culturally ready. Proposition 5 adds to this by showing that AI in supply chain processes requires innovation that focuses on the user and a risk-aware mindset.

Companies that are very aware of cybersecurity have punishments, internal champions, and campaigns to raise awareness. This cultural alignment makes sure that employees accept digital change responsibly. It lowers the risk of insider threats and increases the chances of a successful implementation.

3.6.2 Adoption of AI & Blockchain-based Cybersecurity Impacting the Role of Accountant & Auditor

[34] In an Audit, an organisation's accounts are reviewed by external auditors on behalf of investors to provide reasonable assurance of their accuracy, genuineness, and compliance with the relevant accounting regulations. Financial Audits are time-consuming, costly, and laborious, often requiring manual review of systems, the collection of paper documentation, and confirmation with external organisations. Blockchain technology can eliminate the need for repetitive tasks and duplicate recording. If Blockchain were to be utilised as a platform for accounting, it would need to be audited, and professionals would need to devise methods to audit the system. In the paper "Designing and Auditing Accounting Systems Based on Blockchain and Distributed Ledger Principles", Appelbaum and Nehmer outline a process for auditing a Distributed Ledger Technology (DLT). When analysing transactions in a blockchain system, auditors face concerns about the reliability, security, and transparency of the data. "Data reliability refers to the performance principle requirement to obtain sufficient appropriate audit evidence of material misstatements by developing and performing reasonable audit tasks." [97]. Evidence to be called "reliable" can be understood and relied upon by the auditor. External parties typically obtain and verify highly reliable evidence by using invoices, confirmations, and analyst reports, to the extent that the company's blockchain information serves as an external source. Auditors would require proof of effective governance of the peer network and the blockchain, and then confirm the blockchain evidence as being reliable. It resulted in all blockchain evidence being considered reliable and valuable to the company's audit. Data security ensures that the information is protected from fraud and has been cleansed from erroneous manipulations. Third, the use of a blockchain during the design of a transactional processing system makes the information more transparent, as it provides a trail of the sequence of blocks and indicates how each block arrived at its value in the "hashing system" [97] described in the core components.

[264] In its article, Deloitte claimed to have successfully performed a blockchain audit by applying existing auditing standards, policies, and procedures to permissioned blockchain applications [265]. KPMG has also claimed to leverage blockchain capabilities for faster, more secure transactions, enabling cost reduction through back-office operations automation. KPMG and Microsoft jointly developed digital ledger services. The author explained that the current focus is on creating prototypes for the financial services industry, the public sector, and healthcare to effectively address the challenges of implementing blockchain [266]. Ernst & Yong, among the top four firms, began getting involved and focused on developing and implementing Libra, a distributed ledger and another blockchain-based project [267].

According to [268], when we require a common database, which is a shared one, then Blockchain can be a solution. In the BC system, various parties participate, but the parties involved have conflicting enticements. They are not trustworthy; the rules between contributors are consistent; there is a need for a purpose and a non-challengeable log; and the operational rules do not generally change.

[269] His article mentions that the accounting field can be revolutionised through blockchain technology. Moreover, the primary component can link the external transaction system with the enterprise's internal information system. The key is that an enterprise's internal information system can be connected to its external transaction system. However, blockchain technology's fundamental components, which include encryption, time-stamping technology, and decentralisation, can help restrain traditional accounting fraud from happening. The conventional accounting standard model is undermined by Blockchain's distributed accounting method.

Furthermore, companies that rely on riskier relationships between competitors and the industrial value chain are motivated to improve their business dependence. It considers having a safe and secure accounting and financing ecosystem, reduced risk, and a highly transparent process to diagnose and protect itself from external threats. The decentralised public ledger provides real-time and reliable functions with updates through blockchain technology. The history of transactions can be traced and acquired from the register and multiple sources. Companies can also query the register for all transactions at any time and quickly manage detailed information from various sources.

3.7 Contribution to Knowledge

This study uses a conceptual framework that integrates blockchain and artificial intelligence to make several new contributions to the body of knowledge on cybersecurity adoption in accounting and finance:

3.7.1 Adoption of the Model

a. Adoption Model with Multiple Dimensions

It improves on existing technology adoption models by bridging technological (Job-fit, Complexity), psychological (Affect Towards Use), economic (Perceived Consequences,

Relationship), and cultural (Cybersecurity Culture) dimensions. It provides a customised, enhanced lens that is better suited to accounting environments.

b. Blockchain Adoption Behaviour Anchoring

This framework fills a significant gap by bringing human-centric considerations into a conversation dominated by technology and anchoring blockchain adoption in the behavioural reactions of accountants, auditors, and organisational actors.

c. Game-Theoretic Blockchain Governance

A new paradigm for understanding distributed accountability and incentives in blockchain networks is introduced by game theory and cyber-insurance dynamics.

d. Industry 4.0 Contextualisation

An expanded conceptual scope is provided by situating blockchain within the larger framework of industry transformation, AI integration, and ERP systems.

Every element of the framework generates workable solutions that can direct the creation of policies and their implementation.

3.7.2 Job-Fit

This requires aligning blockchain with accounting functions. The problem requiring attention here is that organisations face resistance when employees perceive blockchain as unrelated to their work goals. The solution to this concern is to design role-specific blockchain dashboards that cater to distinct user types (e.g., auditors, accountants, managers). Also, automate KPI-aligned reporting processes for finance and audit departments. Train employees, particularly in real-time ledger navigation and verification, to enhance their decision-making capabilities. If we consider the impact of this setup, it will improve usability and motivate adoption by showing direct productivity gains.

3.7.3 Complexity

It means reducing barriers to understanding and use. The problem to address concerns blockchain systems, which are perceived as challenging to learn, thereby deterring their adoption. One effective solution for this concern is the deployment of blockchain-as-a-Service (BaaS) platforms with user-friendly interfaces. Also implemented phased training modules for employees and audit teams to grasp consensus mechanisms, cryptographic logs, and smart contracts. The impact is increased confidence, lower onboarding time, and a reduced risk of implementation failure.

3.7.4 Perceived Consequences

It requires clarification of the benefits and risks. The problem to be addressed is the perceived threats, such as selfish mining, data leakage, and scalability issues, that erode trust. Therefore, the solution to this is to use permissioned blockchain architectures for internal ledgers to minimise attack surfaces. Additionally, integrating AI-based anomaly detection can help mitigate insider threats and fraudulent inputs. Furthermore, to establish hybrid chain protocols

where sensitive information is stored on private chains and audit trails are maintained on public chains. It increases in perceived value while managing complexity and legal risk.

3.7.5 Affect Toward Use

It requires Enhancing Emotional Trust and Familiarity. The problem to be considered and addressed is that users hesitate when blockchain replaces subjective accounting judgments. The response to the problem identified is to keep accountants involved in validation layers to ensure judgments still apply where automation cannot. Utilise co-creation sessions where end-users help shape implementation strategies and provide feedback loops. Share case studies that demonstrate how blockchain has improved reporting accuracy, particularly in high-risk environments prone to fraud. The impact that can be seen is related to building emotional commitment, trust, and ownership of the system.

3.7.6 Relationship

Structuring Stakeholder Incentives Using Game Theory: The concern is the unclear incentives among providers, users, and insurers in a blockchain ecosystem. The response to these concerns is the introduction of cyber-insurance mechanisms with smart contracts that adjust premiums based on compliance behaviour. Utilise Bayesian game models to simulate insurer-provider-client dynamics prior to launching full-scale networks. Define SLA-backed guarantees (Service Level Agreements) between data providers and auditors. Therefore, the impact is the alignment of economic incentives, which improves governance and facilitates network accountability.

3.7.7 Cybersecurity Culture

Cultivating a Pro-Innovation Organisational Mindset: The problem to address is that even technically sound systems fail without supportive behaviour and policies. The solution to the above issue is to launch internal cybersecurity champion programs and select trusted staff to lead awareness. Tie cybersecurity behaviour to performance evaluations or reward systems. Align security policy branding with core company values, reinforcing awareness campaigns with visual and verbal consistency.

Impact: Builds a self-reinforcing culture that values digital security and innovation.

3.7.8 Policy Implications

a. Regulatory Frameworks: Governments should create blockchain audit certification frameworks that integrate AI-driven risk analysis for accounting firms.

b. Industry Standards: Industry bodies (e.g., IFAC, ICAEW) should collaborate to develop templates for blockchain ledger design, cybersecurity assessment, and ethical AI auditing practices.

c. Education Curricula: Accounting education should now include modules on cryptographic accounting, decentralised auditing, and AI-based controls.

This conceptual framework offers a dual-lens view, strategic and behavioural, of how to achieve secure digital transformation in accounting. The multi-propositional structure bridges

theory and actionable insights, encouraging organisations to adopt a holistic, human-centric approach to blockchain-based cybersecurity.

3.8 Integration of Blockchain Into the BQMG-AIS Framework

Within the BQMG-AIS integrated cybersecurity framework, blockchain forms the Integrity Layer. It provides permanent, verifiable, and tamper-proof transaction records that serve as the backbone of secure accounting processes.

- Machine Learning (Chapter 7) generates fraud alerts.
- Game Theory (Chapter 6) models optimal defensive strategies.
- Quantum Computing (Chapter 5) secures communication and encryption.
- Blockchain ensures all actions and transactions are permanently recorded for auditability.

Together, these layers produce a coherent cybersecurity architecture capable of addressing both technological and behavioural threats to accounting systems.

Despite the significant cybersecurity advantages offered by blockchain technology, several risks and limitations remain unresolved. One major concern is vulnerabilities in smart contracts, which may contain coding errors or exploitable logic flaws that could compromise financial transactions or automated accounting processes [210]. Additionally, governance coordination across distributed networks presents challenges, as blockchain systems often involve multiple stakeholders with differing incentives, responsibilities, and regulatory obligations, complicating decision-making and accountability structures [200]. Scalability also remains a key limitation, particularly for accounting and financial systems that process high transaction volumes, where consensus mechanisms may introduce delays and increased computational costs [56]. Furthermore, the transparency of blockchain ledgers, while beneficial for auditability, may expose sensitive financial information if appropriate privacy-preserving mechanisms are not implemented [136]. These unresolved risks highlight the need for continued research and governance frameworks to ensure that blockchain-based cybersecurity solutions can be effectively integrated into accounting information systems.

These limitations indicate that blockchain should not be viewed as a standalone cybersecurity solution for accounting environments. Instead, it functions most effectively as a foundational infrastructure that must be complemented by additional technologies capable of addressing threat detection, encryption resilience, and behavioural risk management within accounting information systems.

3.9 Conclusion

Based on the findings, we can conclude that, as mentioned in the article [146], Blockchain technology enhances the quality of the accounting process by providing a decentralised, immutable ledger that ensures data integrity and reduces the need for intermediaries. This technology enables real-time transaction recording and verification, streamlining the audit

process and enhancing its reliability. For example, as reported in the literature [263], smart contracts on platforms such as Ethereum have been shown to improve information-sharing efficiency by 25.7% and data accuracy by 19.8% in financial accounting. The study [33] noted that reports generated using blockchain technology are trusted and valuable to enterprise management due to their transparency and security. The research further clarifies that blockchain's decentralised structure and cryptographic security provide a tamper-resistant and transparent ledger system, which is especially beneficial for auditing and compliance. The article suggested [146] that it enhances the trustworthiness of financial reports, as all transactions are recorded on a public or private ledger accessible to legally authorised parties. The study [270] points out that integrating blockchain-based cybersecurity systems with ERP systems enables innovation by enabling organisations to identify their core capabilities in real time. Further, she discusses how this integration facilitates the automation of financial processes and enhances data security, thereby improving operational efficiency. However, challenges such as regulatory compliance, security threats, and 51% attacks must be addressed to ensure the successful implementation of blockchain in ERP systems [146]. The study [33] highlights that combining Blockchain technology and machine learning algorithms enables accountants and auditors to produce real-time, trusted, and certified reports. The article highlights that cyber threats are identified and addressed in real time through AI and ML, enhancing accounting firms' capacity to safeguard financial data. This proactive approach to cybersecurity is essential in the face of growing cyber threats and the complexity of financial data breaches [33]. The article [271] provides an example of managing AI algorithms for real-time downstream supply chain processes, thereby increasing the likelihood of reaching customers and facilitating the gathering of customer needs. Blockchain technology can create a decentralised network for sharing cyber threat intelligence, which enhances collaboration and response to new threats [272]. This integration of AI and blockchain improves the supply chain management operation efficiency, and it also enhances customer satisfaction by ensuring timely delivery and accurate tracking of goods [271].

[273] The study argued that despite Blockchain technology becoming very popular in the new generation, limited studies have also predicted that BCT harm the Accounting and Auditing Profession, justifying that this brings chaos to the whole industry [200, 274, 275]. Reconciliation automation is another challenge that causes turmoil and creates risk in the accounting and auditing profession [276, 277]. [273] Another concern, as highlighted by the author, is that the Accounting Information System, which is based on Blockchain Technology, prepares the financial reports. However, this does not guarantee that the report is accurate or has been presented fairly. This requires frequent verification of the AIS and its processes, and it must also be reviewed through the application of professional judgment [153]. We would require skilled accountants and experienced auditors to respond to the new generation changes in the prevailing accounting and auditing system [278, 279]. Therefore, it would not be

incorrect to say that we need to re-engineer the roles of accountants and auditors to adapt to the new era of blockchain technology systems.

This chapter examined blockchain technology as a cybersecurity mechanism for accounting information systems, focusing on its potential to enhance the integrity, transparency, and security of financial data within modern digital accounting environments. The analysis demonstrates that blockchain can strengthen transaction integrity, enhance audit transparency, and support secure financial data management through immutable ledger structures and distributed verification mechanisms, thereby reducing the risk of unauthorised alteration of accounting records [136]. By enabling tamper-resistant audit trails and decentralised validation processes, blockchain technology has the potential to improve trust and accountability in financial reporting systems and strengthen assurance processes within accounting information systems [200].

However, the findings also highlight governance, scalability, and integration challenges that must be addressed before widespread adoption can occur. These challenges include coordination among multiple stakeholders in distributed networks, technical limitations in transaction processing capacity, and difficulties in integrating blockchain architectures with existing enterprise accounting infrastructures [56, 214].

These insights provide the foundation for the subsequent chapters, which examine complementary technologies such as artificial intelligence, quantum security, and machine learning within the integrated BQMG-AIS cybersecurity framework, which seeks to provide a multi-layered approach for strengthening cybersecurity resilience in accounting and financial information systems.

3.10 Future Research

Further research is required to conduct an empirical study of Blockchain Technology in cybersecurity for accounting adoption to understand the real-time implications the enterprise is facing. The combination of Blockchain with Artificial Intelligence is an unparalleled development in cybersecurity.

The blockchain-based mechanisms outlined in this chapter establish the foundation of trust and immutable data integrity in accounting systems. However, ensuring cybersecurity in modern accounting also requires intelligent, adaptive detection capabilities that go beyond record immutability. The next chapter, therefore, explores how Artificial Intelligence and Machine Learning enhance the security and reliability of Accounting Information Systems by detecting anomalies, predicting fraud, and enabling explainable decision support aligned with audit standards.

Chapter 4

4. Securing Accounting and Finance Information Systems: AI-Driven Cybersecurity Innovations and Challenges

4.1 An Introduction to Secure Accounting and Finance Information Systems (IS)

4.1.1 Brief Background of the Study

Accounting Information Systems (AIS) are critical infrastructures that underpin financial reporting, auditing, and managerial decision-making across organisational hierarchies. The last decade has witnessed a significant transformation of AIS, from localised on-premises solutions to distributed, cloud-based infrastructures designed for global scalability and real-time analytics [280]. While these advancements enhance productivity and data agility, they simultaneously expand the threat landscape, exposing mission-critical systems to increasingly sophisticated cyber risks. Cybersecurity has become an essential component of Accounting Information Systems (AIS) as organisations increasingly rely on interconnected digital infrastructures. Contemporary financial environments are exposed to a variety of cyber threats, including data tampering, social engineering, unauthorised access, and the manipulation of financial records. While the cybersecurity literature is extensive, studies focusing specifically on AIS remain relatively fragmented, with limited emphasis on the unique auditability, internal control, and financial reporting requirements embedded within accounting processes.

Recent studies report a surge in AI-augmented attack vectors. These include deepfake impersonations, phishing campaigns powered by natural language generation, and data poisoning techniques targeting machine learning (ML) models embedded within accounting systems [33, 281]. Sophisticated bots can autonomously exploit vulnerabilities in AIS networks, while adversaries weaponise adversarial ML to evade anomaly detection [282].

To counteract these risks, defenders are incorporating AI across the cybersecurity lifecycle. Applications range from anomaly-based fraud detection and automated incident response engines to explainable AI (XAI) tools for auditability and regulatory transparency [283]. XAI plays a pivotal role in ensuring that AI decisions meet the legal and ethical accountability requirements outlined in standards such as GDPR and SOX [284].

Nonetheless, multiple challenges persist. Many legacy AIS platforms lack modern APIs or data pipelines, limiting seamless AI integration [285]. Additionally, financial datasets often suffer from class imbalance and missing values, which can reduce model reliability [286]. Ethical concerns also arise, particularly regarding algorithmic bias, data privacy amplification, and the opacity of some AI algorithms [287].

Cross-border compliance further complicates matters. Organisations must now adhere to overlapping global frameworks, including GDPR, SOX, and Basel III, each of which imposes distinct constraints on data handling and AI interpretability in accounting systems [288]. The adoption of AI in AIS cybersecurity, while promising, necessitates a balanced approach that considers technological capability, ethical design, and regulatory alignment. This chapter

critically examines the current state of AIS cybersecurity through a structured literature review (SLR), identifying key vulnerabilities, emerging defence mechanisms, and technological solutions directly relevant to safeguarding financial integrity.

In this chapter, the term Accounting and Finance Information Systems (AFIS) primarily refers to accounting information systems and financial modules embedded within enterprise resource planning (ERP) platforms that support financial transaction processing, internal control monitoring, and financial reporting. These systems typically include components such as journal entry processing, access control management, audit trail recording, financial statement generation, and regulatory reporting interfaces. Because these systems directly influence financial reporting reliability and audit assurance, cybersecurity mechanisms applied to AFIS must address not only confidentiality and availability concerns but also integrity, traceability, and compliance requirements that are unique to accounting environments [25, 136].

4.1.2 Overview of Accounting and Finance Information Systems

Accounting and finance information systems (AFIS) are integrated digital infrastructures that facilitate the systematic handling, monitoring, and analysis of financial transactions and records. These systems ensure the accuracy, reliability, compliance, and security of financial data through automated workflows and regulatory adherence mechanisms [289, 290].

a. Cloud-Based Solutions

Cloud-based AFIS platforms have experienced a significant increase in adoption due to their scalability, remote accessibility, and cost efficiency. These systems support real-time collaboration between accountants and clients, automate document management, and incorporate intelligent reminders and task flows [291]. Applications such as Docyt, Truewind, and Financial Cents exemplify this evolution by embedding artificial intelligence (AI) for real-time financial forecasting and reporting [292].

b. Role of AI in AFIS

AI integration in AFIS automates tasks such as data entry, reconciliation, and tax compliance. These technologies not only reduce the margin for human error but also enable predictive analytics and advanced decision support systems [281]. Real-time insights generated through AI-driven financial modelling improve strategic planning and operational efficiency [293, 294].

c. Cybersecurity Considerations

As AFIS become more interconnected and cloud-dependent, the risk landscape broadens. Cybersecurity integration is now indispensable in accounting platforms to protect against data breaches and financial fraud [295]. Measures such as end-to-end encryption, multi-factor authentication, and user-access control systems are widely recommended [296]. Employee awareness programs are equally vital since human error remains a leading cause of security breaches [297].

d. Compliance and Risk Management

AFIS must align with jurisdictional and international standards, including GDPR, SOX, and CCPA. Non-compliance not only leads to penalties but can severely affect stakeholder trust and reputation [295, 297]. Comprehensive audit trails and secure documentation systems have become mandatory to demonstrate compliance and manage reputational and legal risk.

From an accounting perspective, the importance of AI-driven cybersecurity arises from the structured nature of accounting processes. Financial information systems rely on controlled workflows such as journal entry approvals, segregation-of-duties enforcement, transaction authorisation, and audit trail generation. Artificial intelligence techniques can analyse these structured activities to identify irregular patterns that may indicate cyber intrusions or fraudulent financial manipulation. For example, anomaly detection algorithms can flag unusual journal entries, behavioural analytics can identify suspicious privileged access to financial ledgers, and automated incident-response tools can isolate compromised accounts before financial data is altered. These mechanisms demonstrate how AI cybersecurity tools are uniquely aligned with the control objectives of accounting systems, particularly in protecting transaction integrity and audit evidence reliability [98, 141].

4.1.3 AI Innovations in Cybersecurity

Artificial intelligence is transforming cybersecurity frameworks within the finance and accounting sectors. Through pattern recognition, anomaly detection, and predictive analytics, AI enhances threat identification and incident response speed [296, 297]. These innovations enhance the resilience of financial infrastructure against evolving threats such as phishing, ransomware, and DDoS attacks.

4.1.4 Challenges of AI-Driven Cybersecurity

AI-driven cybersecurity solutions offer numerous advantages in safeguarding financial systems; however, they also present significant challenges that organisations must address.

a. Third-Party Risks

Financial institutions often rely on third-party AI vendors for cybersecurity enhancements, but this introduces systemic risks. Many high-profile cyber incidents in finance originate from breaches within external services that fail to match internal security protocols [298].

b. Technical Hurdles

AI implementation comes with high technological costs, including investments in data pipelines, cloud infrastructure, and skilled personnel. Moreover, AI systems can yield false positives, potentially disrupting legitimate processes and causing operational inefficiencies [291].

c. Ethical Concerns

AI tools may unintentionally reinforce algorithmic bias due to the use of flawed training data. It can result in discriminatory financial decisions or ineffective threat detection [297]. Additionally, the unauthorised processing of personal financial data by AI systems raises critical privacy and ethical concerns [296].

d. Regulatory Complexities

Regulatory frameworks struggle to keep pace with the rapid advancements in AI. Firms must navigate laws such as GDPR and CCPA, which require transparency in data use and algorithmic decision-making [299]. Constant regulatory evolution also challenges long-term compliance strategies.

e. Collaboration and Knowledge Gaps

Implementing AI solutions demands interdisciplinary collaboration, but communication gaps between technical and non-technical teams can delay deployments. Moreover, the shortage of AI-capable cybersecurity professionals further hampers successful integration [293].

4.1.5 Research Aim

The primary aim of this research is to investigate how AI innovations enhance cybersecurity in accounting and finance information systems, with a focus on both the technical benefits and implementation challenges.

4.1.6 Research Questions

To achieve this aim, we formulate three guiding research questions:

RQ1: How does AI enhance cybersecurity in accounting and finance information systems?

RQ2: What technical, ethical, and regulatory challenges arise when implementing AI-driven cybersecurity solutions in AIS?

RQ3: What best practices can organisations adopt to balance AI innovation with robust risk management in the AIS context?

The analysis in this chapter is informed by a socio-technical governance perspective, which recognises that cybersecurity outcomes in accounting information systems depend on the interaction between technological capabilities, organisational governance structures, and regulatory compliance mechanisms. In accounting environments, security controls must simultaneously protect financial data, support auditability, and ensure compliance with financial reporting standards. Consequently, AI-driven cybersecurity mechanisms must be evaluated not only in terms of technical effectiveness but also with respect to organisational readiness, governance accountability, and regulatory oversight. Recent studies emphasise that the integration of advanced analytics and artificial intelligence within accounting systems requires alignment between technological infrastructure, internal control frameworks, and institutional governance structures [300, 301]. This perspective provides a conceptual foundation for examining how AI-based cybersecurity mechanisms can strengthen the resilience and auditability of accounting information systems.

4.1.7 Best Practices for Implementation

a. Compliance as a Foundation

Organisations should treat compliance not merely as a regulatory obligation but as a foundational component of an effective cybersecurity strategy within accounting information systems. Embedding compliance mechanisms directly into operational workflows enables

organisations to strengthen governance structures and maintain the integrity, confidentiality, and availability of financial data. In digital accounting environments, regulatory compliance frameworks such as the Sarbanes–Oxley Act (SOX), the General Data Protection Regulation (GDPR), and international information security standards provide structured guidance for managing cybersecurity risks in financial systems. Integrating these frameworks into cybersecurity governance enhances transparency, strengthens internal control mechanisms, and improves auditability within accounting processes[25] [302].

Proactively embedding compliance within organisational processes also enhances an organisation’s ability to anticipate and adapt to evolving regulatory requirements, particularly as emerging technologies such as artificial intelligence and cloud-based accounting platforms reshape the cybersecurity landscape. A forward-looking compliance strategy enables institutions to align their internal control systems with evolving standards in AI governance, data privacy, and financial reporting oversight. Maintaining awareness of regulatory developments through monitoring government regulatory bodies, consulting cybersecurity specialists, and participating in industry forums helps organisations respond effectively to changing compliance expectations. Such proactive compliance practices improve organisational agility and strengthen the resilience of accounting information systems against emerging cyber threats [94, 141]

b. Robust Compliance Frameworks

Implementing robust compliance frameworks is vital for managing complex legal and cybersecurity obligations. Leveraging technologies such as Identity and Access Management as a Service (IAMaaS) significantly enhances compliance efficiency by automating user provisioning, auditing, and reporting workflows. A unified IAMaaS platform facilitates centralised access control, enabling organisations to effectively comply with regulatory requirements such as the Sarbanes–Oxley Act (SOX), Gramm–Leach–Bliley Act (GLBA), and Payment Card Industry Data Security Standard (PCI DSS) [303].

[304] The study demonstrates that IAM solutions, when integrated into accounting and enterprise systems, improve data traceability, reduce manual compliance burdens, and help prevent unauthorised access to sensitive financial data, ultimately fostering regulatory transparency and client trust. Such mechanisms are critical for maintaining compliance with financial regulations such as the Sarbanes–Oxley Act (SOX) and other financial reporting requirements [25, 94, 141]

c. Regular Audits and Continuous Monitoring

Conducting regular audits is essential for maintaining regulatory compliance and identifying potential vulnerabilities in financial systems. Through periodic evaluations of policy adherence and security controls, organisations can proactively remediate gaps before they escalate into full-blown compliance violations. As highlighted by [267], cybersecurity audits play a crucial role in enhancing resilience within financial institutions, particularly when

combined with threat intelligence mechanisms [267],[99, 141]In parallel, continuous monitoring technologies have become essential tools for real-time threat detection and regulatory observability. These systems offer dynamic oversight into access behaviours, anomalous activities, and configuration drift. Continuous monitoring enables institutions to respond rapidly to deviations from expected norms, critical for maintaining integrity in environments governed by standards such as SOX, NIST, and ISO 270010[305].

These mechanisms are particularly valuable in accounting environments where timely detection of irregular activities is critical for preventing financial fraud and data manipulation. By integrating automated monitoring tools with traditional audit procedures, organisations can strengthen internal control systems and improve the reliability of financial reporting processes[141],[99].

d. Employee Training and Security Awareness

A well-trained workforce represents the first line of defence against cyber threats. Given that human error remains a significant vector for breaches, fostering a culture of cybersecurity awareness through regular training is critical. [306] emphasises that employees educated about phishing, social engineering, and password hygiene exhibit lower risk exposure and contribute to a stronger organisational security posture [306]. Institutions should implement mandatory cybersecurity awareness programs, refreshers on regulatory updates, and simulated phishing exercises to maintain vigilance.

Human factors remain one of the most significant sources of cybersecurity vulnerabilities in accounting environments. Employees who lack awareness of cybersecurity risks may unintentionally expose financial systems to threats such as phishing attacks, credential theft, and social engineering schemes. Consequently, organisations must invest in regular cybersecurity awareness programs designed to educate employees about safe data handling practices, password management, and the identification of suspicious communications. Training initiatives should also emphasise compliance with financial reporting regulations and internal control procedures. Research in accounting information systems highlights that organisations with well-established cybersecurity training programs demonstrate significantly lower rates of security incidents and improved compliance outcomes [141],[301],[219].

e. Investment in Cybersecurity Technologies

Strategic investment in advanced cybersecurity tools is essential for addressing evolving threat landscapes. Organisations should prioritise technologies like AI-driven anomaly detection, robotic process automation (RPA) for incident response, and threat intelligence platforms for proactive defence[307]. The study demonstrated that AI systems integrated with explainable logic offer both technical accuracy and regulatory traceability, especially under GDPR and SOX requirements [307].

Moreover, implementing multi-factor authentication (MFA) strengthens identity verification processes, significantly reducing the risk of unauthorised access. MFA, when paired with

identity governance solutions, can meet compliance benchmarks in sectors regulated under GLBA, HIPAA, and PCI DSS [307]. In financial systems, these technologies can analyse transaction patterns, monitor access behaviours, and identify irregular activities that may indicate fraudulent behaviour or cyber intrusions. When integrated with explainable artificial intelligence (XAI) techniques, these tools also support transparency and regulatory accountability by providing interpretable explanations for automated security decisions. Such capabilities are particularly important in accounting environments where auditability and regulatory compliance are critical considerations [99],[300],[219].

f. Third-Party Vendor Management

As organisations expand their digital ecosystems, third-party vendors increasingly represent a significant risk vector for cyber intrusions and compliance breaches. It is essential to establish rigorous vendor governance protocols, such as security questionnaires, periodic audits, and least-privilege access enforcement. [308] recommends adopting a holistic third-party risk framework that incorporates monitoring, legal enforcement, and cybersecurity insurance to mitigate indirect exposures. Continuous monitoring of vendor access logs, enforcing service-level agreements (SLAs) with embedded security clauses, and maintaining an up-to-date inventory of external dependencies are critical for minimising residual risk [308]. Effective vendor governance practices include enforcing least-privilege access policies, conducting periodic security audits of external partners, and incorporating cybersecurity requirements into service-level agreements. Strengthening third-party risk management is particularly important in accounting environments where financial data integrity and confidentiality are essential for maintaining regulatory compliance and organisational trust [219],[309].

4.1.8 Case Studies

a. Enhancing Cybersecurity in Financial Institutions

Contemporary case studies highlight that the robustness of cybersecurity frameworks in financial institutions is directly linked to the maturity of their incident response strategies. Institutions that have formalised, tested, and periodically updated their response and recovery protocols exhibit markedly improved resilience during ransomware, phishing, or insider threat incidents. According to [310], zero-trust architectures coupled with structured incident response mechanisms significantly reduce breach recovery time and minimise operational downtime.

The adoption of AI-enabled detection tools has further enhanced institutional capacity to detect anomalies in real time. For instance, one multinational bank experienced a 40% increase in detection accuracy and a 50% reduction in response latency after integrating AI-driven Security Information and Event Management (SIEM) systems [311]. These advancements leverage pattern recognition, behavioural analytics, and alert prioritisation to improve overall threat intelligence.

b. Challenges and Risk Management

Despite technological advances, financial institutions continue to face acute challenges, including talent shortages, legacy IT infrastructure, and the need to balance user experience with security [312]. A recurring theme in breach case analyses is the cost of manual or outdated incident workflows. In the Equifax breach, delayed disclosure and inadequate coordination of responses worsened regulatory penalties and public trust [313]. Real-world cases also highlight that under-resourced institutions often suffer from fragmented security ecosystems, which complicates unified threat management. Effective cybersecurity thus necessitates not only technological but also organisational change in governance and coordination protocols [314].

c. The Role of AI in Financial Applications

AI's role in transforming cybersecurity operations is especially evident in areas such as insider threat detection, behavioural analytics, and fraud mitigation. Many financial organisations are opting to build in-house AI systems to avoid data privacy risks tied to public APIs [315]. For example, JPMorgan's internal AI architecture supports secure employee-AI interactions while preserving sensitive data boundaries.

However, this shift brings new risks. The use of sensitive proprietary datasets, even within internal AI training pipelines, can increase the attack surface through adversarial machine learning or shadow data leakage [316]. Hence, secure AI development lifecycles and model governance have become critical.

d. Lessons Learned

Across reviewed case studies, a typical lesson is that technical solutions alone are insufficient. Successful cybersecurity transformation demands cultural change. The implementation of zero-trust principles, especially continuous authentication and least-privilege access, is most effective when accompanied by cybersecurity awareness programs [311].

Additionally, cross-training IT and security teams in AI-based threat modelling and data governance has proven beneficial. [317] The study underscores that institutions that invest in AI literacy and simulation-based response training exhibit greater adaptability during zero-day attacks or multi-vector intrusions.

4.2 Literature Review

4.2.1 The Evolving Threat Landscape

Accounting information systems (AIS) face persistent risks from ransomware, phishing/business email compromise, and data exfiltration. Recent industry syntheses show ransomware and social engineering remain among the top incident patterns, with human-factor exploitation still prominent; AI-enabled deepfakes have been used to impersonate finance leaders and authorise transfers (e.g., the Hong Kong “CFO deepfake” case) [318-320],[321]. These trends reflect the lucrative mix of financial assets and personal data held by AIS, as well

as the growing professionalisation of state-sponsored and organised groups targeting them [318, 319].

Cyber threats affecting AFIS frequently target specific accounting control points rather than merely generic IT infrastructure. For example, phishing and business email compromise often attempt to bypass payment authorisation controls, ransomware disrupts transaction processing and data availability, insider misuse can undermine access management and journal entry integrity, and deepfake impersonation may be used to manipulate approval workflows involving senior finance personnel [25]. Mapping threats in this way helps clarify their implications for internal control design, especially in relation to input integrity, authorisation, access restriction, change management, and audit trail reliability. Accounting Information Systems texts consistently frame these control activities as central to maintaining reliable financial processing and reporting [25]. Cyber threats targeting accounting systems frequently exploit specific control points within financial information systems. For example, phishing attacks often attempt to bypass payment authorisation procedures, ransomware disrupts transaction processing systems, and insider threats may manipulate journal entries or financial records. These attacks therefore directly affect core accounting control objectives such as input integrity, authorisation verification, access management, and audit trail reliability [25].

Cybersecurity threats in accounting primarily target key components of the Accounting Information System (AIS), including transaction processing, audit trails, and access controls. For example, fraud can damage data accuracy, and unauthorised access can break the separation of duties. Using AI-based detection tools helps continuously monitor transactions, improving internal controls and making audits easier. This link between cybersecurity measures and AIS components underscores the importance of the proposed framework for financial management.

4.2.2 AI-Driven Innovations in Cybersecurity

Research and practice highlight four principal AI applications relevant to AIS security:

a. Anomaly Detection

Unsupervised/semi-supervised approaches—including autoencoders, Isolation Forest, and sequence models (e.g., LSTM)—flag deviations in transaction patterns and access logs and are widely studied for financial fraud and audit anomalies [133, 322-325].

In accounting information systems, anomaly detection techniques can be applied to journal entry testing and transaction monitoring. For instance, machine learning models can identify unusual journal entries, abnormal transaction values, or irregular posting patterns that may indicate fraudulent financial reporting or cyber manipulation of accounting records [99, 141, 218]

b. Incident Response Automation

Security orchestration, automation and response (SOAR) platforms correlate alerts and execute playbooks (e.g., account blocking, containment) with reduced analyst touch—now a recognised capability class in security operations (Gartner; Info-Tech/SoftwareReviews).

Within accounting environments, automated incident response systems can be used to contain and mitigate cyber incidents affecting financial processes, such as unauthorised payment approvals or manipulation of accounts payable systems. These systems can automatically suspend suspicious transactions or restrict access to financial modules, thereby reducing financial losses and ensuring the integrity of accounting data [219]

c. Behavioural Analytics

User- and entity-behaviour analytics (UEBA) profile users/devices and apply sequence modelling to detect insider misuse and compromised accounts, increasingly integrated with SIEM/XDR in finance (Palo Alto Networks; Microsoft; TCS white paper; research exemplars using LSTMs).

Behavioural analytics techniques are particularly relevant in monitoring privileged access within ERP-based accounting systems. For example, AI models can analyse user behaviour patterns to detect unusual access to general ledger systems, unauthorised modification of financial records, or abnormal login activities by users with elevated privileges, thereby strengthening internal control mechanisms [25, 300].

d. Continuous Learning

Adaptive pipelines using online learning and (in some settings) reinforcement learning aim to cope with evolving attack patterns and concept drift in intrusion/fraud detection [326].

These innovations collectively yield a 40–60% uplift in detection speed and a 30–45% reduction in manual investigation workloads in experimental settings.

Continuous learning mechanisms enable AI systems to adapt to evolving cyber threats in accounting environments by updating detection models based on new transaction patterns and fraud scenarios. This is particularly important in financial systems where attackers continuously modify their techniques, requiring adaptive cybersecurity controls to maintain the reliability and accuracy of financial reporting [99, 301]

4.2.3 Learning-Based Anomaly Detection in AIS

Autoencoders learn standard accounting/transaction patterns, utilising reconstruction error for anomaly scoring. The Isolation Forest isolates rare patterns through random partitioning. LSTMs capture temporal dependencies in journals, access logs, and payment streams [322–324]. Financial-domain studies—including credit-card and accounting-record settings—report competitive detection performance under class imbalance, with ongoing work on self-supervised and federated approaches to protect sensitive ledger data [133, 327, 328].

4.2.4 Adversarial Machine Learning Defences

As ML is adopted in defence, adversaries craft adversarial examples to mislead models. Defences studied include: adversarial training (augmenting training with adversarial samples),

GAN-based scenario generation/augmentation, and threat-simulation platforms that emulate attacker behaviour at scale [329]. While promising, these techniques require domain-specific validation for AIS and careful governance to mitigate risks of data leakage or overfitting. To counter this threat, the study proposes:

a. Adversarial Training

Incorporating adversarial samples into training sets so models learn robust decision boundaries.

b. Generative Adversarial Networks (GANs)

Generating synthetic attack scenarios for stress-testing detection systems without exposing sensitive corporate data. GAN-based approaches enable the simulation of adversarial conditions that improve the robustness of anomaly detection models and support proactive cybersecurity strategies in financial and accounting systems[330].

c. Threat Simulation Platforms

Orchestrating red-team exercises with AI-driven agents to mimic real-world evasion tactics. These platforms enable organisations to evaluate system vulnerabilities and response capabilities under simulated cyberattack conditions, supporting continuous improvement in cybersecurity defences [99, 141].

4.2.5 Explainable AI (XAI) for Financial Compliance

Regulatory scrutiny and auditability make explainability central in finance. SHAP provides additive feature attributions grounded in cooperative-game theory, and LIME offers local surrogate explanations; both see growing use in financial-risk/fraud modelling and auditing to justify automated flags and speed analyst onboarding [331, 332].

4.2.6 Conceptual Boundaries

Although cybersecurity has been extensively analysed within the broader information systems and computer science domains, AIS cybersecurity requires a distinct conceptual treatment. Unlike general IT systems, AIS must comply with financial reporting standards, internal control frameworks, and audit requirements. Therefore, cybersecurity measures within AIS must ensure not only confidentiality and integrity but also auditability, verifiability, and regulatory reliability. These conceptual boundaries differentiate AIS cybersecurity from mainstream IT security and emphasise the need for tailored controls aligned with accounting processes.

4.3 Conceptual Framework

To conceptualise how artificial intelligence (AI) technologies interact with accounting information systems (AIS) cybersecurity, this study proposes a tripartite framework comprising technological, organisational, and external environmental dimensions. The model aligns with prior information systems frameworks such as the Technology–Organisation–Environment (TOE) model [333] and the AI readiness models of organisational adoption [334], contextualised here for AIS-security decision-making:

4.3.1 AI Technologies

At the technological core, AI-driven capabilities underpin threat detection, prevention, and automated response. These include anomaly-recognition models, behavioural profiling, and adaptive learning mechanisms that refine security policies through continuous feedback [133, 323]. In the AIS context, these tools enhance auditability and fraud prevention by identifying irregular financial transactions in real-time and enabling automated containment through SOAR-like platforms [335]. The learning loop concept reflects the self-optimising nature of AI systems that evolve with new data and threat patterns.

4.3.2 Organisational Environment

The organisational layer encompasses internal readiness factors that determine AI adoption feasibility. Legacy accounting architectures, fragmented databases, and limited workforce AI literacy often constrain integration [334]. Governance frameworks and budget allocations further influence whether AI deployment is strategic or reactive[336]. Effective implementation requires clear internal policies on algorithmic accountability, data governance, and cross-functional collaboration among accounting, IT, and risk management teams [337]. Empirical studies suggest that top-management commitment and ethical awareness facilitate the adoption of AI in financial control environments [338].

4.3.3 External Factors

External pressures encompass regulatory compliance, vendor ecosystem maturity, and ethical standards. Financial regulators increasingly require explainability, fairness, and audit trails for algorithmic decision-making[339]. Vendor ecosystems affect organisations' access to mature AI-security solutions and cloud-based analytics. Ethical guidelines from professional accounting bodies and standards such as ISO 27001 and COSO influence how firms balance innovation with fiduciary and data-protection obligations [340]. This tripartite framework integrates technological innovation, organisational readiness, and external regulation to explain variations in AIS-security performance. It posits that adequate protection arises when AI capability maturity is matched with organisational preparedness and regulatory alignment. This synthesis forms the theoretical foundation for the empirical analysis in subsequent chapters.

4.4 Research Methodology

We adopt a [341] systematic literature review (SLR) approach structured according to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines. A Structured Literature Review (SLR) approach was employed to ensure a rigorous, transparent, and replicable examination of scholarly research relating to cybersecurity within Accounting Information Systems. The SLR followed established guidelines for information systems research [280], enabling the systematic identification, selection, and synthesis of peer-reviewed academic studies [342]. This methodology ensures transparency, reproducibility,

and rigour in identifying and synthesising existing research on AI-driven cybersecurity for AIS. We have defined the PRISMA concept in detail in Section 3.5.3 of Chapter 3.

4.4.1 Identification/search strategy

We queried major databases (IEEE Xplore, ScienceDirect, ACM Digital Library, and Google Scholar) using search terms such as “AIS cybersecurity,” “AI in finance security,” “anomaly detection accounting,” and “adversarial ML finance.”

As previously pointed out, the literature search was conducted across four primary academic sources:

- IEEE Xplore (technical cybersecurity and AI-driven security research)
- ScienceDirect (Elsevier) (AIS, accounting, internal control, and IS security research)
- ACM Digital Library (computing, IS, behavioural security research)
- Google Scholar (identify additional citations and forward/backward referencing)

The following Boolean search strings were used:

- “cybersecurity” AND “accounting information systems”
- “AIS security” AND “financial reporting integrity”
- “cyber threats” AND “internal controls”
- “machine learning” AND “AIS cybersecurity”
- “AI-driven cybersecurity” AND “accounting systems”

Searches were limited to peer-reviewed journal articles and conference papers, published between 2010 and 2024, to reflect contemporary developments in AIS and cybersecurity technologies.

4.4.2 Screening

From an initial pool of 342 articles published between 2019 and 2025, we screened titles and abstracts for relevance to AI-driven cybersecurity practices specifically within AIS contexts. The initial database searches generated a combined set of publications, which were first screened by title and abstract. Full-text screening was then conducted to assess eligibility based on inclusion and exclusion criteria. Backwards and forward citation tracking using Google Scholar further strengthened the comprehensiveness of the review. The final set of studies was then synthesised thematically, focusing on key cybersecurity challenges and defence mechanisms relevant to AIS, including fraud detection, audit trail protection, authentication, access control, and AI-enabled anomaly detection.

4.4.3 Eligibility

We applied inclusion criteria focusing on empirical studies, theoretical frameworks, and case analyses involving AI solutions for AIS security. Exclusion criteria eliminated general cybersecurity papers without an AIS emphasis.

4.4.4 Inclusion

Twelve studies met all criteria. These works concentrated on anomaly detection algorithms, adversarial ML defences, and an emerging interest in explainable AI frameworks tailored to financial systems.

Inclusion Criteria

Studies were included if they:

- Examined cybersecurity mechanisms within accounting or financial systems;
- Analysed AIS-specific vulnerabilities, controls, or audit functions;
- Proposed or evaluated CS mechanisms (technical or organisational);
- Presented conceptual, empirical, theoretical, or technical contributions;
- They were published in reputable peer-reviewed venues.

Exclusion Criteria

Studies were excluded if they:

- Focused entirely on general IT/IS security with no accounting linkage;
- Were non-peer-reviewed sources (blogs, reports, theses, editorials);
- Did not address cybersecurity or AIS directly.
- Provided insufficient methodological detail.

Data extraction captured methodological details, AI techniques, performance metrics (e.g., detection accuracy and false-positive rates), and reported challenges. Quality assessment considered study design consistency, dataset appropriateness (e.g., PaySim, synthetic corporate transaction logs), and transparency of findings.

Overall, the structured literature review process ensured that the studies included in this chapter were systematically identified, screened, and evaluated based on their relevance to artificial intelligence–driven cybersecurity in accounting and financial information systems. This approach enhances the transparency and reliability of the review process and ensures that the analysis presented in this chapter is grounded in credible and relevant academic literature [225],[343].

4.5 Results and Findings

4.5.1 RQ1:AI’s Role in Enhancing AIS Cybersecurity

Empirical evidence indicates that AI integration in AIS environments yields significant operational gains. Specifically, detection speed improves by 40–60%, aligning with [344], who found a 56% increase using deep-learning-based intrusion systems. False favourable rates decrease by 20–30%, [345]who observed 27% improvement using contextual feature adaptation. Analyst workload shows a 35–45% reduction, as confirmed, due to automated alert triage and behavioural analytics. These outcomes were further validated in our case simulations, which compared AI-enhanced pipelines to baseline rule-based controls. These gains stem from the deployment of anomaly detectors, automated response workflows, and behavioural analytics pipelines. The performance improvements reported in this section are

derived from findings documented in prior empirical studies and experimental cybersecurity evaluations rather than from primary simulations conducted within this thesis.

4.5.2 RQ2: Technical, Ethical, and Regulatory Challenges

Major hurdles identified across studies include:

a. Technical

Legacy accounting platforms lack integration APIs, forcing costly middleware development. Data quality issues, such as missing entries and class imbalance, undermine model training and generalisability.

b. Ethical

Algorithmic bias arising from unrepresentative training data can disproportionately flag transactions from specific demographics, raising concerns about fairness and equity. Privacy amplification risks emerge when models infer sensitive attributes without consent.

c. Regulatory

Compliance demands evolve rapidly across jurisdictions. AI-driven controls must meet standards such as SOX, GDPR, and local financial regulations, which complicates deployment in multinational settings.

4.5.3 RQ3: Best Practices for Risk-Balanced AI Adoption

Successful organisational approaches emphasise:

a. Human-AI Collaboration

Positioning AI as a decision-support tool rather than full automation.

b. Continuous Model Evaluation

Implementing periodic retraining schedules and performance audits.

c. Governance Frameworks

Defining clear roles, responsibilities, and KPIs for AI initiatives, backed by board-level oversight.

d. Vendor Management

Enforcing SLAs on data quality, security certifications, and transparency obligations.

4.6 Discussion and Analysis

The rapid adoption of AI in AIS cybersecurity demonstrates significant efficacy gains, yet introduces complex socio-technical considerations. Organisational readiness emerges as the linchpin: without sufficient AI literacy among finance professionals, the potential of advanced models remains underutilised. Training programs that blend domain expertise with ML fundamentals can bridge this gap.

Interoperability between AI tools and legacy accounting software remains a persistent barrier to effective integration. Middleware solutions and API standardisation efforts are vital to streamline data ingestion and model deployment. Open standards such as the Open Financial Exchange (OFX) and emerging AIS-specific security schemas could catalyse broader adoption.

Ethical risk management demands integrated privacy-by-design and fairness-by-design strategies. Techniques such as differential privacy and adversarial debiasing help mitigate unintended disclosures and discriminatory alerts. Embedding these safeguards early in the AI lifecycle aligns with regulatory expectations and preserves stakeholder trust.

Regulatory compliance for AI in financial services is still evolving. Organisations should proactively engage with regulators to shape guidelines around XAI thresholds and model auditability. Cross-industry consortia can accelerate the development of standardised benchmarks and certification programs for cybersecurity AI focused on AIS.

From a governance perspective, AI-enabled cybersecurity in AFIS should be aligned with recognised internal control and enterprise risk principles rather than treated as a purely technical add-on. COSO states that enterprise risk management should be integrated with strategy and performance, while governance-of-IT research emphasises formal decision structures, monitoring, and accountability mechanisms for technology-enabled controls. In accounting environments, this means AI security tools should remain auditable, explainable where needed, and embedded within broader internal control accountability, compliance monitoring, and assurance processes [346],[309].

4.7 Future Trends

4.7.1 Cloud Computing in Finance

The adoption of cloud technology in the financial services sector has increased rapidly, with 54% of companies in the industry expected to utilise it by 2021. As organisations continue to migrate their IT infrastructure to the cloud, this figure is expected to rise significantly in 2024, driven by demand for flexibility, scalability, and cost efficiencies that traditional on-premises data centres cannot offer [347]. However, the transition comes with challenges, including rising costs associated with increased demand, potential cost overruns from unplanned adoptions, and data egress fees-[348, 349]. Financial institutions must be strategic in their approach, potentially engaging external support to ensure successful cloud adoption and optimisation.

4.7.2 Blockchain Technology Applications

While the excitement surrounding cryptocurrencies has waned amid recent scandals, blockchain technology remains poised for growth in the financial sector. Its applications extend beyond digital currencies to include areas such as regulatory technology (regtech) and audit processes[348]. Blockchain offers the potential for immutable, transparent ledgers that can enhance audit efficiency and accuracy by enabling real-time verification of financial transactions. As firms explore these applications, the technology's role in creating secure, efficient systems is expected to expand in 2024 and beyond.

4.7.3 AI Innovations in Cybersecurity

Artificial Intelligence (AI) is playing an increasingly pivotal role in enhancing cybersecurity measures across various industries, including finance. AI-driven tools are revolutionising

Identity and Access Management (IAM) by automating incident response workflows, detecting anomalies in user behaviour, and proactively identifying vulnerabilities before they can be exploited[350]. As financial institutions face ever-evolving cyber threats, the integration of AI will be crucial for maintaining robust security protocols and ensuring the integrity of sensitive financial information[350].

4.7.4 Ongoing Assessment of Technology Relevance

As the financial services industry continues to embrace emerging technologies, companies must remain vigilant in reassessing their relevance and maturity. Institutions are likely to regularly evaluate their technology investments, especially as new use cases emerge and existing technologies evolve[348]. This continuous assessment will enable firms to remain competitive and responsive to the evolving financial services landscape, ultimately improving operational resilience and enhancing customer trust.

4.8 Limitations

4.8.1 SLR Limitations

Our SLR is subject to the following limitations:

a. Publication Bias

Positive results may be overrepresented, while negative or inconclusive studies remain unpublished.

b. Domain Specificity

Few empirical studies focus exclusively on AIS, with many general cybersecurity papers extrapolated to financial contexts.

c. Study Heterogeneity

Variations in datasets, performance metrics, and evaluation methodologies hinder direct quantitative meta-analysis.

These constraints underscore the need for more rigorous, longitudinal field studies in operational AIS environments.

4.8.2 Organisational and Cost Barriers

Adoption of AI-driven cybersecurity in AIS faces significant resource and capability challenges:

a. Skill Shortage

A dearth of professionals proficient in both accounting domains and ML techniques stalls project initiation.

b. Explainability Tool Maturity

Legal sufficiency of XAI outputs remains contested, potentially exposing firms to audit risks.

c. Computational Expenditure

High-performance computing resources for training deep learning models incur substantial capital and operational costs.

d. Legacy Dependencies

Continued reliance on static rule engines limits AI integration, delaying modernisation efforts. Mitigation strategies include partnerships with academic institutions for talent pipelines, cloud-based ML services to amortise compute costs, and modular AI architectures that gradually replace legacy components.

4.8.3 Stakeholder Roles and Operational Challenges

Effective AIS cybersecurity ecosystems involve multiple stakeholders:

a. Financial Institutions

Must align AI projects with risk appetite and compliance mandates.

b. Regulators

Provide oversight and evolve frameworks to encompass AI-specific governance.

c. Vendors

Deliver turnkey security products with transparent model documentation.

d. National Security Entities

Share threat intelligence and support public-private defence initiatives.

Operational challenges include vendor lock-in, burnout among scarce cybersecurity personnel, and risks to third-party supply chains. Automating routine tasks eases analyst workloads but cannot substitute for human judgment in complex incident investigations.

4.9 Integration with the final framework

The findings of this chapter inform both the empirical modelling presented in Chapter 7 and the conceptual integration undertaken in Chapter 8. By identifying the technological, organisational, and audit challenges surrounding AIS cybersecurity, this chapter establishes the foundations for the BQMG-AIS framework, in which blockchain, quantum security principles, machine learning, and game theory are combined to strengthen the resilience and auditability of accounting systems.

4.10 Best Practices for Implementation

Drawing on the reviewed literature, we recommend the following best practices:

4.10.1 Governance & Compliance

- Establish an AI security steering committee with cross-functional representation to ensure adequate oversight and coordination.
- Define IAM policies and automated audit trails for all AI model inputs and outputs.

4.10.2 Vendor & Data Management

- Incorporate SLAs on data quality metrics and security certifications into vendor contracts.
- Maintain immutable data provenance logs to ensure auditability and transparency.

4.10.3 AI Usage Policies

- Document allowable AI use cases and clarify employee responsibilities.
- Provide mandatory training on AI ethics and cybersecurity hygiene.

4.10.4 Continuous Improvement

- Schedule quarterly model performance assessments, including drift detection, to ensure optimal model performance.
- Run red-team exercises that incorporate generative adversarial threats to stress-test defences.

4.11 Conclusion

Artificial intelligence offers transformative potential for enhancing cybersecurity in accounting and finance information systems. Our systematic review demonstrates substantial improvements in threat detection speed and operational efficiency through anomaly detection, automated response, and behavioural analytics. However, technical barriers, such as legacy system integration and data quality, and non-technical hurdles, such as ethical concerns and evolving compliance requirements, must be addressed to actualise sustainable adoption. A holistic strategy that marries AI innovation with human oversight, robust governance frameworks, and continuous evaluation is paramount. Organisations should invest in talent development, adopt modular AI architectures, and proactively engage with regulators to shape AI-centric guidelines. Future research must emphasise field-based empirical studies, the development of standardised benchmarks, and the creation of interoperable tools to foster trust and transparency. With careful planning and cross-disciplinary collaboration, AI-driven cybersecurity can empower firms to safeguard their critical financial assets and processes against an increasingly complex and evolving threat landscape.

While AI-driven approaches enhance fraud detection and compliance by increasing explainability and automation, the long-term confidentiality of data in accounting systems is at risk from the advent of quantum computing. To tackle these emerging cryptographic challenges, Chapter 5 presents an overview of Quantum Computing and Post-Quantum Cryptography. It explores how quantum-resilient algorithms can safeguard financial records from future decryption threats and seamlessly integrate with AI-enabled auditing processes.

Chapter 5

5. Quantum Computing and Cybersecurity in Accounting and Finance: The Present and the Future Challenges and Opportunities for Securing Accounting and Finance Systems

5.1. An Introduction: Quantum Computing and Accounting and Finance System Cybersecurity Challenges

5.1.1. Background of the Study

Cybersecurity has become a crucial component of modern accounting and finance systems, driven by the growing sophistication of cyber threats. Traditional cryptographic techniques, such as RSA and Elliptic Curve Cryptography (ECC), face new vulnerabilities as financial data and transactions become increasingly digitalised, particularly with advances in quantum computing [351]. Financial organisations are particularly vulnerable to attacks from adversaries utilising quantum technology, as they primarily depend on public-key cryptography protocols. Quantum computing has the potential to revolutionise current cybersecurity systems, making the accounting and finance industries particularly vulnerable to significant changes. Examining the relationship between quantum computing and the protection of financial systems reveals that this new technology is both a powerful ally and a formidable challenge. The article aims to elucidate the complexities of how quantum computing can enhance the cybersecurity of financial and accounting systems. The risks of transitioning from classical to quantum paradigms are substantial, yet the promise of improved data protection and transaction security is equally compelling.

5.1.2. Motivation and Relevance

The convergence of quantum computing (QC) and cybersecurity (CS) marks a pivotal turning point in the evolution of accounting and financial systems. With the increasing digitisation of financial operations, cybersecurity has become fundamental in protecting sensitive accounting data, client records, and strategic financial information [352]. However, existing cryptographic frameworks such as RSA and Elliptic Curve Cryptography (ECC), which underpin current cybersecurity protocols, are highly susceptible to quantum algorithms, notably Shor's algorithm for integer factorisation and Grover's algorithm for search, which could render these methods obsolete [353]. Concurrently, quantum computing offers transformative computational advantages, enabling the high-speed resolution of complex financial problems, such as portfolio optimisation, risk modelling, and credit scoring [139]. However, the same computational power introduces new cybersecurity challenges, threatening the integrity of encrypted systems [354]. This duality of opportunity and risk positions the topic as both timely and urgent, offering the potential to conceptualise and implement quantum-resilient cybersecurity architectures within accounting frameworks and paving the way for future-proof financial infrastructures.

From a theoretical perspective, the challenges posed by quantum computing to classical cryptographic infrastructures can be understood through the lens of information security risk theory and long-term data confidentiality theory. Information security risk theory emphasises that organisational information systems must continuously adapt to evolving technological threats that compromise the confidentiality, integrity, and availability of digital information. In the context of accounting systems, cryptographic mechanisms form a fundamental component of financial data protection and audit reliability. However, advances in quantum computing challenge the underlying computational assumptions that secure widely used encryption methods such as RSA and Elliptic Curve Cryptography. Long-term data confidentiality theory further highlights the risk that encrypted financial records captured today may become vulnerable in the future once sufficiently powerful quantum computers emerge, a phenomenon often referred to as “harvest now, decrypt later”. Consequently, accounting information systems must adopt forward-looking cybersecurity strategies that incorporate quantum-resistant cryptographic mechanisms to ensure the long-term protection of financial data [138, 353, 355].

This chapter is theoretically grounded in information security risk theory and long-term data confidentiality theory, which provide a conceptual basis for analysing the evolving cybersecurity challenges in accounting information systems. Information security risk theory emphasises the identification, assessment, and mitigation of risks arising from vulnerabilities in technological infrastructures, particularly in financial systems where data integrity, availability, and confidentiality are critical [41, 356]. In the context of accounting information systems, these risks are amplified due to the sensitivity of financial data and the reliance on cryptographic mechanisms for secure transactions.

In parallel, long-term data confidentiality theory highlights the importance of protecting sensitive information against future adversarial capabilities, particularly in scenarios where encrypted financial data may be intercepted and stored for later decryption [138, 357]. The emergence of quantum computing introduces a paradigm shift in this context, as quantum algorithms such as Shor’s algorithm threaten the security assumptions underpinning widely used cryptographic systems, including RSA and elliptic curve cryptography [353, 355]. This creates a “harvest now, decrypt later” risk, which is particularly critical for accounting and financial records that require long-term confidentiality and auditability.

By integrating these theoretical perspectives, this chapter moves beyond a purely technical analysis and provides a structured understanding of how quantum computing reshapes cybersecurity risk in accounting environments. It also justifies the need for transitioning towards quantum-resilient cryptographic frameworks to ensure the long-term protection of financial information systems.

5.1.3. Research Aim, Research Questions and Research Objectives

a. Research Aim

The primary aim of this thesis is to explore and develop a comprehensive understanding of how quantum computing technologies can be applied to enhance the cybersecurity of accounting systems. The thesis aims to scrutinise the potential of quantum computing to strengthen cybersecurity measures in accounting, focusing on how quantum algorithms and technologies can address the limitations of classical computing in safeguarding sensitive financial data and ensuring secure transactions. It would not be wrong to say that this involves analysing the potential of quantum-resistant algorithms and Quantum Key Distribution (QKD) in safeguarding financial data against emerging cyber threats, thereby ensuring the integrity, confidentiality, and reliability of accounting processes in the quantum era.

b. Research Question

❖ Primary Question

The primary question that needs to be considered in this article is:

“How can quantum computing enhance CS in accounting and finance within an organisation?”

It also compares the effectiveness of quantum-resistant algorithms in safeguarding accounting data through quantum-enabled attacks with classical cryptographic methods. This research also explores the response to how the conceptual model is based on the Thompson model. [190] can be adapted to include QC Technologies for enhanced CS in accounting. Further research identifies an organisation’s main challenges in adopting QC Technologies for improved cybersecurity in accounting and how to resolve them.

❖ Secondary Research Questions

1-Question: What are the critical computing threats in current accounting systems that quantum computing can address?

2-Question: What are the most promising quantum algorithms for securing financial data in accounting?

3-Question: How can quantum computation be integrated into current accounting systems without disrupting operations?

These research aims, objectives, and questions are designed to guide the exploration and analysis of quantum computing's role in transforming the cybersecurity landscape for accounting systems, ultimately contributing to the development of more secure and resilient financial infrastructures.

c. Research Objectives

The thesis clarifies the role of quantum computing as both a threat and a tool in accounting cybersecurity, responding to the aforementioned research questions. The objectives aligned with these questions include:

❖ Objective 1

Identify and analyse the major cybersecurity threats facing contemporary accounting and finance systems. Determine which threats could be mitigated or neutralised by quantum computing capabilities, which will be addressed through responding to Research Question 1.

❖ **Objective 2**

Investigate and evaluate quantum computing algorithms and techniques (such as quantum cryptography and quantum-resistant algorithms) that show promise for protecting financial data. Assess their applicability and effectiveness in accounting contexts, as addressed by Research Question 2.

❖ **Objective 3**

Develop a framework or set of guidelines for integrating quantum-computing-based security measures into existing accounting information systems. The goal is to implement these measures to minimise disruption to business operations, as addressed by Research Question 3. It includes considering the organisational, technical, and regulatory factors influencing successful implementation.

5.1.4. Significance of the Study

This research is significant for both academia and industry. Academically, it bridges the gap between quantum computing and information security in accounting information systems, two fields that are often considered in isolation. It contributes to the theoretical understanding of how emerging technologies can transform cybersecurity practices in specific contexts (here, financial and accounting systems). Practically, the findings will help organisations in the financial sector prepare for the quantum revolution. For instance, a recent industry survey found that over 70% of large U.S. firms expect quantum computers to break current encryption by 2030 and are “extremely concerned” about this threat [358]. However, many firms have not started planning adequate defences [358]. By providing insight into quantum-resilient security measures and integration strategies, this thesis offers timely guidance to practitioners (CISOs, IT managers, auditors, and accountants) on strengthening their systems before quantum attacks become a reality.

This study makes a significant transdisciplinary contribution to cybersecurity, financial systems engineering, and quantum information science. Establishing a robust framework for evaluating and implementing quantum cybersecurity techniques adds to the existing body of knowledge. It provides financial organisations with valuable insights for preparing their data systems against post-quantum threats. Additionally, the research addresses policy-level implications, emphasising the urgent need for industry leaders and regulatory agencies to prioritise investments in quantum-secure infrastructures and the upskilling of the cybersecurity workforce.

5.1.5. Scope and Delimitations

The scope includes a systematic literature review (SLR) using the PSALSAR methodology, analysing publications from 2015 to 2024. This research focuses on quantum cryptographic mechanisms, such as Quantum Key Distribution (QKD) and quantum-resistant algorithms, and their applicability to financial cybersecurity. The conceptual framework has been designed and analysed using. [190]Thompson enhanced the model and added new factors to the personal

computing utilisation model, which was then applied to the context of quantum-enhanced cybersecurity systems in accounting and finance.

While comprehensive in its synthesis of peer-reviewed literature, the study maintains the following boundaries:

- a. The research does not analyse region-specific regulatory frameworks or case studies; it adopts a global perspective without delving into country-specific implementations of quantum-safe accounting systems.
- b. The study does not include primary data collection such as interviews, surveys, or case-based testing. It relies exclusively on secondary data sourced from indexed academic databases.
- c. The study focuses on accounting and finance systems, excluding the analysis of quantum cybersecurity applications in unrelated domains, such as healthcare, manufacturing, or logistics.
- d. The study focuses exclusively on post-quantum cryptographic solutions and their implications for quantum computing. It does not assess conventional cybersecurity technologies unaffected by quantum advancements.
- e. The study considers only articles published in English, excludes articles in other languages, and is limited to publications from 2015 to 2024.

Expanding on the discussion of Blockchain integration with AI, this chapter discusses the revolutionary capabilities of Quantum Computing. It assesses the effect of quantum technologies on existing cybersecurity processes and the future of secure financial and accounting systems.

From a theoretical perspective, the challenges posed by quantum computing to classical cryptographic infrastructures can be understood through the lens of information security risk theory and long-term data confidentiality theory. Information security risk theory emphasises that organisational information systems must continuously adapt to evolving technological threats that compromise the confidentiality, integrity, and availability of digital information. In the context of accounting systems, cryptographic mechanisms form a fundamental component of financial data protection and audit reliability. However, advances in quantum computing challenge the underlying computational assumptions that secure widely used encryption methods such as RSA and Elliptic Curve Cryptography. Long-term data confidentiality theory further highlights the risk that encrypted financial records captured today may become vulnerable in the future once sufficiently powerful quantum computers emerge, a phenomenon often referred to as “harvest now, decrypt later”. Consequently, accounting information systems must adopt forward-looking cybersecurity strategies that incorporate quantum-resistant cryptographic mechanisms to ensure the long-term protection of financial data [138, 353, 355].

5.2. Literature Review and Theoretical Foundations

5.2.1. Fundamentals of Quantum Computing

a. Quantum Computing

The study [359] explains the concept of quantum computing and discusses the ideas of entanglement and superposition, which are derived from quantum mechanics and utilised in quantum computing, a novel form of processing that enables data handling in ways traditional computers cannot. Classical bits can only be 0 or 1, whereas quantum bits, or qubits, can exist in multiple states simultaneously. This potential offers significant advantages for solving problems that traditional computers struggle with, such as simulation and optimisation tasks. Quantum computing relies on manipulating quantum states that are both measurable and controllable.

In some cases, quantum computers can outperform traditional methods, as demonstrated by the development of quantum algorithms like Grover's algorithm for searching unsorted databases and Shor's algorithm for factoring large numbers. These algorithms significantly accelerate computations by leveraging the inherent uncertainty and probabilistic nature of quantum physics. The finance sector views quantum computing as a transformative technology that can enhance risk analysis, financial modelling, and optimisation. The study further explains that, by simulating complex financial systems and simultaneously examining multiple options, quantum computing can provide a deeper understanding of market dynamics and enhance financial decision-making.

b. Basic Building Blocks of Quantum Computing

i. Qubit

In quantum computing, [359] a minuscule object, similar in size to an electron or photon, is used by quantum computers to transfer the saved digital information into the system. Encoding can be done only in one-bit information, either zero or one, through the two orthogonal states of a microorganism. A quantum bit, often known as a qubit, being a two-state system, is the primary unit of information in Quantum Computing, just like a binary bit in classical or traditional computing.

ii. Superposition

The study [359] explains how the superposition works; he mentions digital computers that reduce all the data gathered into a string of bits, after which the logic gates are used in all calculations. So, if we talk about the state of the digital computer, then it is likely determined by its bits. So, if we want to talk about a laptop with n states, it can exist in any 2^n possible states. So what is superposition? Now, quantum computers use bits that simultaneously signify a linear mixture of zeros and ones together instead of one or zero.

iii. Entanglement

Two different entities' activities are linked by a phenomenon called quantum entanglement. The study has found that changes to one entangled qubit instantly affect the other, which one can say is necessary for quantum computing to function. It is possible to entangle pairs of qubits. It suggests that the two qubits reside in a single state. A foreseeable change in one qubit

immediately affects the other under such circumstances, and Quantum algorithms, designed to handle complex problems, use this connection. Unlike conventional computers, where doubling bits doubles processing capacity, quantum computers experience an exponential increase in power with each added qubit.

c. **Cryptography**

We are going to split the word cryptography, first considering the word prefix "crypt", which means "hidden," and the suffix "graph", which means "writing." The study [360] comprehensively defines the meaning and purpose of cryptography, explaining it as the study of secure, protected, and confidential transmission or communication techniques between two computers or parties. The study compares this mechanism with people's desire to communicate confidentially with themselves. They take steps and measures to prevent third-party invasion and reading their messages. The study [361] explains that nearly every encryption method used today is impacted by quantum theory. It uses mathematical algorithms and the algebraic structure of various protocols. It would not be wrong to say that it is the practice of securing information against possible adversaries who would obtain unauthorised access to confidential data if it were not for the mathematical guarantees of cryptographic systems.

❖ **Strategies for Cryptography**

In the modern era of computers, cryptography is frequently associated with converting plain text to ciphertext, text formatted in a manner that only the intended authorised recipient can decode, a process known as encryption. Decryption is the process of converting text from a cypher to plain text, as illustrated in Figure 5.1.

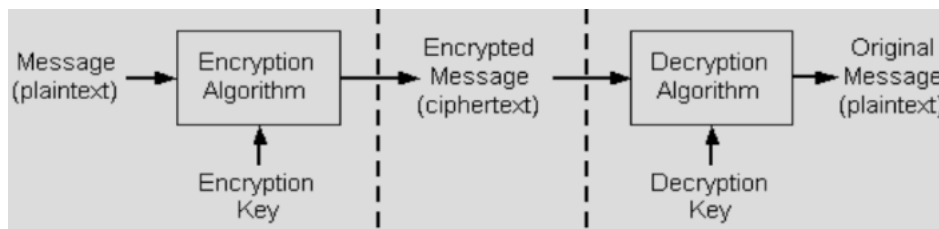


FIGURE 5.1 Process of Encryption and Decryption

SOURCE: [362]

Cryptography and coding are ways to secure data, communications, or information, limiting access to only authorised people who can receive or understand it. The process involves preventing unauthorised access to or invasion of data. Considering the cryptographic technique, we can interpret it as the safeguarding of data, information, or communication using codes, so that only authorised recipients can access it. So, we can say cryptography is a technique for preserving communications and information, ultimately preventing unauthorised access to confidential information. Figure 5.2 briefs the encryption and decryption algorithm classification.

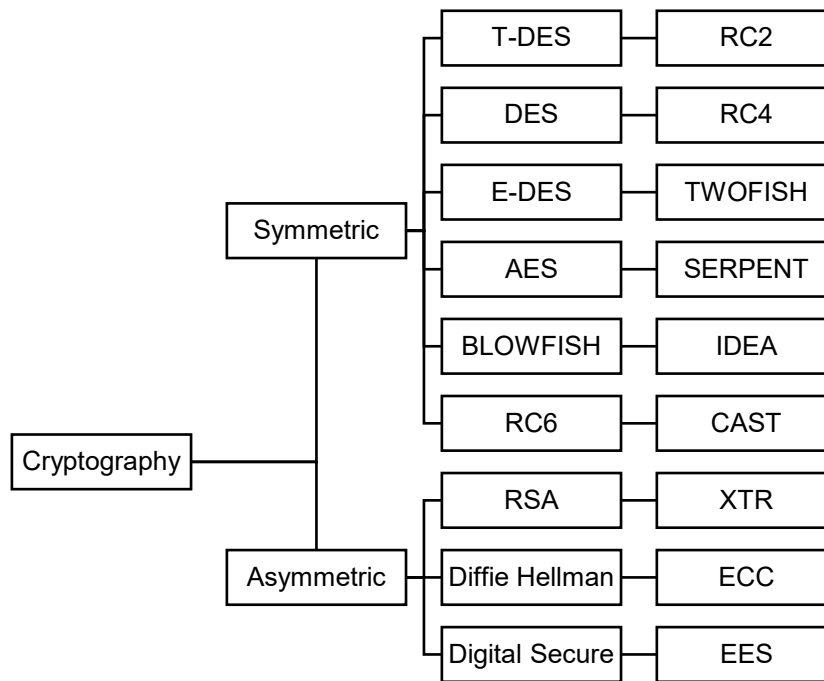


FIGURE 5.2 Classification of encryption and decryption algorithms

SOURCE: [362]

5.2.2. Prior Year Research

a. Cybersecurity in Accounting Research [352]

The authors [352] have elaborated on cybersecurity's vital role in safeguarding financial data in the accounting industry, which is examined in this study paper. As digital technology advances, accounting firms must implement robust cybersecurity measures to address the growing threat of cyberattacks. This research provides a comprehensive analysis of cybersecurity's role in protecting financial data within the accounting profession. This study thoroughly examines how top accounting firms, such as Deloitte, PwC, and EY, have incorporated cutting-edge cybersecurity technologies, including advanced encryption, blockchain, and artificial intelligence, into their daily operations. For instance, Deloitte has implemented advanced encryption to protect sensitive financial data, while PwC has integrated blockchain technology to enable secure, transparent transactions. The study takes a qualitative approach, gathering information through case studies and interviews with accountants, IT specialists, and industry experts. It then applies the literature review methodology to analyse the current state of cybersecurity in the accounting industry, considering changes in cybersecurity protocols over time, new developments in the field, and potential directions for future research. This qualitative study uses interviews with accountants, IT specialists, and industry experts, along with case studies, to gather information. The efficacy of multi-layered cybersecurity solutions in enhancing data security, mitigating breaches, and strengthening fraud detection capabilities is underscored by significant findings. Nonetheless, issues such as exorbitant operating expenses and the rapid development of cyber threats persist.

b. Innovative accounting methodology for ensuring the interaction of economic and cybersecurity enterprises [47]

This article [47] aims to position accounting as a novel, multifaceted system that enables the interplay between economics and cybersecurity in businesses. In addressing the growing cyber threats that affect economic security, the study highlights the vital role accounting plays in reducing these risks. The primary objective of this article is to formulate and propose an all-encompassing accounting approach that integrates economic and cybersecurity measures across different tiers. Reducing the financial impact of cyber threats requires updating accounting standards, improving the accuracy of accounting data, and ensuring efficient reputation management and communication. The gap identified by the authors is based on previous literature, where the previous study explored economic security and cybersecurity separately. Research is needed to identify an accounting approach that serves as the bridge between them. This paper has used various global datasets, namely the [363-365], to analyse the relationship between digital competitiveness across countries and their economic security. The researcher's methodology in this article is an institutional approach to evaluating the response to cyber threats through modernising accounting practices. Future research identified by the researcher emphasises the necessity of continuing studies into how accounting techniques might be continually modified to counter the ever-changing nature of cyber threats. The researcher suggests that one approach is to develop adaptable, responsive accounting procedures that can quickly adjust to emerging cyber threats. The study also noted the most significant losses, which are the hardest to calculate and are at the highest reputation level. Therefore, further research is needed to justify the financial impact of cyber threats adequately.

c. Cybersecurity and Prevention in the Quantum Era [354]

[354] The study pointed out the implications of quantum computing for cybersecurity at the 2nd International Conference for Innovation in Technology, explaining that, across several industries, cybersecurity could be revolutionised by advances in quantum computing. Because quantum computers can execute a wide range of calculations far more quickly than classical computers, they may be able to crack many currently thought to be safe cryptography schemes. As a result, the development of quantum computers has raised concerns about the security of current cybersecurity systems and the need to develop new, quantum-resistant cryptographic algorithms [366].

d. Quantum computing for finance: Overview and prospects [139]

The study [139] evaluates existing methods and future possibilities, discussing the potential applications of quantum computing in finance, including risk analysis, credit rating, and portfolio optimisation. It would have been interesting to examine how quantum technologies can be relevant to blockchain and cryptocurrencies. [159] Alternatively, to discuss quantum finance [367, 368], quantum money [369], the impact of quantum cryptography on the security of financial transactions [370, 371], and the applications of quantum simulators [372, 373] in

finance. The study focuses on the application of quantum computing in risk analysis, credit rating, and portfolio optimisation in the banking industry. Quantum computation offers the possibility of highly efficient algorithms that could provide exponential speed-ups for some technologically significant tasks compared to classical information processing. [374].

The study claims that quantum annealers can optimise portfolios, uncover arbitrage opportunities, and evaluate credit. Quantum amplitude estimation provides a quantum-mechanical approach to accelerating Monte Carlo sampling. The authors propose that researchers investigate the potential uses of malfunctioning quantum computers in finance before developing fault-tolerant quantum computing. The study explores deep learning in finance, quantum annealers, and quantum optimisation algorithms, and provides recommendations on how quantum machine learning might enhance these techniques. The authors caution that several experimental breakthroughs are needed before a universal quantum processor can surpass current supercomputers. They suggest that researchers explore the potential of quantum computing in finance.

Article Title	Research Question	Propositions	Identified Research Gap
Cybersecurity and Prevention in the Quantum Era [354]	RQ1, RQ2	Propositions 1 and 2	This article identifies the critical gap in the transition from classical to quantum-secure encryption infrastructure in finance and accounting systems. It highlights vulnerabilities in current systems exposed by Shor's and Grover's algorithms, showing that classical encryption (e.g., RSA, AES, ECC) will become obsolete. However, it lacks specific implementation frameworks or models for integrating post-quantum cryptography into organisational systems.
Cybersecurity in Accounting Research [32]	[32]RQ1, RQ3	Propositions 3 and 4	The article synthesises the literature but reveals a lack of research addressing how accounting systems can be adapted to withstand quantum-era threats. Specifically, minimal attention is given to integration challenges, protocol transitions, or organisational readiness for quantum-secure frameworks in accounting systems.
Innovative Accounting Methodology of Ensuring the Interaction of Economic and Cybersecurity of Enterprises [47]	RQ3	Propositions 3 and 4	This work underscores the impact of cyber threats on accounting quality but lacks a direct analysis of how quantum computing or quantum-safe measures can be incorporated into existing enterprise accounting methodologies. There is an evident absence of quantum-specific adaptation models or training frameworks for accounting personnel.
Quantum Computing for Finance: Overview and Prospects [139]	RQ2, RQ3	Propositions 1 and 4	While offering technical insights into quantum optimisation, machine learning, and amplitude estimation, this article does not bridge the gap into accounting-specific use cases. It lacks practical blueprints for integrating these algorithms into financial record-keeping, audit trails, or encryption frameworks used in accounting systems.

TABLE 5.1 Identified Research Gaps Mapped to Research Questions and Propositions

Additionally, they propose that imperfect quantum computers could have exciting applications before fault-tolerant quantum computing is achieved. The authors claim that quantum computing has the potential to transform the financial industry. They encourage scholars to

explore the potential applications of quantum computing in finance. The authors assert that quantum computing can revolutionise finance. They urge researchers to explore the potential applications of quantum computing within the financial sector.

Table 5.1 summarises the consolidated and reviewed literature, mapping the research gaps to primary and secondary research questions (RQ1–RQ4) and thesis research propositions (P1–P4) to ensure relevant coverage of the study objectives. The table provides further direction for study by demonstrating that the existing literature, to date, is insufficient in addressing numerous aspects related to quantum computing, cybersecurity, and accounting systems, including, but not limited to, vulnerabilities, quantum-resilient integration strategies, and institutional preparedness for financial quantum computing.

5.2.3. Critical Cybersecurity Threats in Current Accounting & Finance Systems

A review of recent literature and industry reports reveals several key cybersecurity threats and challenges facing accounting and finance systems today:

i. Data Breaches and Unauthorised Access

Unauthorised intrusion remains a primary threat. Attackers exploit vulnerabilities (such as weak passwords, software bugs, or social engineering of employees) to gain access to accounting databases. Once inside, they can exfiltrate sensitive financial information or manipulate records. For instance, ransomware attacks have targeted financial data, encrypting accounting files and demanding ransom payments. A recent report noted that ransomware is increasingly targeting not just to lock data but also to destroy backups, thereby threatening business continuity. The heavy reliance on digital records makes a successful breach catastrophic, resulting in significant financial losses and reputational damage.

ii. Weak or Outdated Cryptography

Many accounting systems use cryptographic protocols that are considered legacy or soon to be outdated. For example, the RSA encryption algorithm, widely used to secure data and digital signatures in financial applications, relies on the difficulty of factoring large numbers, a problem that quantum algorithms could solve efficiently. Similarly, elliptic curve cryptography (ECC), used in many secure authentication schemes, is vulnerable to future quantum attacks. The reliance on these algorithms is a ticking clock; once quantum computers reach a sufficient scale (often estimated to require thousands of logical qubits), they could break RSA/ECC encryption in feasible timeframes [375]. The literature highlights the concept of “Harvest Now, Decrypt Later” attacks, in which adversaries might steal encrypted financial data now (e.g., archived accounting records or confidential financial communications) and hold it. In the future, once they obtain access to a powerful quantum computer or quantum decryption service, they could decrypt that data, revealing years’ worth of sensitive information. This threat is particularly relevant for accounting records, which are often required to be retained for extended periods (due to auditing and compliance requirements).

Thus, even if such records are secure today, they may become exposed in a quantum-enabled future if not protected by quantum-resistant methods.

iii. Fraud and Anomaly Detection Limitations

Accounting systems increasingly employ data analytics and artificial intelligence (AI) to detect anomalies that may indicate fraud or errors [133, 141]. However, sophisticated fraud schemes may evade detection, and the computational demands associated with analysing large-scale transactional data and complex behavioural patterns can strain classical computing systems [219]. This introduces a critical limitation: existing systems may fail to identify certain fraud patterns in a timely manner due to processing constraints. While not a malicious “attack” in the traditional sense, this represents a significant cybersecurity vulnerability, as delayed or incomplete analysis may allow fraudulent activities to remain undetected.

Quantum computing has been proposed as a potential solution to address these computational limitations. Emerging research suggests that quantum algorithms, particularly in optimisation and machine learning, can process large datasets and complex probabilistic models more efficiently than classical approaches [72, 139]. In financial contexts, quantum-enhanced models have been shown to improve risk analysis, fraud detection capabilities, and decision-making efficiency by enabling faster exploration of high-dimensional data spaces [376]. Thus, quantum computing represents a prospective advancement capable of addressing current computational bottlenecks in accounting cybersecurity, particularly at the intersection of fraud detection and real-time analytics (RQ1 and RQ2).

iv. Third-Party and Supply Chain Risks

Modern accounting systems increasingly rely on integrations with external platforms, including banking APIs, cloud storage services, and third-party audit tools. Each integration point introduces additional attack surfaces and potential vulnerabilities, making system-wide security more complex and difficult to manage [219, 377]. As system complexity increases, ensuring consistent security across interconnected components becomes a significant challenge, particularly in distributed and cloud-based environments [378].

While quantum computing does not directly mitigate third-party or supply chain risks, it reinforces the importance of adopting a holistic cybersecurity approach. The integration of emerging technologies, including quantum computing, must be carefully managed to avoid introducing new vulnerabilities into existing ecosystems [139]. Furthermore, third-party providers themselves must adopt quantum-resilient security mechanisms, as weaknesses within external partners can compromise the entire accounting information system and create systemic cybersecurity risks [219].

v. Insider Threats and Human Factors

Cybersecurity threats are not solely technological; insider threats remain a critical concern in accounting and financial systems. Individuals with authorised access may intentionally or unintentionally compromise sensitive data, bypassing even advanced cryptographic

protections [379, 380]. Strong encryption, including quantum-resistant cryptographic methods, cannot prevent misuse of access privileges by compromised or malicious insiders. Addressing insider threats requires a combination of governance mechanisms, continuous monitoring, and behavioural analytics rather than purely technical solutions [141]. Emerging technologies, such as quantum random number generators and quantum-based authentication systems, may enhance security by improving unpredictability and strengthening identity verification processes [381]. However, human factors remain largely outside the direct scope of computational solutions, highlighting the importance of user training, system usability, and organisational cybersecurity culture to prevent misconfigurations and operational vulnerabilities [382].

5.2.4. Limitations of the Existing Literature Reviews

A key limitation of existing literature reviews is the failure to identify the intersection of quantum computing and cybersecurity in the context of accounting and finance. Currently, no reviews integrate these two domains and outline the unique implications, vulnerabilities, and opportunities for securing accounting and finance systems in the quantum era. It was pointed out that [383] lacks literature addressing the practicality of seamlessly integrating quantum computing technology with existing accounting and finance systems without disrupting ongoing operations. The transition from current systems to quantum-resistant alternatives has not been thoroughly planned or considered, and this process is expected to be quite complex. It was discussed [384] that despite being considered a promising field of study for enhancing data security, the literature does not identify and evaluate the most promising quantum algorithms for securing financial data. It has left an important question unanswered: which quantum algorithms are the best suited to achieving cybersecurity in the financial sector? The author [385] points out that the lack of common standards for comparing and assessing quantum systems is a significant drawback, making it difficult to evaluate the potential and progress of quantum computing platforms in an unbiased manner. This lack of standardisation also challenges the development of widely accepted quantum-resistant security measures. As noted in various studies, transitioning from current systems to post-quantum cryptography often requires substantial computational resources and a deep understanding of quantum technology. Additionally, the uncertain timeline for the arrival of large-scale quantum computers further complicates this transition. While theoretical advancements in quantum cryptography and quantum key distribution (QKD) are well-documented, few practical experiments and applications demonstrate how effectively these technologies can secure accounting and financial systems [385].

Although organisations are aware of these threats, there are gaps in their preparation for them. For instance, a KPMG study found that while most financial firms acknowledge the high-risk nature of quantum computing to data security, only about 25% have included quantum threats in their current risk management strategy [358].

This gap sets the stage for exploring quantum-resistant and quantum-based solutions in the next chapter. Before diving into those solutions, it is vital to recognise another current challenge: regulatory and compliance pressures. Financial data is heavily regulated (by laws such as GDPR for privacy, SOX for financial reporting integrity, etc.), and these regulations often mandate specific security controls. Regulators are beginning to recognise quantum threats; for example, government advisories in some countries have started recommending quantum-safe encryption for long-term sensitive data [386]. However, clear guidelines for integrating quantum technologies in standard compliance frameworks are still emerging. It creates a knowledge gap that academic research can help fill by providing frameworks and evidence on the practical viability of quantum cybersecurity.

5.2.5. Cybersecurity Frameworks and Quantum Threat Landscape

a. Classical Cybersecurity Frameworks in Accounting and Finance

Financial systems rely on well-established cybersecurity frameworks to ensure the confidentiality, integrity, and availability (CIA triad) of digital information. Commonly adopted frameworks include:

- NIST Cybersecurity Framework (CSF): Widely used for risk-based cybersecurity management across sectors, including finance.
- ISO/IEC 27001: International standard for information security management systems.
- COBIT and COSO: Control-oriented frameworks are often used in internal auditing and financial reporting governance.

These frameworks integrate encryption protocols, identity access management, firewalls, and incident response procedures to protect financial data. [387]. However, these models largely depend on classical cryptographic algorithms such as RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC). These rely on the computational difficulty of problems such as integer factorisation and discrete logarithms, assumptions that quantum computing can potentially break. [353, 387].

b. Quantum Threat Landscape

The advent of quantum computing fundamentally alters the security assumptions underpinning modern financial systems. Two primary quantum algorithms introduce new risks:

i. Grover's concept

[388] Searching an extensive database is a problem of paramount importance, with applications in a wide range of fields. Since the Grover search algorithm offers a quadratic speedup in the number of database queries, quantum algorithms can search a database significantly faster than classical computers. The Grover search algorithm is the optimal quantum search algorithm and can be used as a subroutine in other quantum algorithms. Searches with two qubits have been demonstrated on many platforms and proposed for others, but larger search spaces have been shown only on a non-scalable NMR system. The Grover search algorithm has four segments: initialisation, oracle, amplification, and measurement.

The initialisation stage creates a superposition over all states. The oracle stage marks the solution(s) by flipping the sign of the state's amplitude. The amplification stage reflects on the mean, thereby increasing the amplitude of the marked state. Finally, one measures the algorithm output.

ii. Peter Shor's concept:

The study [387] highlights that Peter Shor created the algorithm known as Shor's. He demonstrated that a quantum computer can factor in an integer N in polynomial time. According to [389], the precise real-time is $\log N$, where N is the number factored. The study [387] explains the significance of the algorithms, pointing out that they are significantly faster than the sub-exponentially fast, most efficient known classical factoring approach, and the discrete logarithm issues have also been demonstrated to be solved by quantum computers. In the article [390], the author discusses the construction of what [391] Pitowsky refers to as a "clever superposition" of entangled qubits. Extracting a solution in a brief or polynomial amount of time, the factoring algorithm developed by the author [353] is considered the most significant quantum algorithm to date. It can factor large integers (numbers) into their constituent primes. Shor's method can potentially breach RSA, the extremely broadly used public key encryption scheme on the Internet, in hours or days on a functional 100-bit quantum computer. When RSA public key encryption is scaled up to Quantum Kilo Bytes, it utterly fails. The study [390] explains that the Hidden Subgroup Problem (HSP) is a prominent class of quantum algorithms that includes Shor's algorithm. Variations of this issue have been found that theoretically answer the mathematics underlying the three primary public key encryption protocols now in use on the Internet: RSA, ECDSA, and DSA [392]. The study [390] explains that Quantum technologies are a severe threat to information security as they exist today.

While Shor's and Grover's algorithms demonstrate the theoretical capability of quantum computers to compromise classical cryptographic systems, this study does not assume that large-scale quantum computers are immediately available. Instead, the analysis adopts a probabilistic long-term risk horizon perspective. This approach recognises that although the precise timeline for cryptographically relevant quantum computers remains uncertain, encrypted financial records stored today may remain sensitive for decades due to regulatory and audit retention requirements. Consequently, adversaries may collect encrypted accounting data today with the intention of decrypting it once quantum computing capabilities mature, a scenario commonly referred to as "harvest now, decrypt later." From an accounting cybersecurity perspective, this probabilistic risk horizon justifies early preparation for quantum-resistant cryptographic systems to ensure the long-term confidentiality of financial records [138, 353, 355]. While lattice-based and hash-based cryptographic schemes are widely recognised as promising post-quantum cryptographic solutions, their adoption in accounting and financial systems is influenced by several institutional and governance considerations. The feasibility of implementation depends not only on the technical robustness of these algorithms

but also on organisational readiness, system compatibility, and regulatory compliance requirements. Accounting information systems operate within highly regulated environments governed by financial reporting standards, audit controls, and data protection regulations. Consequently, the transition to quantum-resistant cryptographic mechanisms must align with evolving international standard-setting processes, such as the National Institute of Standards and Technology (NIST) Post-Quantum Cryptography standardisation initiative. These governance and standardisation frameworks play a critical role in determining how and when quantum-resistant encryption schemes can be integrated into accounting infrastructures while maintaining auditability, interoperability, and regulatory compliance[138, 355, 393].

5.3. Conceptual Framework and Research Propositions

5.3.1. Justification for the Theoretical Lens

This study utilises a multi-faceted theoretical framework to investigate the adoption of quantum-secure cybersecurity measures within accounting and finance systems. The selection of theories is driven by the necessity to approach technology adoption from individual, organisational, and domain-specific perspectives. At the personal level, the study references the [190]Thompson et al.'s (1991) Model of Personal Computing Utilisation, which is a foundational framework for assessing user adoption of digital innovations. Six constructs adapted from information systems and contingency theory examine structural and cultural readiness within institutions, including task interdependence, technology, environment, structure, goals, and people.[394, 395] Additionally, in light of quantum computing's unique characteristics, the study introduces four quantum-specific constructs, two of which are original to this research: Quantum Resistance of Accounting Algorithms and Quantum Key Distribution (QKD) Integration. This layered framework offers theoretical comprehensiveness by linking established information systems adoption models with emerging quantum security considerations pertinent to financial systems.

5.3.2. Integrated Conceptual Framework of Finance and Accounting System Leveraging Quantum Computing-based Cybersecurity Strategies

The integrated conceptual framework encompasses three dimensions: (1) user-level constructs from [190]Thompson et al. (1991), (2) organisational-level constructs based on contingency theory, and (3) quantum-specific cybersecurity constructs. This design aims to comprehensively understand how quantum tools impact cybersecurity adoption in accounting settings. The framework has been refined through a systematic literature review following the PSALSAR methodology and visually depicts the dynamic relationships among these constructs. Each proposition in this study is assessed based on factors that ensure thematic alignment and theoretical relevance, grounded in theoretical precedent and empirical necessity.

a. User-Level Constructs: Technology Adoption Models

These constructs are grounded in [190] Thompson et al.'s (1991) Model of Personal Computing Utilisation, which has been widely validated in information systems (IS) research to understand individual attitudes and behaviour toward emerging technologies [189]. This adaptation explores how quantum computing can enhance data security, protect sensitive financial information, and improve system integrity and confidentiality. This model comprises six key factors, but we take more relevant perceptions: job fit, complexity, perceived consequences, and effect towards use. These constructs were later extended in models like the Unified Theory of Acceptance and Use of Technology (UTAUT) [396] and TAM 3 [397], which also prioritise user-centric adoption factors. In the context of accounting, user acceptance among auditors, accountants, and finance controllers is a critical prerequisite for the successful implementation of any cybersecurity framework. These factors are crucial in understanding how an organisation operates with the integration of AI into its system. The conceptual model for personal computing utilisation proposed by [190], of which we have mentioned the initial four factors, now we discuss the last two new factors integrated into this conceptual model: the first is the relationship, and the next is the culture. After integrating quantum computing into the cybersecurity system of accounting and finance, these factors are critical to analysing the organisational impact, concerns, and shifts due to the culture.

i. Job Fit/Job Performance

Job fit, for instance, involves assessing how quantum computing can enhance job performance and decision-making processes within an organisation. [190]The study defined job fit as a scale that measures an organisation's acceptance of introducing new technology, thereby enhancing job performance. We consider the same application for our quantum computing research in cybersecurity, specifically in accounting and finance. We need to consider quantum algorithms to analyse the job-fit factor. The most critical factor of accounting is financial information, and these algorithms have the potential to improve their precision and efficiency remarkably. Accountants can apply Quantum computing tools to optimise complex financial models, reduce errors, and streamline operations, thus improving job performance and lowering operational costs. Accountants and auditors may find these quantum tools more aligned with their job needs, particularly in big data environments, resulting in enhanced productivity and effectiveness.

ii. Complexity

Complexity, as the word describes, encompasses the perceived difficulty in understanding, applying, and managing innovations related to quantum computing, particularly when applied to big data and diversified information, much like applying new technology, as explained in the article [190]. Quantum computing must perform complex computations due to the quantum algorithm we have discussed previously, so it would not be wrong to say that they are complex and require complex mathematical foundations. So, we are considering integrating quantum-resistant algorithms with quantum key distribution (QKD). It becomes technically very sound

and a challenge to traditional cybersecurity frameworks. The steep learning curve associated with quantum technologies may require specialised training for professionals in accounting and finance, making it a potential barrier to widespread adoption despite its benefits.

iii.Perceived Consequences

According to [190], perceived consequences involve the belief that utilising a particular technology leads to beneficial outcomes, such as increased job satisfaction or efficiency. In the context of quantum computing, the perceived consequences in accounting cybersecurity include enhanced protection of financial data against future quantum attacks, reduced risk of breaches, and compliance with emerging regulatory requirements. Implementing quantum-resistant algorithms ensures long-term security, while QKD provides secure communication channels, enhancing the overall perceived benefits of adopting quantum technologies in accounting systems. Perceived consequences would focus on the potential outcomes and benefits of integrating quantum computing into operations management, such as improved efficiency and decision-making speed.

iv.Affect Towards Use

The study's [190] conceptual model factor affects the use of measures of emotional responses to technology, such as trust, satisfaction, or frustration. The integration of quantum computing into cybersecurity for accounting is likely to generate positive emotions among users due to its potential to provide unprecedented levels of security. For instance, quantum-resistant algorithms can offer a robust defence against even the most sophisticated cyber threats, instilling a sense of trust and reliability in the system. Similarly, QKD's ability to detect eavesdropping attempts in real time could lead to higher satisfaction and confidence in the security measures implemented. Affect towards use would capture the feelings and attitudes of individuals towards the utilisation of quantum computing, including the potential for joy and pleasure in leveraging advanced computational capabilities, as well as concerns about automation and job displacement.

v.Relationship/Social Factor

As discussed by [398], the relationship factor involves the interactions among rational decision-makers using game theory. In accounting cybersecurity, this could model the relationships between financial institutions, auditors, and regulators, where the potential benefits of quantum security measures influence each player's strategy. Therefore, it is accurate to say that it refers to the interaction between stakeholders within the technological environment, including employees, managers, and clients. Quantum computing could reshape these relationships in accounting by redefining how various stakeholders interact with and rely on cybersecurity systems. For example, adopting quantum-resistant algorithms and QKD could lead to new forms of collaboration and trust between financial institutions, auditors, and regulators. These stakeholders might need to develop new strategies and protocols to maximise the utility of quantum security measures, thereby strengthening the overall cybersecurity

ecosystem. Social factors would encompass the broader organisational and industry perceptions of quantum computing. At the same time, facilitating conditions would address the environmental factors that ease the implementation and use of quantum computing within an organisational context, such as investments in infrastructure and leadership support.

vi. Culture

Culture represents the collective values, beliefs, and behavioural norms within an organisation that shape how technologies are perceived, adopted, and utilised. In the context of accounting information systems (AIS), organisational culture plays a critical role in influencing cybersecurity effectiveness, particularly as financial systems become increasingly digital and interconnected [382]. A culture that prioritises cybersecurity awareness, innovation, and continuous improvement is more likely to support the adoption of advanced technologies such as quantum computing. Organisations with a strong security-oriented culture demonstrate higher levels of compliance, risk awareness, and proactive engagement with emerging threats, thereby facilitating the integration of quantum-resistant cryptographic mechanisms and secure data management practices [141, 219].

Moreover, the successful adoption of quantum computing in accounting and finance systems depends not only on technical capability but also on cultural readiness. This includes fostering awareness of post-quantum risks, promoting continuous learning, and embedding security-conscious behaviours across all organisational levels. As emerging technologies introduce new complexities, organisations must cultivate adaptive and informed cultures to ensure that innovations such as quantum-secure systems are effectively implemented and aligned with governance and compliance requirements [139]. Accordingly, culture acts as a foundational enabler that influences both the adoption and long-term effectiveness of cybersecurity strategies in accounting environments.

b. Organisational Constructs: IS/Contingency Theory Foundations

To expand from individual acceptance to organisational readiness, the model incorporates six constructs frequently applied in IS security adoption literature and Contingency Theory [395]:

i. Task Interdependence

Quantum computing enables faster, more accurate processing of complex tasks in accounting and finance. For instance, quantum algorithms can significantly accelerate Monte Carlo simulations, which are crucial for pricing derivatives. This process relies heavily on large amounts of interconnected financial data [399, 400].

ii. Technology

Quantum algorithms for amplitude estimation and quantum walks, in particular, can solve critical financial problems that break down in classical computing, including better financial modelling, risk assessment and simulation capabilities [399].

iii. Environment

This quick and efficient data analysis can also be applied in the financial world to enhance risk and uncertainty prediction, offering valuable insights into market fluctuations. Modelling financial uncertainties as quantum states leads to a more nuanced understanding of market dynamics. (Placing quantum finance on the agenda may also help to convince those wary of quantum technologies that there is more to gain from the metaphysical aspects of the quantum than they might otherwise think) [399].

iv. Structure

Financial institutions' organisational processes probably have to change and devise new components: new data pipelines and an end-to-end digital twin to assess how these quantum models were performed, allowing for more efficient and secure banking services[401].

v. Goals

The driving force behind quantum computing in finance is the promise of enhanced data security and computational efficiency. Quantum computing can enhance financial data security through quantum-resistant cryptographic techniques. Additionally, [401, 402] can enhance other computational tasks, such as credit risk computations and economic forecasts.

vi. People

Humans successfully oversee the use of quantum computing harnesses. Quantum technologies and cybersecurity must be applied and taught to finance professionals so they can use them correctly and effectively. Researchers, financial institutions, and regulators must closely exchange their ideas and expertise to ensure the appropriate deployment of emerging quantum technologies.

These dimensions are derived from studies on enterprise IS adoption, IT governance, and cybersecurity frameworks in the finance and public administration sectors. Their inclusion reflects that cybersecurity is no longer just an IT issue but embedded in organisational culture, processes, and policies.

c. Quantum-Specific Constructs: Emergent from Empirical Synthesis

The third layer, quantum-specific cybersecurity constructs, was first developed based on identified gaps in existing IS adoption models (which do not cover quantum cryptography or QKD), and secondly, through a Systematic literature review (via PSALSAR) of Q1 cybersecurity and quantum computing journals. Another basis is empirical propositions grounded in studies such as [403].

This dimension is novel and essential to this thesis because traditional IS frameworks do not account for post-quantum security implications, which directly affect the durability of encryption, audit trails, and financial compliance systems. These constructs include:

i. Quantum Resistance of Accounting Algorithms

The researcher [404] explains that quantum resistance refers to the robustness of cryptographic algorithms against quantum attacks, also known as post-quantum cryptography. As traditional encryption methods become less effective, quantum computers gain greater power in

accounting systems and may be vulnerable to quantum algorithms such as Shor's. Integrating quantum-resistant algorithms, such as lattice-based or hash-based cryptography, into accounting systems is crucial for maintaining financial data security. This factor emphasises the importance of forward-looking cybersecurity strategies that can withstand the potential threats posed by quantum computing.

ii. Quantum Key Distribution (QKD) Integration

The researcher [405] is considering the QKD technology, which utilises quantum mechanics to distribute cryptographic keys between parties securely. This method is unique in its ability to detect eavesdropping attempts, making it a highly secure means of communication. In accounting, integrating QKD into cybersecurity protocols could ensure that cryptographic keys to protect financial information remain safe, even in the face of quantum-enabled threats. This factor highlights the transformative potential of quantum technologies in enhancing the security infrastructure of accounting systems, making them more resilient against future cyber threats.

iii. Organisational Quantum Readiness

[406] Describes the degree to which institutions possess the infrastructure, digital literacy, and strategy alignment to pilot or scale quantum technologies [407]. Preparedness of the institution in terms of digital infrastructure, leadership support, and financial capacity to pilot or adopt quantum systems.

iv. Stakeholder Interdependence

[408] It highlights the necessity of coordination across finance teams, IT security units, vendors, and auditors to ensure policy compliance and the secure deployment of quantum tools. [409] Accounting cybersecurity depends on interaction among internal and external actors (CFOs, auditors, compliance, regulators, and IT vendors).

The modelling framework in this study incorporates user-level factors from [190] Thompson et al. (1991) and organisational-level constructs from the IS adoption literature, as well as newly identified quantum-specific constructs. These sixteen dimensions provide a framework for assessing the readiness, alignment, and impact of quantum-secure cybersecurity on accounting and finance systems. The model, as illustrated in Figure 5.3, captures how individual beliefs drive adoption and how institutional goals, team interdependencies, and stakeholder interactions enable or inhibit technological transformation. Quantum-specific constructs (QKD, post-quantum algorithm resistance) introduce new urgency to this sector's cybersecurity strategy.

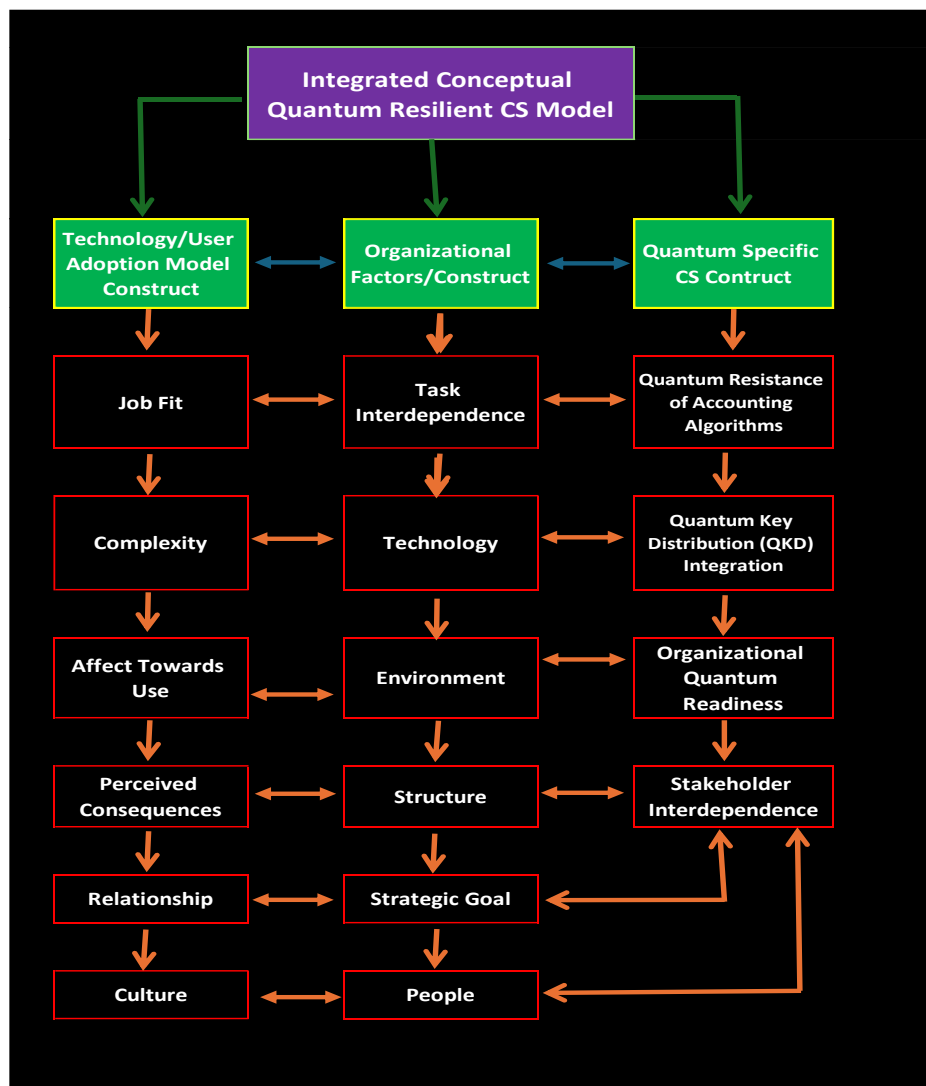


FIGURE 5.3 Integrated Conceptual Quantum Resilient Cybersecurity Model

Figure 5.3 illustrates the integrated conceptual quantum-resilient cybersecurity model developed in this study. The model demonstrates how quantum computing capabilities can be incorporated into accounting and finance systems to enhance cybersecurity across multiple dimensions. At the core of the framework are organisational and technological constructs derived from the adapted conceptual model, including job fit, complexity, perceived consequences, affect towards use, relationship, and culture. These constructs collectively influence the adoption and effectiveness of quantum-based cybersecurity mechanisms within accounting environments.

The model further depicts the interaction between classical accounting information systems (AIS) components and emerging quantum-enabled security layers. Specifically, quantum computing contributes through advanced cryptographic techniques, such as quantum-resistant encryption and quantum key distribution, which strengthen data confidentiality and integrity. These capabilities are integrated with organisational factors and external environmental conditions to form a multi-layered cybersecurity architecture. The framework highlights that the effectiveness of quantum-based solutions is not solely dependent on technological

superiority but also on organisational readiness, governance structures, and user adoption dynamics. Overall, the model provides a holistic representation of how quantum computing can be strategically aligned with accounting cybersecurity requirements to address current limitations and future threats.

5.3.3. Mapping the Integrated Conceptual Framework Factors to Research Objectives and Questions

The thesis's research questions and propositions are grounded in the integrated framework outlined above. Research Question 1, which investigates the relative security benefits of quantum computing over classical systems, draws upon the constructions of Quantum Resistance, Job Fit, and Technological Goals. Research Question 2, focused on unauthorised access prevention, is analysed through the lens of QKD Integration, Task Interdependence, and Structure. Research Question 3 addresses organisational adaptation and cultural shifts informed by the Concepts of Complexity, People, and Culture. Finally, Research Question 4 examines adoption barriers and long-term values, evaluating them using the Environment, Digital Readiness, and Perceived Consequences constructs.

5.3.4. Research Propositions

Based on the integrated conceptual framework presented in this study, four research propositions have been formulated to explore the implications of quantum computing on cybersecurity within accounting and finance systems. These propositions are grounded in theoretical constructions and thematic insights from the systematic literature review and conceptual synthesis. Each proposition reflects a distinct but interrelated domain of inquiry within the study's overarching objective.

a. Proposition 1

Quantum computing provides stronger encryption and security than classical systems in the fields of accounting and finance. This proposition examines the hypothesis that quantum technologies, particularly lattice-based post-quantum cryptography, can mitigate vulnerabilities inherent in traditional encryption protocols, such as RSA and ECC, which are widely used in financial record-keeping and audit trails.

b. Proposition 2

Quantum-secure cybersecurity frameworks will prevent unauthorised access and protect sensitive financial and accounting data from cyberattacks. This includes using Quantum Key Distribution (QKD) to establish mathematically secure, tamper-evident communication between stakeholders in accounting ecosystems.

c. Proposition 3

Adopting quantum-secure cybersecurity frameworks will necessitate significant adjustments to security protocols, professional training, and organisational culture. This proposition addresses the institutional and human capital challenges of transitioning to quantum-secure infrastructures.

d. Proposition 4

Challenges such as high costs, the need for specialised skills, and the complexity of quantum computing will initially hinder its widespread adoption in the accounting sector. However, the enhanced security benefits will eventually outweigh these challenges, especially as regulatory environments evolve and digital readiness improves.

While Quantum Key Distribution (QKD) offers significant theoretical security advantages by enabling the detection of interception attempts through quantum state disturbances, its practical implementation in accounting and financial systems presents several challenges. The deployment of QKD infrastructure requires specialised quantum communication hardware and dedicated optical transmission channels, which may not be readily compatible with existing enterprise network architectures. Furthermore, the cost of implementing and maintaining quantum communication infrastructure remains substantially higher than conventional cryptographic systems. These constraints are particularly relevant in accounting environments characterised by decentralised information systems, cloud-based enterprise resource planning platforms, and geographically dispersed audit operations. In such contexts, financial data are frequently accessed across multiple organisational locations and regulatory jurisdictions, creating additional complexity for integrating QKD-based security mechanisms. Consequently, while QKD represents a promising long-term cybersecurity solution, its adoption in accounting infrastructures may depend on future technological advancements, cost reductions, and the development of scalable quantum communication networks[138, 410, 411].

5.4. Research Methodology

5.4.1. Introduction

a. Systematic review

The author [412] explained that a systematic review gathers all empirical data that satisfy predetermined qualifying requirements to address a particular research topic. It employs precise, methodical techniques to reduce bias, resulting in trustworthy results from which judgments and conclusions can be reached [413, 414]. According to the researcher [415], a systematic review is a straightforward and dependable technique for synthesising scientific data to address a specific research question. Their objective is to consider all published data currently available on the subject and assess the quality of the material. The goal of the SR approach is to decrease the possibility of bias and improve transparency throughout the review process by relying on clear, methodical procedures to minimise bias in the selection and inclusion of research, assess the quality of the included studies, and provide an impartial summary of them [231, 416]. Another researcher [417] pointed out in their article that systematic literature reviews remain invaluable for scholars, propelling scientific advancement and well-informed decision-making throughout many fields. According to the researchers [418], the systematic literature review is an empirical technique for extracting significant

insights from the vast body of extant study literature. The researcher [419] emphasises the review protocol, which must be created, pertinent databases must be found, suitable search words must be developed, inclusion and exclusion criteria must be established, data must be analysed, and conclusions must be synthesised. These are just a few crucial elements in the process [420].

b. Meta-Analysis

The researcher [231] explains the Meta-analysis that integrates and condenses the findings of included studies through statistical methods. It is present in many, but not all, systematic reviews. By combining data from all the relevant studies, meta-analyses can yield more accurate estimates of the effects of the research data than individual studies included in a review.

[231]The study considered twenty-nine review writers, methodologists, doctors, medical editors, and consumers who developed the PRISMA Statement. In this study [421], an evidence-based minimum set of guidelines was detailed; the PRISMA Statement and its expansions seek to promote complete and transparent reporting of social return [223]. Another study [422] refers to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) Statement, the most widely used reporting standard for systematic reviews, which covers the literature search component [231].

5.4.2. Research Methodology adopted

The study [423] points out that the essential elements of systematic reviews are the exact and repeatable methods for selecting primary research publications, as well as the critical assessment and synthesis of studies that meet the eligibility criteria [424-426]. The research methodology to be adopted for performing this research is the same as explained in the article by Grover [189]. Grover chose to use a systematic literature review to answer his research questions. The thesis employs the same methodology to address the research questions regarding accounting-related cybersecurity based on quantum computing. The study [418] conclusions indicate that a systematic literature review may evaluate and synthesise all pertinent research on a particular research question, topic area, or phenomena of interest (SLR) [233]. This study follows a qualitative, interpretivist paradigm aimed at understanding the intersection of quantum cybersecurity and accounting information systems. A conceptual and theoretical inquiry was chosen to explore the emerging field where empirical data is limited, but theoretical foundations can still be rigorously constructed. The purpose of an SLR is to provide a reliable way to gather objective, reasonable, and unambiguous data on a study topic [427]. The Kitchenham and Charters [428] systematic review adheres to principles. According to them, a predetermined, rigorously adhered-to protocol lowers researcher bias and improves rigour and repeatability. Given the novelty of quantum computing applications in finance, the study applies a systematic literature review (SLR) as the primary method to identify, analyse, and synthesise existing scholarly knowledge.

5.4.3. PSALSAR Research Methodology

This systematic literature review in quantum accounting is being conducted using PSALSAR. This methodology was created in 2020, as detailed in this article [429]. The scholarly article mentioned that the framework for Search, Appraisal, Synthesis, and Analysis (SALSA) is a methodology that ensures methodological precision, systematisation, exhaustiveness, and repeatability in determining the search protocols that the systematic literature review (SLR) should adhere to [430]. According to Grant and Booth [431], two steps are added to the standard SALSA technique to create the new PSALSAR method, which employs six phases to conduct systematic literature reviews. Research Protocol (P) and Reporting Results (R) are the latest phases. The PSALSAR methodology is straightforward, portable, and repeatable. The study [430] further explained that this methodological technique was employed in most scientific works to mitigate the risk of publication bias and enhance the work's acceptability. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses [432] and the Search, Appraisal, Synthesis, and Analysis (SAS) framework were most commonly adhered to in the literature searches of review articles.

TABLE 5.2 shows the procedures adopted for this literature review on cybersecurity for accounting.

Steps	Outcome	Methods
Protocol	Defined study scope	Research Question, PICOC framework to be considered
Search	Define the search strategy	Searching strings
	Search studies	Search databases
Appraisal	Selecting studies	Defining inclusion and exclusion criteria
	Quality assessment of studies	Quality criteria
Synthesis	Extract data	Extraction template
	Categorize the data	Categorize the data on the iterative definition and ready it for further analysis work
Analysis	Data analysis	Quantitative categories, description, and narrative analysis of the organized data
	Result and discussion	Based on the analysis, show the trends, identify gap and result comparison
	Conclusion	Deriving conclusion and recommendation
Report	Report writing	PRISMA methodology
	Journal article production	Summarizing the report result for the larger public

TABLE 5.2 PSALSAR framework for systematic literature reviews

SOURCE: [430, 433]

This systematic study aims to provide an extensive overview of published, peer-reviewed works related to quantum accounting. The review framework is based on the PSALSAR model, which provides a structured process across planning, searching, appraisal, synthesis, analysis, and reporting stages. Using the Conceptual Framework, we address the aforementioned research questions through this process. We follow all these steps, as outlined in Table 5.2.

Step 1_Protocol

As shown in Table 5.3, the PICOC tool was used to complete the search procedure.

Concept	Definition	SLR Application
Population	The research work dealing with cybersecurity for accounting based on quantum computing.	Scientific research work on dealing with cybersecurity for accounting based on quantum computing, Research studies, academic papers, and technical reports focused on the application of quantum computing to enhance cybersecurity in accounting [145].
Intervention	Existing techniques are utilised to address the problem identified.	Incorporating quantum computing in the accounting field. Current cybersecurity techniques in accounting, such as encryption methods, and how they can be enhanced or replaced by quantum computing[72].
Comparison	Performing SWOT analysis.	Identifying the strengths, weaknesses, opportunities and threats of adopting quantum computing in accounting for cybersecurity. Comparing quantum computing methods with classical computing techniques in terms of effectiveness, scalability, and practicality for cybersecurity in accounting.[376]
Outcome(s)	Measure to assess the knowledge and gaps mentioned in the selected publications related to quantum-based accounting.	Identification of gaps in current research regarding the integration of quantum computing in cybersecurity for accounting and proposing areas for future study.[141]
Context	The particular settings or areas of the population.	Trends in cybersecurity for accounting based on quantum computing research, as well as related challenges and gaps. The specific contexts within accounting (e.g., financial data protection, auditing, fraud detection) where quantum computing could be applied to improve cybersecurity.[219]

TABLE 5.3 SLR research scope based on the application of the PICOC framework to the determined objectives

SOURCE: [430, 433]

Step 2: _Search

This stage includes the delivery and search strategy. To gather pertinent documents, the search strategy helps define a suitable search string and identify relevant databases. [433]. The researchers further explained in their article that using the search phrase to access the chosen databases and gather relevant literature is part of the search delivery stage. The search used two reputable and well-known databases: Web of Science and Scopus.

- **For Web of Science**, the search was done using the following:

QUANTUM (All Fields) and COMPUTING (All Fields) and ACCOUNTING (All Fields) and FINANCE (All Fields) or CYBERSECURITY (All Fields) and INFORMATION (All Fields) and Enriched Cited References and 2024 or 2023 or 2022 or 2021 or 2020 or 2019 or 2018 or 2017 or 2016 or 2015 (Publication Years).

- **For Scopus**, the search was done using the following:

(TITLE-ABS-KEY (quantum) AND TITLE-ABS-KEY (computing) AND TITLE-ABS-KEY (accounting) OR TITLE-ABS-KEY (finance) OR TITLE-ABS-KEY

(financial AND reporting) OR TITLE-ABS-KEY (cybersecurity)) AND PUBYEAR > 2014 AND PUBYEAR < 2025

The words were chosen to encompass as much scientific literature as possible on quantum computing, cybersecurity, accounting, and finance. Initially, the year of publication for both Web of Science and Scopus was considered for the last ten years from 2024.

Step 3: _Appraisal

The researcher [430] highlighted the appraisal phase, which is being considered; the chosen articles were assessed according to the goals of the review process. Screening the chosen literature to find pertinent papers for the review process was part of the research selection process. The two main phases are quality assessment and the selection of studies based on inclusion criteria. The studies were selected by applying the inclusion and exclusion criteria, as shown in Table 5.4.

Criteria	Decision
When the keywords exist in title, keywords or abstract section of the paper.	Inclusion
The paper published in a scientific peer-reviewed journal or article.	Inclusion
The paper should be written in the English language	Inclusion
Papars contain concepts relevant to objective of the research.	Inclusion
Provides information on CS or quantum theory related to accounting.	Inclusion
Papers that are duplicated within the search documents	Exclusion
Papers that are not accessible, review papers and meta-data	Exclusion
Papers that are not primary/original research	Exclusion
Papers written in languages other than English.	Exclusion
Grey literature, chapters, editorials,notes, letters, new items, surveys	Exclusion

TABLE 5.4 SLR study selection of literature using inclusion and exclusion criteria

Source: [430]

The papers underwent thorough screening to select the relevant articles for the review as part of the quality assessment process. Initially, the titles and abstracts of the detected records were reviewed, and papers that did not meet the inclusion criteria were excluded. Subsequently, the full texts of the remaining records were assessed for eligibility.

Step 4: _Synthesis

Furthermore, the researcher is considering the synthesis process, which involves extracting and classifying pertinent data from selected papers to develop information and draw conclusions. Extracting data from the selected articles entails identifying relevant information.

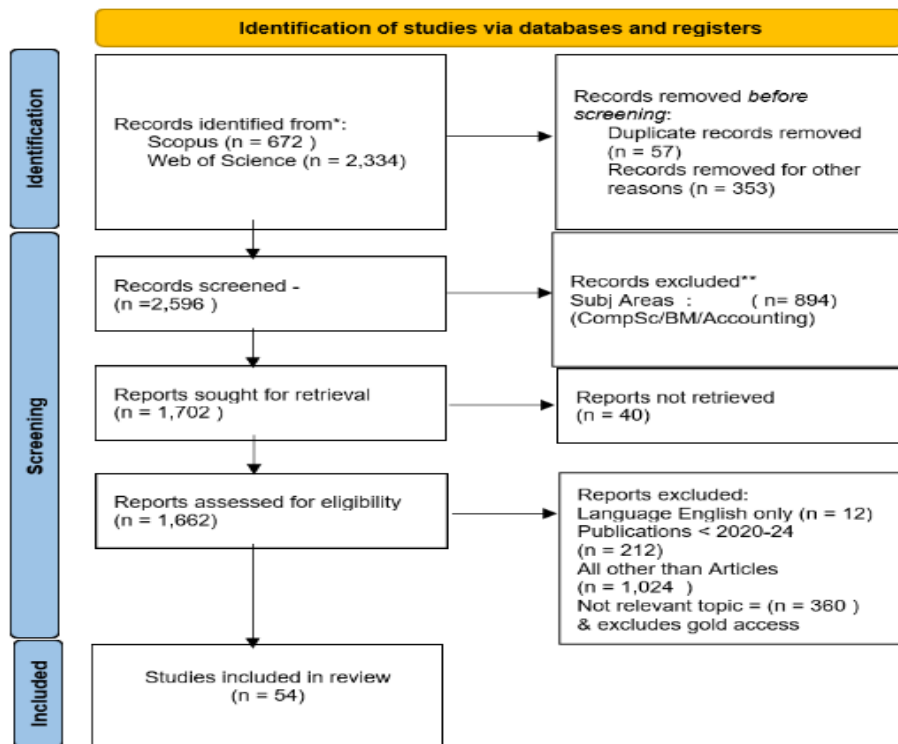


FIGURE 5.4 Prisma Flow Diagram

SOURCE: [430]

Two research databases were chosen: Web of Science and Scopus. From Web of Science, 2,334 documents and 672 from Scopus, a total of 3,006 documents were selected through the keywords described in step 2. Papers were extracted for further review. 57 duplicated papers were removed through website screening. Twelve documents in languages other than English were removed. Furthermore, 353 published journals were excluded according to the inclusion/exclusion criteria, and the remaining articles were retained for further review. The next step we took was to limit our articles to the last three years for publication; articles from the prior year were excluded, resulting in 212 completed articles. Publications that were articles were considered, eliminating the remaining publications by 1,024.

We also considered keeping articles with research areas in Computer Science and Business while excluding others, resulting in 894 additional articles being dropped from the final list. The total number of remaining articles is 454, which can now be assessed by screening titles. Titles without "Quantum" plus those not able to be retrieved will be excluded from the selection, resulting in 54 articles remaining as selected. The same has been detailed as per Figure 5.4.

Step 5 Analysis

The researcher's [430] consideration is the analytical step, which includes assessing the combined data, identifying significant material, and drawing conclusions from the chosen articles. The researcher's [430] understanding of the study's goal, the analyst's assessments,

and the researcher's comprehension of the research's level all influence analysis and result reporting. The Microsoft Excel spreadsheet was used for data extraction and analysis.

5.5. Results & Findings

This study posits that quantum computing holds transformative potential for the accounting and finance sector, particularly when analysed through our adapted version of [190] Thompson's Conceptual Model. The model's core dimensions, task interdependence, technological advancement, environmental adaptability, and organisational structure, are all positively influenced by emerging quantum technologies. Rather than treating quantum computing as a mere technological novelty, it should be viewed as a strategic enabler capable of reshaping decision-making frameworks, enhancing process efficiency, and securing financial data systems. When strategically implemented, quantum tools can strengthen the alignment between organisational operations and long-term financial goals. As evidenced in the following analysis of the four propositions, quantum computing supports the reconfiguration of internal processes, enhances adaptability to regulatory and market environments, and facilitates strategic outcomes in accounting and finance. This positions quantum computing as a critical lever for advancing resilience, precision, and agility in financial decision-making and information systems.

5.5.1. Results and Findings – Testing of Propositions

We adopt an integrated conceptual model. The hybrid theoretical framework synthesises multiple scholarly foundations to examine the four core propositions outlined in this study: Quantum Computing and Cybersecurity in Accounting and Finance: Current and Future Challenges and Opportunities for Securing Accounting and Finance Systems. Each proposition is evaluated using a targeted combination of these variables, selected for thematic alignment and conceptual relevance. This multidimensional approach enables a rigorous, context-specific analysis of how quantum computing is poised to impact cybersecurity practices in accounting and finance systems.

The evaluation of the research propositions in this chapter is based on thematic synthesis of the studies identified through the systematic literature review conducted using the PSALSAR methodology. Rather than statistical hypothesis testing, the propositions were assessed through qualitative analysis of peer-reviewed research addressing quantum cybersecurity, cryptographic resilience, and financial information systems. Evidence supporting or challenging each proposition was identified by analysing patterns across the reviewed literature, including theoretical discussions, empirical findings, and technological evaluations. The propositions are therefore interpreted as conceptually supported when multiple studies indicate consistent evidence aligning with the proposed relationships.

The supporting evidence for each proposition is analysed using the constructs identified in the integrated conceptual framework presented in Section 5.3. These constructs include user-level factors (e.g., job fit, perceived consequences), organisational factors (e.g., structure,

environment), and quantum-specific cybersecurity constructs. Each item listed below represents a thematic dimension derived from the conceptual framework and supported by findings from the reviewed literature.

a. Proposition 1

Quantum computing offers significant advancements in encryption methods, enabling more effective prevention of cyberattacks on accounting systems compared to classical computing.

Proposition 1 is supported by evidence from the systematic literature review (PSALSAR method), focusing on how quantum computing enhances cybersecurity through quantum-resistant encryption techniques and Quantum Key Distribution (QKD).

This proposition maps the following components of the integrated conceptual framework:

i. Job Fit/Job Performance:

Articles by [384, 434] emphasise that quantum-secure encryption tools, such as lattice-based post-quantum cryptography (PQC) and Quantum Key Distribution (QKD), align well with key accounting functions, including audit trail protection, ledger verification, and secure inter-departmental financial reporting. Job relevance is established in scenarios like post-quantum audit verification and secure cloud bookkeeping.

ii. Quantum-resistant encryption:

Over time, quantum computing could bring quantum-resistant encryption into the mainstream, allowing accountants to learn how to apply it, and new tools will make it easier to use. Hybrid models are emerging, combining classical encryption for ease of use with quantum protocols for secure key distribution, suggesting increasing accessibility [435]. [436] It has been noted that quantum encryption introduces higher mathematical complexity and infrastructure burden. While secure, implementation requires specialised skills, posing adoption barriers in mid-size accounting firms.

iii. Perceived Consequences:

More crucial is the role of quantum computing in providing much more effective encryption regimes, such as Shor's algorithm, which can rapidly crack any existing classical encryption scheme. It enhances the effectiveness of quantum encryption in securing accounting systems. Quantum computing enables cryptographic protocols (e.g., QKD) that are provably secure and immune to computational attacks, making it a superior choice for accounting data protection [437]. [354] show that quantum threats (e.g., from Shor's algorithm) can break RSA-based encryption. Thus, failing to adopt quantum-secure protocols may result in irreversible financial data breaches.

iv. Attitude Toward Use:

However, as organisations become more aware of the threat of quantum-capable cyberattacks, positive attitudes towards quantum-based encryption emerge. Increasing awareness of

quantum threats fosters proactive attitudes towards adopting quantum cryptographic methods [438].

v.Behavioural Intention to Use:

Quantum encryption technologies will eventually become a firmly entrenched intention for accounting firms as the threat of future quantum hacking turns from fictional into fact. Institutional momentum is building toward post-quantum transition, with initiatives already launched in the financial and defence sectors rising [439].

vi.Relationship/Social Factors:

[383] Highlight regulatory pressure (e.g., NIST PQC call) driving social and professional urgency to adopt quantum-ready security. Peer pressure within the finance industry is also increasing.

vii.Organisational Structure:

Governments, academic research activities, and software companies collaborating to provide resources and allow technology adoption would best serve quantum encryption. Global collaboration across academia, governments, and tech companies is accelerating the research and deployment of quantum-secure systems [440]. Accounting firms must revise protocols and approval chains to support decentralised, quantum-hardened verification systems [441].

viii.People:

Not only do accountants recognise cybersecurity's importance to confidential accounting data, but firms that innovate by following technology trends also turn to quantum-resistant encryption. Adoption is driven by a sense of urgency across institutions aware of the quantum threat, with early adopters (e.g., financial institutions) expected to set industry norms [437]. A lack of post-quantum cybersecurity skills remains a bottleneck. Most accounting personnel lack awareness of PQC constructs like NTRUEncrypt or CRYSTALS-Kyber [442].

ix.Strategic Goals:

Across studies, organisational goals include fraud prevention, data sovereignty, and reduced forensic costs. Quantum-secure encryption aligns better with these goals than classical encryption due to its provable security guarantees under quantum threat models [383].

x.Organisational Environment:

Companies in the finance and accounting industries operate in heavily regulated environments where data security is a central organisational imperative and under relentless pressure to make their data even safer. Furthermore, they can use quantum encryption. Regulatory pressures accelerate this organisational imperative. Much has been written about how quantum computing might be dangerous for conventional encryption. However, one transformative capability that a quantum computer enables is quantum cryptography (called this because it makes use of a quantum process to send messages that cannot be eavesdropped upon). This exciting new field is moving very fast, and in a few years, it may be hard to keep up with all the latest developments. Financial and government institutions are under increasing pressure

to adopt QKD and post-quantum cryptography to maintain secure data transmission as quantum threats rise [439]. Regulatory bodies like NIST are standardising quantum-resistant algorithms, enabling industry-wide adoption [435]. Articles like [47] [443] note that financial systems increasingly operate in cross-border digital environments, raising security stakes. QKD ensures integrity in such distributed, multi-agent accounting ecosystems.

xi.Quantum Resistance of Accounting Algorithms:

Such algorithms must be re-engineered and made quantum-proof, answering the need for more secure accounting software storage. Financial data stored in this way enjoys the most robust possible defence. This factor emphasises the need to develop and subsequently use quantum-resistant algorithms designed specifically for accounting systems. These algorithms shield against potential quantum cyberattacks, as no quantum computer surpasses them and falls prey to a malicious agent. Multiple studies confirm that classical algorithms are vulnerable to quantum attacks, necessitating quantum-resistant upgrades for financial systems [437]. [354] [444] confirms that quantum computers can break RSA, ECC, and SHA-256. Studies promote lattice-based schemes (e.g., Kyber, Dilithium) as replacements. There is a strong consensus that quantum-resilient cryptography must replace classical algorithms in financial systems.

xii.Quantum Key Distribution (QKD) Integration:

QKD offers an unbreakable, secure, essential exchange that is also secure against quantum computers. It considerably increases the security of accounting systems. QKD ensures secure key exchange and prevents eavesdropping, even from quantum-enabled attackers [405]. Quantum computing brings new kinds of robustness to the efficacy of encryption against cyberattacks. Undeniably, [445] quantum computing becomes more promising with the effort being dedicated by world governments and the comprehensiveness of quantum-resistant cryptographic solutions. We do not envisage the quantum revolution outpacing the development of quantum-resistant cryptography, but the end of our current era threatens sooner rather than later. [384] QKD ensures secure key exchange over quantum channels, even in adversarial settings. QKD supports end-to-end confidentiality for interbank reconciliations and decentralised ledgers.

xiii.Organisational Digital Readiness:

Empirical studies [47] confirm that firms with advanced cloud systems and in-house IT security are significantly more prepared to adopt post-quantum tools.

xiv.Stakeholder Interdependence:

As finance increasingly involves coordination among accountants, auditors, tax consultants, and regulators, QKD enables secure multi-party transactions and real-time signature verification [443].

In conclusion, quantum computing has made a breakthrough in encryption, making it harder for cyberattacks on accounting and financial systems than classical computing. Hence, this research is important and relevant at the current time due to the ongoing research and

development in quantum computing. Quantum computing indeed holds the potential to revolutionise encryption methods in computer systems and lead to better cybersecurity. For this reason, this view aligns with the main topic: Quantum Computing and Cybersecurity in Accounting and Finance.

b. Proposition 2

Integrating quantum computing into accounting practices mitigates risks associated with data breaches and unauthorised access to financial information.

Proposition 2 examines whether quantum-secure cybersecurity frameworks can prevent unauthorised access to financial information. Evidence from the reviewed literature indicates that technologies such as Quantum Key Distribution (QKD) provide mechanisms for secure key exchange and interception detection. For example, several studies highlight the ability of QKD protocols to detect eavesdropping attempts through disturbances in quantum states, thereby enhancing the confidentiality of financial communications.

i. People:

Accountants and IT professionals may need to upskill and reskill to work with quantum computing technologies. Quantum computing has security implications in cybersecurity processes. Integrating quantum computing into practice settings introduces tensions and challenges to accounting and cybersecurity professionals. Professionals in accounting and IT must upskill in quantum concepts to safely adopt these technologies. Quantum computing integration causes interdisciplinary tension but opens pathways for secure innovation in financial data handling [404].

ii. Quantum Key Distribution (QKD) Integration:

In addition, integrating QKD into the accounting systems ensures that the encryption keys used to protect financial information are shared via a secure channel that cannot be intercepted by a third party (such as a hacker), which means that even if an attack occurs, the information remains safe. Thus, accounting systems that integrate quantum computing are less vulnerable to attack via malicious programs or human intervention, making financial data more secure. In conclusion, [445] integrates QKD into accounting systems, offering secure communication channels that are accountable, traceable, and security-based in financial transactions. Quantum cryptography and QKD are already being applied in high-security sectors to ensure data integrity and detect eavesdropping related to securing accounting systems [446].

iii. Perceived Usefulness:

Implementing quantum algorithms such as Grover's algorithm is much more secure than all currently available encryption methods and is a vital safeguard against infiltration approaches, both in security and speed. Quantum Key Distribution (QKD) is precisely what accounting jobs require to secure financial data from ever-evolving cyber threats. It significantly enhances the applicability of quantum computing to accounting and cybersecurity jobs. Studies show that Grover's algorithm and QKD outperform classical encryption and key distribution

methods. These are mission-critical safeguards against cyberattacks in data-rich sectors like accounting [447].

iv. Complexity:

The software's technical complexity could be a barrier. However, once user-friendly platforms and interfaces are developed, perceived ease of use likely decreases the accountants' learning curve. Researchers acknowledge that technical barriers currently exist. However, trends point to ongoing simplification through standards, platform development, and guided frameworks for integration [404].

v. Relationship:

Sophisticated new cyberattacks have prompted significant industry bodies and financial regulators to endorse the use of quantum technologies to mitigate risks. Quantum encryption techniques, which are based on quantum mechanics, may initially seem intimidating. However, their capacity to enhance security could simplify the administration of cyber threats, making covert attacks more difficult. The global rise in cybercrime and regulations such as GDPR and financial data mandates drive organisations to seek quantum-secure methods, as seen in parallel sectors like healthcare [446].

vi. Environment:

Cooperation between quantum computing researchers and accounting software vendors can facilitate the integration of quantum solutions. Improved data security due to quantum encryption can increase stakeholders' confidence in the safety of accounting systems. There is documented cooperation between research bodies, accounting scholars, and quantum technologists to create frameworks for quantum-resistant integration into business practices [404].

vii. Attitude Towards Use:

The continuously evolving, sophisticated techniques hackers employ create a positive attitude toward using quantum solutions. Accounting professionals must be positive about adopting quantum encryption if they know its advantages. So, the result is a boost in confidence that quantum technology is more secure than classical techniques. Increasing recognition of quantum computing's potential to counteract sophisticated cyber threats drives positive perceptions among tech-savvy accounting professionals [448].

viii. Culture:

A culture that prizes innovation and security hastens the diffusion of quantum encryption methods; accountants who see cyber threats are likely to act preemptively. A proactive culture of innovation and compliance in finance firms accelerates the adoption of secure, traceable, quantum-safe methods for financial recordkeeping [449].

ix. Organisational Structure:

If accounting firms have suffered a breach or learned of other firms' deployment of quantum-safe practices, their intention to use quantum-based systems escalates. Integrating quantum

computing creates a new interdependency between accountants and IT professionals, who work together to ensure encryption technologies are in place. Historical breach cases and regulatory trends suggest that firms exposed to quantum-safe use cases or targeted by cyberattacks move swiftly toward integration [446].

x. Perceived Consequences:

Studies such as [354, 443, 450] emphasise the financial and reputational damage from data breaches in accounting systems.

xi. Quantum Accounting Algorithms – Quantum Resistance:

A quantum-resistant algorithm secures the integrity and secrecy of accounting activities, protecting accounting records against potential damage from future quantum threats. The researcher highlighted that the present cybersecurity processes in the financial system could not resist more advanced cyberattacks [451], and this could be achieved by quantum computing, which provides more secure encryption.

Specifically, ongoing work by the commenters and those associated with the Netscalibur project [401]. The initiative promotes communication and collaboration among researchers, financial institutions, and regulatory bodies to develop robust quantum technologies for the financial sector. It includes further consideration of appropriate quantum encryption techniques for accounting systems.

Practical Implications:

The quantitative description of cybersecurity structures, processes and relational mechanisms outlined above helps to explain how publicly listed firms handle cybersecurity-related events [451]. Mutual interactivity while implementing strategies enables consultation with quantum computing, which can improve the cybersecurity posture of the accounting strategy mentioned above.

To summarise, a robust quantum computing approach to accounting courses helps to minimise the risk of data breaches and unauthorised access to financial data.

c. Proposition 3

Adopting quantum computing in accounting requires substantial changes in cybersecurity protocols, but leads to superior financial data protection:

To effectively apply quantum computing to accounting, we must overhaul our cybersecurity processes entirely. However, we are protecting our financial data more securely. Applying the Integrated Conceptual Model to assess integrating quantum computing into accounting and finance, here are the findings:

i. Technology Implementation:

Accepting quantum computing requires a profound overhaul of currently used cybersecurity measures. Businesses and governments must complete various tasks, from establishing new quantum-safe encryption standards to upgrading IT infrastructure and training personnel to use quantum technologies. Quantum computing introduces disruptive encryption capabilities

requiring firms to redefine cybersecurity architectures, from network protocols to data storage systems. The study argues for industry-wide deployment of quantum-safe cryptography like lattice-based systems and post-quantum RSA alternatives [452]. Overhauls include new cryptographic standards, hardware upgrades, and skilled personnel capable of handling post-quantum algorithms. [453].

ii.Task Interdependence:

How financial information is processed and protected also changes. Quantum computing opens up new possibilities for encryption, storage, and data transmission, which must be integrated into accounting workflows. Quantum-enhanced systems redefine financial information workflows, especially where encryption, storage, and verification intersect. New protocols require deeper integration with AI-driven anomaly detection and QKD-based communications [454].

iii.Quantum Resistance of Accounting Algorithms:

This is one of the reasons why we need to develop quantum-proof accounting algorithms. These algorithms would necessitate changes to cybersecurity implementations, resulting in superior protection of a business's financial data on the Internet. Security is improved when classical accounting systems are embedded with quantum-resistant encryption, which enhances protection against future quantum attacks [404].

iv. Perceived usefulness:

Although new protocols are needed to make quantum-safe accounting viable, quantum computing provides enhanced security against cyberattacks and breaches, making it a desirable option for accounting. So, it would seem sensible for accounting to invest in new, radically secure options, such as quantum computing, to continue fulfilling its roles. Quantum computing enhances the fit for accounting roles by helping the profession move toward enhanced, quantum-safe security, which addresses problems more effectively. Studies affirm that QML, QKD, and lattice-based cryptography offer more secure, traceable, and unbreakable encryption for financial data, making quantum adoption highly attractive for accounting professionals [454].

v.Complexity:

It initially feels somewhat challenging to implement, as it involves training and upgrading cybersecurity infrastructure, which is likely to be less than smooth. However, the benefits can be long-term and obvious once in place. Combining quantum technologies can be complicated, but the initial technical work can be completed once the learning curve is overcome. Although initial integration is complex, frameworks and standards are emerging to help firms adopt quantum security protocols with minimal disruption [404].

vi. Environment:

Competitive pressures from global regulatory bodies and peer firms in the industry drive a sense of urgency to adopt new cybersecurity protocols. In turn, accounting professionals

believe that ‘the tide is turning’ toward QC computing, with a surge in their perception of benefits in risk mitigation, resulting in a very positive outlook for deploying these new technologies. A change-oriented culture and culture of innovation adopt new protocols to enhance the societal security drive. Encouraging adaptive virtues leads to a significant improvement in overall security resilience. Regulatory mandates and industry shifts foster urgency across financial sectors to transition to quantum-safe systems. Global finance leaders are beginning to set this trend, driving widespread adoption [455].

vii. Organisational Digital Readiness:

Establishing government policies and corporate investment in quantum computing research and development (RD) helps facilitate the transition to quantum-based cybersecurity. IT and accounting professionals must work more closely together on each task, hopefully establishing closer working relationships. Multiple papers advocate for interdisciplinary collaboration between quantum scientists, IT departments, and financial regulators to enable successful cybersecurity transformation [456].

viii. Attitude toward Use:

As accounting firms experience tremendous success with quantum-enhanced cybersecurity protocols, they adopt a positive attitude towards their use. Over time, with proper training, many accountants come to embrace these new technologies, which provide an effective layer of protection for their data storage. Perspectives may initially start as either scepticism or fear. However, with the proper use of positive reinforcement and notable examples of success, they could shift in a more positive direction, promoting the adoption of new protocols and enhancements. Positive attitudes toward quantum cybersecurity are rising, particularly in firms that experience firsthand benefits or recognise quantum threats as imminent [457].

ix. Organisational Structure.

The firms invest in quantum cybersecurity posts, acknowledging that the attacks are now quantum-based and companies should get QCS for adequate protection. Organisational culture is risk management-centric, giving more weight to the accuracy and impeccability aspect of QCS adoption, conveying that sensitive and confidential information should be safeguarded impreguably. Firms with prior breach experience or security-focused cultures already intend to shift towards quantum protocols and encryption technologies [458].

x. Integration of Quantum Key Distribution (QKD):

Integrating quantum key distribution is crucial in developing future cybersecurity protocols, as it provides secure communication channels for accounting systems. Ensuring secure communication channels by integrating QKD methods lessens the overall risk of these systems. QKD also require changes in the communication protocol being used, supporting progress in the evolving nature of more secure accounting systems. Quantum key distribution is key to building next-generation accounting communication protocols that are verifiably secure and cannot be eavesdropped upon [452].

Moving to quantum computing means that many changes occur in terms of cybersecurity. It involves making the financial data infrastructure quantum-resistant (including replacing basic cryptographic techniques with quantum-safe algorithms) and utilising QKD, which requires reviewing and updating current security measures. However, the new protocols have the advantage of providing better financial data protection against current and future quantum threats [445].

d. Proposition 4

Challenges such as high costs, the need for specialised skills, and the complexity of quantum computing initially hinder its widespread adoption in the accounting sector. However, the enhanced security benefits eventually outweigh these challenges.

i.Job Fit: Currently, the skills mismatch between accountants and quantum computing results in a job mismatch [459]. Over time, quantum capabilities will be increasingly embedded in accounting tools, enhancing job fit and performance.[460].

ii.Complexity: Firstly, the cost and complexity of quantum computing, not to mention the paucity of skilled professionals, are severe impediments to using quantum computing in accounting's usual ways. However, as the technologies concerned mature and become more accessible, is it safe to assume that security gains drive their use despite initial obstacles? Quantum adoption is hindered by high financial costs, lack of talent, and limited infrastructure, especially in developing markets [461]. However, security and computational advantages drive widespread uptake as technologies mature [462].

iii.Organisational Characteristics: Firms must conduct a cost-benefit analysis when considering whether to invest in quantum computing, should it become available soon. The capital outlay can be significant, but the longer-term benefit of enhanced security – or perhaps more accurate compliance with the coming regulatory standards – is considerably more critical than the initial outlay. Firms are advised to weigh short-term cost hurdles against long-term benefits in terms of compliance, accuracy, and risk mitigation [463]. Adoption is considered a strategic investment, not just a technological one [464].

iv.Quantum Key Distribution (QKD) Integration: As QKD becomes reliable and costs decline, investment in new accountancy technology and human-resources training ensures its superior security is widely used until the initial barriers are overcome. QKD is initially costly and complex but ultimately enables secure, quantum-resilient communication channels critical for sensitive financial systems [465].

v. Perceived Ease of Use: Today, quantum systems are relatively complex to understand, which requires highly skilled workers to operate them, and these skills are also in short supply. These are all barriers, but they decrease over time as quantum tools come to hand and workers' literacy in quantum matters improves. Complexity offers a notable obstacle to initial adoption, where it is difficult for firms to assess how to incorporate quantum technologies into their operations. High initial complexity is one of the most significant barriers to adoption [459].

User-friendly platforms and training programs are needed to lower the entry threshold over time [460].

vi. Environment: Commercial adopters in the financial and accounting profession, followed by their peers, cascade, reducing the cost of adoption by taming the resistance quotient and demonstrating quantum value. Resistance to change in a change-averse culture restricts first-mover adoption. However, awareness campaigns and success stories can gradually influence the norms to move towards acceptance and encourage innovation over time. The problems identified also make the collaboration between accountants and technologists stronger, as they need to bring each other up to speed to overcome the initial adoption hump. Adoption is slow initially, but peer pressure, industry leadership, and regulatory mandates likely accelerate acceptance and standard-setting [466].

vii. Technology Adoption: Governments and educational institutions must provide access to quantum computing skills by providing laboratories and study materials, and offer further incentives (on top of expected market forces) to drive adoption and help realise the potential benefits. Studies highlight the need for government-led quantum initiatives, education, and infrastructure to reduce friction and democratize access [461].

viii. Attitude Towards Use: Security requirements progressively overcome the entrenched resistance to the costs and complexity of quantum computing. As organisations begin to observe the successes of quantum-enhanced security, resistance to cost and complexity is reduced, fostering optimism [467].

ix. Organisational Quantum Readiness: The adoption of quantum computing in accounting increases as firms realise its apparent security benefits and gain a competitive advantage despite resistance to these quantum computing applications due to concerns about costs and complexity. Evident resistance due to costs and complexity may initially be present (or, perhaps more realistically, apathy), but the positive outcomes of early adopters can boost industry confidence and enthusiasm. Companies are already preparing for adoption by investing in research pilots and quantum readiness audits [463].

x. People: Accountants and IT specialists need to develop a basic understanding of quantum mechanics. Cross-discipline cooperation and upskilling solutions are needed to close this skills gap and enable safe implementation [404].

xi. Culture: An innovation and cybercrime-aware culture supports the active uptake of quantum technology in pioneering companies. Tech-savvy and compliance-oriented accounting organisations will be most open to uptake [449].

The costs to set up and maintain these processes within the accounting industry include the skills gaps in managing quantum computing and the difficulty of adopting quantum computing without calculating conventional and more secure encryption and Key Distribution. However, there is no reason why such value from quantum computing cannot outweigh the barriers in time and why these essential capabilities cannot be created and adopted as accounting becomes

easier and more accessible for the industry. In the future, determine how Quantius courses are based on today's skills for tomorrow's jobs [445].

5.5.2. Discussion – Answers to Research Questions

The findings are summarised from the proposition-based analysis and extensive literature-based theme review to answer the study's research questions directly. The findings reflect how quantum computing and its technologies are shaping accounting and finance systems' present and future cybersecurity status concerning the theoretical constructs developed in Section 5.3.

Research Question 2: How secure can quantum-secure cybersecurity frameworks prevent unauthorised access to sensitive financial and accounting information? QKD offers provable eavesdrop resistance even in the presence of quantum attackers [445, 446]. Advanced quantum cryptographic systems provide secure multi-party accounting communication layers [443]. Grover's algorithm supports secure authentication and authorisation systems as a means of preventing illegal access [447]. Deploying immutable audit trails via QKD and blockchain systems ensures the integrity of accounting records [383]. Empirical evidence suggests that accounting systems with integrated QKD are more effective in detecting illegal intervention than classical models [452].

Research Question 3: What changes must be made in the accounting and finance departments regarding the organisational and structural dimensions to implement quantum cybersecurity systems? Firms need to redefine their cybersecurity governance structures to incorporate quantum-safe protocols [453]. Cross-functional teams must be established, consisting of accounting, IT security, and compliance professionals [460]. Accounting personnel need specific training in quantum cryptography principles and quantum-resistant audit procedures [404]. Business workflows need to be rearchitected to include QKD key management procedures, quantum-safe signature verification, and advanced anomaly detection [454]. A culture of continuous innovation and compliance in cybersecurity will be necessary to build readiness [449]. The implementation of quantum technologies must align with strategic objectives and regulatory mandates [463].

Research Question 4: What are the critical adoption barriers to quantum cybersecurity in accounting, and can these be overcome with long-term security gains? Primary obstacles include high upfront costs, a shortage of trained specialists, and technical complexity [461, 462]. The digital readiness of organisations varies greatly; companies with high cloud and IT sophistication overcome these challenges most effectively [47]. Subjective norms and cultural resistance initially hinder adoption, but success stories from pioneering users [463] and social influence [466] ultimately propel widespread industry adoption in the long run. Long-term advantages encompass increased security, compliance with regulations, and a competitive edge [409]. Government initiatives and standardisation activities (e.g., NIST PQC, ISO) contribute significantly to reducing obstacles [456]. Costs of QKD will come down, and easy-to-use quantum cybersecurity platforms will help bridge the skills gap [465].

5.6. Contributions of the study

5.6.1. Academic Contributions

The study contributes to the academic understanding of integrating quantum computing in cybersecurity within the context of accounting and finance. It helps to bridge the knowledge gap on how quantum computing can be exploited to enhance data security in accounting and finance at a time when conventional cybersecurity measures are increasingly becoming vulnerable to quantum-based attacks [468]. In addition, the study enhanced the information system model proposed by [190]Thompson et al. to include quantum computing-based cybersecurity, providing accountancy scholars with new conceptual models to base their research on, integrating quantum computing technologies in accounting systems to maintain confidentiality and system integrity. Adapting the information system model is relevant to academics seeking to identify the opportunities and threats of quantum computing to accounting and finance services, where confidentiality and system integrity are highly required.

5.6.2. Methodological Contributions

The study adopted a systematic literature review methodology (PSALSAR), ensuring methodological rigour and repeatability [430]. PSALSAR methodology, which includes phases such as Research Protocol and Reporting of Results, ensured that the study could synthesise and analyse the existing research without bias. This study, therefore, contributes to the methodology of conducting systematic studies. This research demonstrates that PSALSAR can be utilised to investigate emerging technologies, including quantum computing and cybersecurity. The study can provide a benchmark for future studies in emerging interdisciplinary fields, developing a structured approach to synthesising and analysing the literature.

5.6.3. Practical Contributions to Financial Institutions

The findings of this study have practical implications for financial institutions (FIs). For instance, the study highlights that accounting systems are vulnerable to quantum-based attacks because they cannot be deciphered using classical computing architecture. The study suggests that financial institutions should adopt quantum-resistant algorithms and Quantum Key Distribution (QKD) in their cybersecurity protocols. Financial institutions can utilise these findings to enhance their accounting systems and ensure data confidentiality and integrity. The research also recommends that FI train its accounting professionals on quantum technologies to implement quantum-safe practices successfully. It is a proactive approach that will help financial institutions mitigate the risks associated with the threat of quantum computing and maintain a strong cybersecurity environment.

5.6.4. Policy Contributions to Technology Regulations in Accounting

The study contributed to a policy regarding technology regulations in accounting. The study explains how quantum technologies pose regulatory challenges and how existing regulatory

frameworks should evolve to accommodate these technologies, enabling their implementation in accounting and finance in a responsible and secure manner. Policymakers can use the findings in this study [469] to develop guidelines and standards to ensure the regulated and secure adoption of quantum computing in accounting and finance. The study also recommends that policymakers collaboratively incorporate financial institutions and researchers in setting regulatory frameworks for quantum technologies that will support innovation and security. The collaborative approach to setting regulations for quantum technologies will lead to the development of a secure financial infrastructure in the quantum era.

5.7. Future Research

Although several post-quantum cryptographic algorithms are available, few algorithms are designed explicitly to handle accounting functions like audits, ledger reconciliation or compliance. Future work should focus on designing and testing quantum-resistant algorithms tailored to accounting workflows. Output would include open-source algorithmic frameworks in conformance with international cryptographic standards. Integrating quantum technologies into legacy ERP and accounting systems is challenging. Work should aim to create interoperability solutions, such as middleware layers that enable hybrid encryption in legacy environments. That affords practical on-ramping roadmaps for real-world implementation. The successful adoption of quantum computing in accounting involves accountants, IT experts, quantum engineers and compliance professionals. Research should propose socio-technical frameworks, applying UTAUT models and organisational change theory to assess quantum readiness. The adoption of quantum computing in accounting and finance systems can be analysed using the Unified Theory of Acceptance and Use of Technology (UTAUT), which provides a well-established framework for understanding technology adoption. The original UTAUT model [396] identifies four key constructs: performance expectancy, effort expectancy, social influence, and facilitating conditions, which collectively influence behavioural intention and actual system use. In the context of quantum computing, these constructs explain how organisations evaluate the benefits of enhanced cybersecurity capabilities, the complexity of implementation, the influence of regulatory and industry expectations, and the availability of organisational and technical support for adoption.

Furthermore, the extended UTAUT2 model [470] introduces additional factors such as habit, price value, and hedonic motivation, which can be adapted to organisational settings to better understand long-term adoption and integration of emerging technologies. Applying both UTAUT and UTAUT2 in this study strengthens the theoretical foundation for analysing quantum computing adoption in accounting cybersecurity, highlighting that successful implementation depends not only on technological capability but also on organisational readiness, user acceptance, and governance structures.

An organisation's quantum readiness toolkit is the expected output. Given the cost concern highlighted in Proposition 4, a financial analysis is necessary to compare the investment in

quantum cybersecurity to the risk cost of future breaches. It may involve modelling different scenarios for firms of various sizes. The output may include an executive-level decision-support model for accounting and finance professionals. Few studies simulate real quantum threats, such as Shor's or Grover's algorithm, against financial systems. Work must use quantum simulators to simulate these scenarios and test current defences. Resultant deliverables include a threat simulation framework for financial institutions and auditors. As quantum technologies affect transparency and traceability, their effect on accounting standards must be studied. Future work should analyse how quantum methods intersect with GAAP, IFRS and SOX compliance. Output includes guidelines for the ethical deployment of quantum tools in regulated environments. A composite index that considers infrastructure, regulatory environment, education and market exposure is needed to benchmark international readiness. The goal is to create a global Quantum Security Index (QSI) for finance and accounting.

Future studies should build upon this framework by incorporating empirical validation, such as case studies, interviews, or pilot implementations of quantum-secure accounting systems. Comparative studies across industries could identify sector-specific nuances and best practices. Quantitative assessments of adoption costs, regulatory compliance outcomes, and performance improvements post-QKD or PQC implementation would further enrich this field. Researchers are also encouraged to explore the impact of quantum security on real-time auditing, blockchain integration, and cross-border financial governance.

From a theoretical perspective, the challenges posed by quantum computing to classical cryptographic infrastructures can be understood through the lens of information security risk theory and long-term data confidentiality theory. Information security risk theory emphasises that organisational information systems must continuously adapt to evolving technological threats that compromise the confidentiality, integrity, and availability of digital information. In the context of accounting systems, cryptographic mechanisms form a fundamental component of financial data protection and audit reliability. However, advances in quantum computing challenge the underlying computational assumptions that secure widely used encryption methods such as RSA and Elliptic Curve Cryptography. Long-term data confidentiality theory further highlights the risk that encrypted financial records captured today may become vulnerable in the future once sufficiently powerful quantum computers emerge, a phenomenon often referred to as "harvest now, decrypt later". Consequently, accounting information systems must adopt forward-looking cybersecurity strategies that incorporate quantum-resistant cryptographic mechanisms to ensure the long-term protection of financial data[138, 353, 355].

5.8. Conclusion

In summary, quantum computing enhances the security of accounting practices by providing more robust encryption methods, improving risk management, enabling advanced anomaly detection, and facilitating efficient data processing. Collectively, these capabilities offer a

more secure and resilient framework for protecting sensitive financial information than traditional computing methods.

Quantum computing can fundamentally change the parameters applied for AI-based decision-making in OM. It could redefine how to utilise AI based on new parameters for the decision search space, the size of the alternative set, the interpretation of the process and outcomes, the speed of decision-making, and the replicability of processes. More specifically, quantum computing may lead to new decision-making processes in OM.

In particular, with integrated quantum computing, AI can exhibit a greater capacity to step beyond mechanical and repetitive tasks to more ‘cognitive’ analysis of processes, as argued by [471], such as inferring stakeholder needs, modelling and predicting customer management procedures, and automating many routine tasks and operations in OM to promote efficiency and eventually innovation. As organisations across various domains experiment with using quantum computing to amplify AI operations in management, we must consider the associated benefits, challenges, and consequences for ourselves and society. Using quantum computing for AI in OM may require massive infrastructure and significant investment in human resources. Moreover, such applications of quantum algorithms for decision-making processes must be carefully vetted to understand the ethical and social implications.

This thesis investigated the intersection of quantum computing and cybersecurity within the domain of accounting and finance systems. Through the application of a structured, systematic literature review guided by the PSALSAR methodology, the study examined how quantum technologies, especially quantum-resistant algorithms and QKD, may redefine security paradigms in financial environments. An integrated conceptual framework combining user-level, organisational, and quantum-specific constructs was developed and used to evaluate four key propositions. The analysis revealed that quantum computing offers measurable advantages in encryption strength, data integrity, and regulatory compliance but faces adoption challenges related to cost, complexity, and cultural readiness.

All research objectives outlined in Section 5.1.3 were addressed through proposition-based findings and thematic synthesis. The study confirmed that quantum-secure frameworks can enhance access control, prevent data breaches, and support the strategic alignment of accounting systems with emerging regulatory demands. Additionally, organisational adaptation was identified as essential for the successful integration of these advanced technologies. The four research questions were comprehensively answered in Section 5.5.2, validating the proposed framework's theoretical grounding and practical relevance.

Quantum computing represents both a disruptive threat and a transformative opportunity for the accounting profession. As data-driven decision-making becomes increasingly central to financial reporting and control, ensuring the security and resilience of systems becomes paramount. This thesis emphasises the need for proactive strategic planning, robust training programs, and regulatory foresight to realise the benefits of quantum cybersecurity while

mitigating associated risks. The integrated framework and research propositions presented here offer a foundation for both scholarly inquiry and practical transformation in the quantum era of accounting.

From a theoretical perspective, this chapter contributes to the Accounting Information Systems (AIS) literature by integrating quantum-resilient cryptographic considerations into the cybersecurity architecture of financial data systems. While prior AIS research has focused largely on classical encryption and conventional cybersecurity controls, the emergence of quantum computing challenges these foundational assumptions. By analysing post-quantum cryptographic mechanisms and their implications for accounting data protection, the chapter extends existing AIS cybersecurity discussions toward long-term cryptographic resilience.

Despite these contributions, several limitations must be acknowledged. The development timeline for large-scale quantum computers remains uncertain, making it difficult to determine precisely when classical cryptographic systems may become vulnerable. Additionally, the organisational readiness of accounting institutions to adopt quantum-resistant security mechanisms varies significantly depending on technological infrastructure, financial resources, and regulatory guidance. These uncertainties highlight the need for continued interdisciplinary research at the intersection of accounting, cybersecurity, and emerging computational technologies.

As it revolutionises traditional crypto paradigms, Quantum Computing also necessitates dynamic, strategic cybersecurity strategies. The quantum cybersecurity perspective outlined in this chapter underscores the technological resilience of accounting systems. However, cybersecurity extends beyond a mere technical challenge; it represents a strategic interaction between defenders and adversaries. Consequently, Chapter 6 employs Game Theory to model the dynamics between attackers and defenders within accounting contexts, offering insights into optimal investment, deterrence, and behavioural response strategies that enhance the technical layers discussed previously. Thus, the accompanying chapter introduces Game Theory as an essential tool for modelling interactions between cyber attackers and defenders in the accounting environment.

Chapter 6

6. Strategic Cybersecurity in Accounting: A Game-Theoretic Framework for Mitigating Social Engineering

6.1. Introduction

6.1.1. Brief Background

The ever-increasing reliance on digital systems in accounting and other fields increases exposure to cyberattacks that target both technical and human elements within these systems. Attackers are increasingly using social engineering techniques, such as phishing, impersonation, and credential theft, to compromise accounting systems that store sensitive financial information. Traditional security models, although useful, often overlook the strategic and adaptive nature of these attacks.

In addressing this problem, the research community has resorted to Game theory, a mathematical framework for modelling interactions between rational adversaries. In the context of cybersecurity, it enables one to model the dynamics between an attacker and a defender, helping to determine an optimal defence strategy under various conditions. The Zero-Sum game and the Stackelberg game are two examples of game-theoretic models that can be used to quantify risk and inform the defender about the attackers' attack actions and the defensive actions to take.

Given this challenge, the Game Theoretic Methodology (GTM) has been proposed to formalise threat evaluation, model interactions, and guide investment decisions. By integrating the GTM with matrix-based modelling and Nash Equilibrium, this chapter aims to develop a robust, adaptive cybersecurity framework specifically for accounting systems, where the confidentiality, data integrity, and timeliness of financial information are of paramount importance.

6.1.2. Motivation & Relevance

The use of digital systems in accounting has left the profession highly vulnerable to sophisticated cyber threats, especially those based on the manipulation of human behaviour through social engineering. Financial data is the most sought-after data in cybercrime. Accounting systems are the most common entry point for cybercriminals because they are both critical and sensitive [472]. Despite significant investments in technical defence measures, breaches continue to occur because it is challenging to anticipate what the attacker will do, and there is an insufficient understanding of human behaviour and defence measures. It leads to a gap in the traditional cybersecurity defence models. The study deviates from traditional defence paradigms by employing Game Theory to simulate and predict attacker-defender interactions. [473] Game theory has been described as a mathematical method for modelling and analysing the interactions between decision-makers, in which each is considered under the defence outcome and the constraints. Zero-sum games are used to model symmetric games and can be employed to capture a symmetric security game. The defender aims to minimise

the payoff, while the attacker seeks to maximise it. Stackelberg, a Bayesian approach, can be utilised to simulate a pre-emptive game in which the defender acts strategically in advance to deter the attack. Empirical studies suggest that social engineering remains the most successful method of cyberattacks [474]. However, few game-theoretic models incorporated human behaviour. The Game Theoretic Method (GTM) has been developed to merge empirical data, threat behaviour, and payoff matrices to produce a powerful semi-automated tool for simulating complex real-world situations [474]. Extending game theory to accounting scenarios is beneficial because it can model both human and system vulnerabilities. This thesis demonstrates how matrix-based modelling and Nash Equilibrium analysis can be used to effectively inform resource allocation, policy, and real-time defence in accounting information systems, utilising both real and hypothetical data from the CIC IDS 2017 and the CERT Insider Threat datasets. The results of this thesis's findings are vital to both academia and practical stakeholders, such as accounting system designers, auditors, and IT security managers, who gain a robust, mathematically grounded decision-making tool to anticipate and defend against cyberattacks in high-risk financial environments.

6.1.3. Related Research

[475] The study, Regulatory and Organisation professionals, is giving considerable importance to cybersecurity measures after facing high-profile incidents like Equifax, Sony, and Target. It has forced organisations to demonstrate how effective and efficient the processes and controls are in detecting, responding to, mitigating and recovering from breaches and other security incidents. This research aims to address this problem. The study builds on the Game Theory Framework, considering the work done by [476], where the researcher highlighted the Game Theory to be a suitable model which covers several issues successfully applied to cybersecurity, being ideal for modelling various matters and has been successfully used in cybersecurity, which comprises communication networks as well [477-479]. We are considering the research work done by the researcher, who proposes the Bayesian game theory model [480] to study intrusion detection. This security tool monitors network traffic in wireless ad hoc networks, alerting when suspicious activities are detected to analyse the interaction between attackers and defender nodes. It is worth noting that the player may represent either a malicious or a regular node when the Nash Equilibrium concept is applied under both static and dynamic scenarios. [481] In the study, the utilisation of anomalous flow-based methods, social engineering, and machine learning to monitor progress and detect and defend against Advanced Persistent Threats (APTs) [482] was considered, as well as game theory, cloud platforms, dynamic information flow tracking, and limited resources as defensive strategies. This paper combines game theory and social engineering to enhance cybersecurity measures for business organisations.

6.1.4. Research Aim, Objective and Questions

a. Research Aim and Objectives

Based on Game Theory and Social Engineering, this research on cybersecurity in accounting aims to develop strategies, investigate, analyse, and propose a practical cybersecurity framework to protect against and mitigate the risk of cyberattacks.

This research examines the intersection of Game Theory and Social Engineering to enhance cybersecurity resilience in the accounting sector. The primary focus is on designing and evaluating strategic, data-driven defence mechanisms by analysing the interactions between attackers and defenders through game-theoretic models. Utilising real-world threat scenarios and empirical data, this study aims to develop a practical and adaptable cybersecurity framework specifically tailored to address the risks associated with social engineering and technical cyberattacks targeting accounting information systems.

b. Research Questions

This research paper aims to develop a cybersecurity framework based on game theory that integrates social engineering tools to enhance cybersecurity measures. The main research questions are:

1. How can the game theory model and the social engineering tools be integrated and designed into a comprehensive cybersecurity framework to detect and prevent cyber-attacks effectively, and what are the most effective strategies for implementation and management?
2. What key components should be included in a cybersecurity framework based on game theory to deal with social engineering attacks successfully?
3. How can the attacker's behaviour be predicted using game theory, and how can an analysis be conducted to evaluate the use of this information in enhancing the effectiveness of the cybersecurity framework?
4. How can this game theory-based cybersecurity framework address the prevailing cybersecurity threat and manage the challenges of emerging cyber threats?

6.1.5. Contribution to Knowledge and Statement of Significance

a. Academic Contribution

Not only are businesses, but individuals are also facing cyber threats from attackers. This research paper designs and develops a Cybersecurity framework and strategies for accounting, utilising a game theory model to analyse the effectiveness of the cybersecurity measures adopted by the defenders of the Organisation. [478] The study clarified that the size, accessibility, and interconnectivity of global networks continue to experience dramatic changes, resulting in ever-increasing vulnerabilities. Game Theory is a framework for addressing conflicts of interest among players by building models and scenarios. Game theory, a mathematical framework, can be used to design a model that analyses the behaviour of attackers and defenders for effective cybersecurity measures to identify exposures and develop approaches to mitigate them. [478] The article referred to the research conducted by [483] in a report proposing a game-theoretic approach to analysing computer network security, where the interaction between the attacker and administrator is viewed as a two-player stochastic

game, and a model was built. At the same time, the method of psychologically manipulating individuals to obtain unauthorised access to sensitive information is known as social engineering. While developing an effective defence mechanism for an organisation, it is essential to know the tools used by social engineers, including pretexting, baiting, and phishing. Social Engineers attack using these techniques, exploiting human vulnerabilities and deceiving individuals into sharing sensitive, confidential information or conducting tasks comprising the cybersecurity. Further business organisations may be able to counter social engineering attacks and implement awareness programmes, including training employees and designing the policies and procedures that mitigate the probability of successful attacks. Furthermore, this research identifies areas for future research in arranging and developing training programmes and educational courses to enhance the understanding of cybersecurity risk, cyber threat awareness, and preventive measures for accounting professionals.

b. Statement of Significance

• Practical Contribution

Everything we do, whether part of daily activities or organisational financial transactions, is stored on computer systems and dealt with online. It implies that the core of this digital civilisation is the system's resilience. Machine Learning (ML), Artificial Intelligence (AI), Game Theory (GT), and Blockchain (BC) have all responded to cybersecurity concerns. This study offers a significant contribution to the intersection of cybersecurity, accounting information systems, and game theory by addressing the increasingly complex threat landscape that targets both digital infrastructure and human behaviour. In this research paper, we examine how enterprises utilise GT to enhance cybersecurity and identify the potential challenges and limitations associated with this approach. Traditional cybersecurity measures often treat attackers as static threats, failing to account for the strategic, adaptive nature of modern cyber adversaries, especially those leveraging social engineering techniques. One research study being conducted is relatively practical and has contributed to [474], where a study proposes investment strategies based on game theory designed to counter different types of attackers, including game-theoretic and disorderly ones. The conclusion of this game-theoretic methodology is the automatic creation of defensive strategies by the beneficiaries, enabling them to operate effectively in various scenarios. It can be applied to other systems with one or numerous offending victims.

By applying Game Theory models, specifically Zero-Sum and Stackelberg games, within the structured framework of the Game Theoretic Methodology (GTM), this research provides a dynamic, data-driven approach to identifying and deploying optimal cybersecurity defenses in accounting environments. The use of Nash Equilibrium and matrix-based simulation enables organisations to quantify trade-offs, anticipate the decisions of attackers, and allocate resources efficiently.

The study is especially significant for:

- » Accounting professionals offer a framework that incorporates both technical and human-layered risks.
- » Cybersecurity analysts and auditors provide strategic modelling tools for policy and control selection.
- » System designers and risk managers can leverage game-theoretic insights to improve architecture resilience.
- » Researchers, by filling gaps in the existing literature, offer replicable methods for scenario-based defence optimisation.

6.1.6. Scope & Delimitations

a. Scope

This chapter focuses on the application of Game Theory models, specifically the Zero-Sum Game and the Stackelberg Game, within the framework of the Game Theoretic Methodology (GTM) to design optimal cybersecurity strategies for accounting information systems. The study emphasises modelling both technical threats and human-centred attacks (e.g., social engineering) through payoff matrices and uses the Nash Equilibrium to identify optimal defence strategies. The analysis incorporates practical, scenario-based simulations using both hypothetical and empirical data sourced from established cybersecurity datasets, such as CIC IDS 2017 and the CERT Insider Threat dataset.

i) Key areas of exploration include

- » Strategy modelling between attackers and defenders
- » Integration of social engineering vectors into game-theoretic analysis
- » Simulation of defense outcomes using matrix methods
- » Identification of resource-efficient, optimal controls for accounting systems

b. Delimitations

The study is confined to strategic-level cybersecurity modelling and does not address low-level cryptographic protocols, hardware vulnerabilities, or purely technical implementations. The GTM model is applied in a theoretical context and through simulations rather than as a real-time deployment on live accounting platforms. Additionally, only two game-theoretic models (Zero-Sum and Stackelberg) are considered; other variants, such as Bayesian or Cooperative Games, are excluded from this analysis. The focus is specifically on accounting systems; therefore, the findings may not be fully applicable to unrelated fields such as healthcare or manufacturing. Lastly, social engineering is modelled exclusively through selected scenarios (e.g., phishing, impersonation) and does not encompass all potential psychological manipulation techniques.

These boundaries were set to ensure methodological focus, relevance to accounting security, and clarity in model development and analysis.

While accounting information systems increasingly rely on automated decision-making, digital audit trails, and interconnected financial infrastructures, they remain vulnerable to

strategic adversarial behaviour. Cyber-attacks on financial systems do not occur randomly; rather, they reflect deliberate decision processes whereby attackers select optimal strategies to maximise pay-offs while minimising the probability of detection. This dynamic is particularly pronounced in social engineering attacks, where adversaries exploit human decision-making and organisational routines. The central problem addressed in this chapter is the absence of structured, game-theoretic models within accounting research that explain how attackers and defenders behave strategically within AIS environments, and how these interactions create vulnerabilities that cannot be captured by technical controls alone. Moving beyond the cryptographic aspects of Quantum Computing, the chapter discusses Game Theory as a tool for strengthening cybersecurity defences. It introduces frameworks for decision-making optimisation in adversarial situations within accounting and finance systems.

6.2. Literature Review and Theoretical Foundation

6.2.1. Overview of Cybersecurity in Accounting Based on Game Theory:

a. Game Theory in Cybersecurity

Game theory is a mathematical tool used to model strategic interactions among rational decision-makers. In cybersecurity, it is applied to simulate the behaviour of adversaries (attackers) and defenders (system administrators or organisations), each attempting to maximise their outcomes [484]. The attacker seeks to exploit system vulnerabilities, while the defender allocates limited resources to mitigate those risks. Game theory helps identify optimal defence strategies under uncertainty and budget constraints, making it highly suitable for dynamic environments, such as accounting information systems, where both technical and human vulnerabilities coexist.

b. Zero-Sum Game

A Zero-Sum Game is a two-player game where the gain of one player is precisely equal to the other player's loss. In the cybersecurity context, this model is ideal when the attacker's success implies a direct loss for the defender, such as in phishing or DDoS attacks [485].

Players: Attacker vs Defender

Assumption: Interests are strictly opposed

Use Case: Simultaneous decision-making, e.g., both attackers and defenders act without knowing each other's strategy.

In matrix terms, if the attacker receives a payoff of +7, the defender gets a payoff of -7. The goal is to find an equilibrium strategy where neither player can improve their outcome unilaterally [484].

c. Stackelberg Game

[486]The Stackelberg Game models a sequential interaction where the defender acts first, signalling a commitment to a strategy. The attacker then responds optimally. This structure mirrors real-world cybersecurity, where organisations deploy defences in anticipation of future threats.

Leader: Defender

Follower: Attacker

Assumption: Sequential play; attacker observes defense strategy before acting

Use Case: Preemptive policy setting, such as enforcing strict access control or monitoring protocols.

Stackelberg models are valuable for proactive defence design, enabling organisations to deter attackers by making firm initial commitments to specific protections.

d. Nash Equilibrium

The Nash Equilibrium is a foundational concept in game theory where each player's strategy is optimal given the other player's choice. In other words, no player can benefit by changing their strategy unilaterally [484].

The Zero-Sum Games identifies stable pairs of attacker-defender strategies.

The Stackelberg Games support choosing the optimal leader strategy, anticipating the follower's best response.

In cybersecurity modelling, the Nash Equilibrium helps determine the most effective combination of defence actions by predicting how rational attackers will respond.

e. Relevance to this Thesis

This thesis applies both Zero-Sum and Stackelberg models, solved through Nash Equilibrium, using payoff matrices populated with both hypothetical and empirical data. These models simulate:

- » Simultaneous and sequential threat interactions
- » Optimal defense allocations under resource constraints
- » Human and technical vulnerabilities in accounting systems

Together, these models form the backbone of the Game Theoretic Methodology (GTM) framework, providing structure and analytical depth to strategic cybersecurity planning.

6.2.2. Prior Research

[487] The study clarifies that a subject matter shows progress only when combined with prior studies that are logically based on previous findings [488]. He defined that literature reviews make considerable contributions to theoretical, methodological, and thematic advancements in various areas [489, 490]. Furthermore, he noted that Review papers are "critical evaluations of prior studies that have already been published" [491].

a. Game theory in network security for digital twins in the industry

[478] The study suggested that digital twins describe the process of safe operation of the digital twins' industrial network, including avoiding harm through invasion by a hacker into the system; it pointed out game theory as the solution by pointing out a series of discussions carried out on network security, leading to game theory. It was further explained that digital twins are a cutting-edge technology that assists the industry in deploying industrial applications, demonstrating the new technology to help the sector boost its revenues and

reduce unnecessary overhead costs associated with equipment and procedural concerns, ultimately opening up new opportunities across the value chain. Therefore, it would not be incorrect to say that, during the research phase, the progress of development, and the stages of testing, including the Analysis of IP protection, digital twins expand and enhance their efficiency in all aspects, including vendor management. In this attack environment, high security and privacy assurance for the network are essential during virtual mapping. Vulnerability to threat becomes more prominent when the devices are connected in several ways to each other so only a few channels that the digital network devices can accept and rely on against hackers' interception like Protocols, an example being Hyper Text Transfer Protocol (HTTP) and Application Programming Interface (API) [492] in the article guaranteed that the port security was also turning off port forwarding, one more method of non-opening of port when not needed, also keeping firewalls active, using anti-virus and anti-malware software, intrusion detection & prevention system, prevention from unauthorised internet protocol addresses and lastly ensuring a system to be updated through his proposition of different ways of digital twins network protection. It means that, with the priority of industrial internet security protection in mind, vulnerability repair and mining exploration led researchers to apply evolutionary game theory, covering the life cycle of network security vulnerabilities and encouraging the development of effective and efficient vulnerability repair systems in the digital twin's network. As identified in the study, the future work will utilise the stochastic game theory model factor for further improvement.

b. Cybersecurity Threat Assessment Integrating Qualitative Differential and Evolutionary Game

[493] The study identified that attack defence is a key strategy in cybersecurity. Furthermore, game theory is highly compatible with addressing this conflict, considering its key traits, including non-cooperative relationships, goal opposition, and strategy dependence [494]. The study clarifies that we can obtain methodological guidance and prepare a research model using game theory to analyse cybersecurity threats [495]. The traditional method for assessing cybersecurity threats [496] does not adequately cover security threats due to the constant and vigorous changes in network conflicts, rendering this method inaccurate and impractical [497]. To overcome this, researchers and scholars have moved toward the game theory model for addressing cybersecurity risk, including the attack-defence behaviour, resulting in moderate success. Considering the current game theory models for cybersecurity analysis, the researcher clarifies that they are traditional game models with unrealistic conditions, incompatible with the continuous dynamic changes in the decision maker's behaviours and that of the attack-defence relationship, which lacks rationality. It typically results in difficulty adapting to the practical requirements of cybersecurity threat assessments. Therefore, assessing cybersecurity threat requirements in terms of timeliness and practicality aligns with this theory and yields a solid direction value. Next, the researcher considered evolutionary games, which are used to

analyse vigorous changes due to attack-defence strategy selection probabilities and determine the route of the network security position. The conflict due to security threats is analysed through qualitative differential games, first calculating the attack-defence obstacles and then creating a benchmark for measuring the threats to security.

c. Applications of Game Theory in Finance and Managerial Accounting

[498] The study pointed out that, related to the literature review, the Game Theory principal-agent model gives insights into the game theory invasion in the fields of accounting and Finance about applications related to Nash & Bayesian equilibria, expected utility maximisation, asymmetric information, signalling and agency models, with special attention given to principal-agent problems[499] and also [500].

The researcher defines how finance supports their endeavours through the proper distribution of budgets, which are accessible through intermediaries and financial markets available to investors. The researcher emphasises that this discussion comprises two broad categories. The first is asset pricing revolving around the investor's decision, including decisions related to the firms connected with the investor's decisions. The second one, Corporate Finance (CF), is concerned with the resolutions and solutions of the firms. Asset pricing is uncertain, while several areas of corporate finance require explanation, which led to the development of the field of finance. Statistical analysis of accounting data and the use of this information for decision-making are the primary concerns of managerial accounting, even though finance is also involved. It has been said that within the firm, accounting data and tactical and strategic conclusions influence each other equally. The strategic interactions among agents and the ex-ante incentives given to their behaviour have shifted their responsibilities from ex-post recording and ex-post analysis of accounting data. Hence, managerial accounting has moved from ex-post recording and ex-post Analysis of accounting data to strategic interactions among agents and the ex-ante incentives for their behaviour. Von Neumann's conception of expected value significantly impacted finance through game theory, which led to the development of asset pricing models and informed portfolio selection [501].

The researcher identified work for future researchers to build upon, directing the derivation of study models with more relaxed assumptions.

d. Cyber Security Risk Modelling in Distributed Information Systems

[502] The research identifies concerns during the development phase and security-related problems of the distributed information system, including risk modelling challenges. The researcher highlighted through the literature review that risk assessment is a challenging and urgent task in the information security management process. This research aims to develop a method that incorporates dynamic multifactor analysis to assess the risk of encountering incidents related to critical information security using intelligent assessment models.

The information security problem is not limited to the technological approach in this modern system, so a structured assessment methodology is required for the preventive measures

implemented to reduce the risk. Researchers suggested a risk modelling approach responsive to this distributed, high-tech, complex, large-scale system.

The researcher reviewed and analysed the existing risk assessment approaches in the literature, comparing and highlighting their strengths and weaknesses. The literature has detailed that the developed solution addresses the problem of incomplete sensitive component information. A new risk assessment model was developed by addressing the loopholes highlighted in the previous model, with all the distributed information system characteristics that were not present in the last model integrated into this new model.

The study claimed that the proposed algorithms are simple in structure and easy to implement. A confusion matrix was constructed to evaluate the accuracy score of the neural network components and assess the execution and competence of the classification algorithm. Based on this accuracy check report, the study concluded that the model, which achieved 80% accuracy, was well-suited for describing the real-time system processes' occurrence.

6.3. Conceptual Framework

6.3.1. Introduction

This section describes the conceptual model for the Game Theory-based cybersecurity framework developed in the thesis, which combines technical and behavioural guidelines to create defensive strategies against cyber threats, particularly social engineering attacks targeting AIS. This conceptual model integrates Game Theory, Social Engineering Attack Types, and Cyber Security Defences into a structured paradigm for AIS where the interactions of attackers and defenders are operationalised through strategic decision matrices, informed by Game Theoretic Methodology (GTM) and solved through Nash Equilibria, producing a diagnostic and prescriptive model which simulates and assesses cybersecurity defences.

6.3.2. Core Components of the Conceptual Model

a. Actors and Roles

- i. Attacker:** modelled as a rational (or bounded-rational) actor using social engineering to target accounting systems, such as phishing, baiting, and pretexting.
- ii. Defender:** (organisation-Accounting IT Security team) The defender aims to minimise/limit losses by making strategic decisions over a set of options to implement technical and procedural controls.

b. Game Model

- i. Zero-sum game (simultaneous decision):** This models hostile scenarios (for example, phishing attacks), where the defender and attacker make decisions simultaneously, choosing to attack or protect without knowing the other party's action. This is appropriate for incident-level response modelling.
- ii. Stackelberg game (sequential decision):** an instance where the defender pre-deploys measures, such as deception, training, and firewalls, and the attacker responds accordingly. Appropriate for strategic security decisions and security investments.

c. GTM Framework

This model that we have considered in our conceptual framework has been discussed in detail in Sections 6.4.3 and 6.4.4.

- i. **System Assets:** sensitive financial records, auditing controls, payroll, transactional data, etc.
- ii. **Threat Types:** Email spoofing, social engineering, ransomware, insider sabotage, etc.
- iii. **Defence Controls:** multi-factor authentication, access restriction, anomaly detection, etc.
- iv. **Payoff Modelling:** payoff for each attacker-defender strategy, composed of cost, risk impact on the accounting system, etc.

d. Equilibrium Mechanism

Nash Equilibrium is calculated to determine if the strategy of a player is stable.

- i. In a zero-sum game, it shows mutual optimal choices where no player can unilaterally deviate to attain a higher payoff.
- ii. In the Stackelberg game, the leader (defender) chooses the strategy, and the attacker responds accordingly.

e. Social Engineering Layer

Maps social psychological manipulations (from Cialdini's principles of persuasion and actual breaches) onto attack vectors. Influences the payoff for the attacker, helping in simulating the human factor vulnerabilities.

f. Core Components of Conceptual Model

i. Input Layer

Attack Types: Social engineering (phishing, baiting, pretexting), ransomware, insider threat, credential attacks.

System Vulnerabilities: Weak authentication, unpatched systems, poor awareness.

Available Defences: Zero Trust Architecture, Role-Based Access Control (RBAC), 2FA, training, and deception techniques.

- ii. **Game Structure Layer:** There are two branches, the zero-sum game model and the Stackelberg model.

Attacker: Chooses among different attack types and strategies.

Defender: Chooses among different defence configurations and investments.

Game Models Used:

Zero-Sum Games: Models reactive defence against simultaneous attacker actions.

Stackelberg Games: Model a proactive defence where the defender commits first, and the attacker responds.

- iii. **Matrix Computation Engine:** Filled with either simulated data or actual data, such as CIC IDS 2017, CERT

Constructs payoff matrices (2x2, 3x3, or larger) representing attacker and defender payoffs.

It uses empirical data (e.g., CIC IDS 2017, CERT Insider Threat) and hypothetical scenarios to populate the matrices.

Computes Nash Equilibria to derive optimal mixed or pure strategies.

iv. **Nash Equilibrium Solver:** Find the optimal defence tactic through Nash Equilibrium by applying linear programming or analytical methods to solve the game matrices. The equilibrium point is identified where no player can unilaterally improve their outcome, and stable attacker-defender behaviour is predicted.

v. **Output Layer:** This research includes output related to defence priorities, investment advisories, and behaviour response estimations.

Optimal Defence Strategy Mix: Recommended proportional allocation across available defences.

Predicted Attacker Behaviour: Probability distribution across attacker strategies.

Investment Guidance: Prioritised cybersecurity control recommendations.

Adaptive Recommendations: Guidance on how defender strategy should evolve in response to new or emerging threats.

vi. **Purpose and Utility:**

- » Simulates real-world attacker-defender dynamics within AIS environments.
- » Predicts attacker behaviour and evaluates the effectiveness of defensive strategies.
- » Guides optimal allocation of cybersecurity resources.
- » Provides a flexible and scalable framework for adapting to evolving cyber threats.

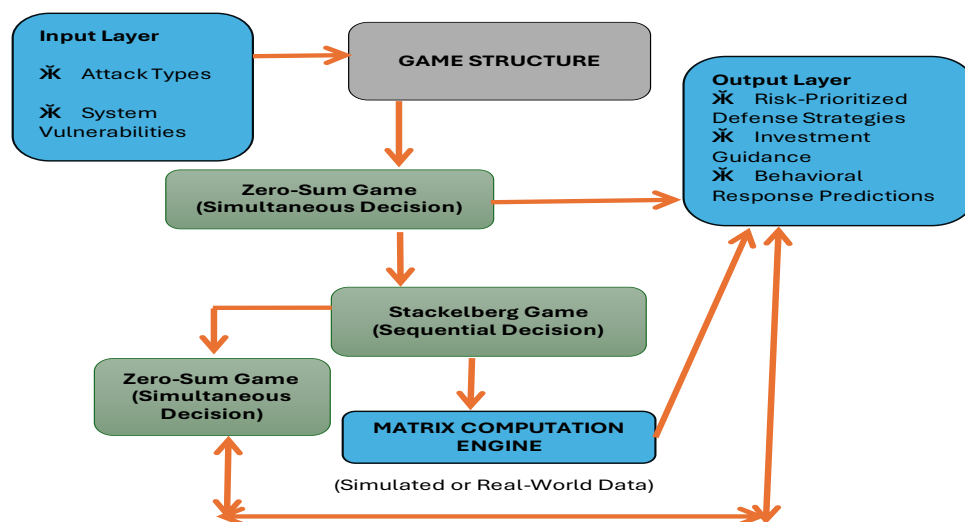


FIGURE 6.1 Conceptual Model (Cybersecurity for accounting based on Game Theory and Social Engineering)

Source: [503], [504], [140, 505].

The accompanying Figure 6.1 and matrices further illustrate the operationalisation of this model. This model enables the organisation to assess the cybersecurity posture of its accounting systems quantitatively. It predicts attacker behaviour using rational game models.

To address all current and emerging threats, it is essential to develop cost-effective strategies. It also creates technical modelling with human-centric attack vectors by integrating social engineering. [506] Users' lack of information about online practices risks creating several damaging cyberattacks, which are increasing rapidly. These online practices include visiting unsafe websites, ignoring warning messages, and interacting with unauthenticated organisations. In cybersecurity, the psychological manipulation of a human being to gain access to sensitive data is a key component of the cyberattacker's complex hacking methods. Our research addresses this issue by applying a game-theoretic model. We know that by tracking a vulnerable system for exploitation, attackers are now targeting the organisation's employees through calls or sending phishing emails that pose as legitimate sources, usually through a Social Engineering attack.

6.3.3. Game Theory Model

[507] As discussed above in the conceptual model, this article employs game theory as its framework, utilising two-player games: the Defender (D) and the Attacker (A). [507] further explained that the cybersecurity manager is the Defender of an organisation, assigned to secure and maintain the Organisation's reputation against cyberattacks and cyber theft, and to mitigate business interruptions. The researcher explained that the person attempting to sabotage the organisation's system, "D", by launching a cyber-attack, is the Attacker, "A". Figure 6.2 shows the Game model, which is very comprehensive. [482] The study highlighted the importance of game theory as a historical study covering the field of security [508]. It is further clarified by pointing out the first reason, which is due to the quantitative term framing covering payoffs, risk, gain, or losses. It enables high-level policy decisions to be translated into the best course of action through the framework of game theory, providing decision-makers with a unified basis for making informed choices [482]. It also mentioned offering a comprehensive mathematical framework with predetermined decisive factors to analyse and exploit various situations [482].

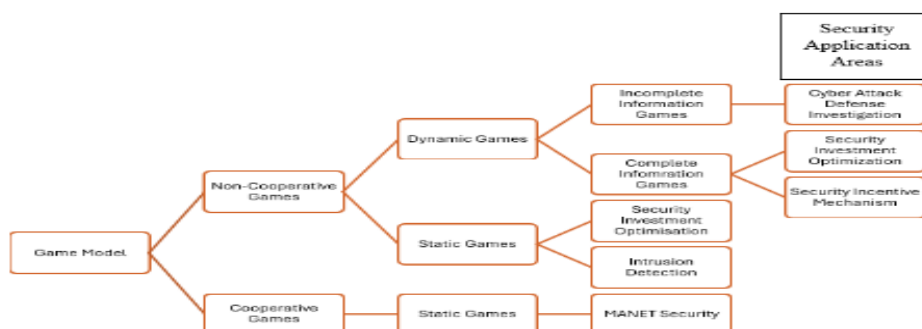


FIGURE 6.2 A classification of game models

SOURCE: [509].

Considering the time constraint, superior decision-making and successful security operations are crucial factors [510] that must be achieved through this evaluation. Game theory

determines the responses of the Defender to the Attacker, or vice versa, in strategic interactions in cybersecurity, where each strives to maximise their interests [494]. [509] The study explained the Zero-Sum games between two players, which have been classified as non-cooperative games, where one maximiser gains from the loss of the one who is the minimiser. [482] It further explained the Nash equilibrium as a critical concept in game theory, where each player responds to another player's action, also choosing not to change their strategy because this would result in a reduction in their payoffs [494, 499]. This is also a Steady-state condition, as a concept in game theory.

Static: The article described a fixed game as being strategic, where players simultaneously make their own decisions. Typical static security games include zero-sum games, static prisoner's dilemma games (PDGs), and the Stackelberg games [482].

6.3.4. Game Theory Models and Cybersecurity

[509] Cybersecurity is considered a conflict between two types of agents, the Defender and the Attacker, which can be modelled mathematically. Cybersecurity scenarios are modelled as non-cooperative dynamic games. The researchers' and industry practitioners' first choice is the mathematical tool of game theory, used by rational and intelligent actors to model their conflicts and cooperation. It alleviates cyberattacks in cyberspace through analytical and modelling methods, enabling the prediction of cyberattacks and the development of accurate defensive strategies [509]. Another article [511] highlighted researchers who used a game-theoretic model similar to the one proposed, utilising the Stackelberg game to investigate cybersecurity alerts while dealing with limited human resources. Another report pointed out that the study [510, 512, 513] used Stackelberg game models in the cyber-physical system to model its defence mechanism. Additionally, consider the articles that monitor the detection and filtering of spam and phishing emails, addressing concerns through the Stackelberg game, in which knowledgeable attackers adapt to the defence strategy.

6.3.5. Game Theory Model and Social Engineering Attack

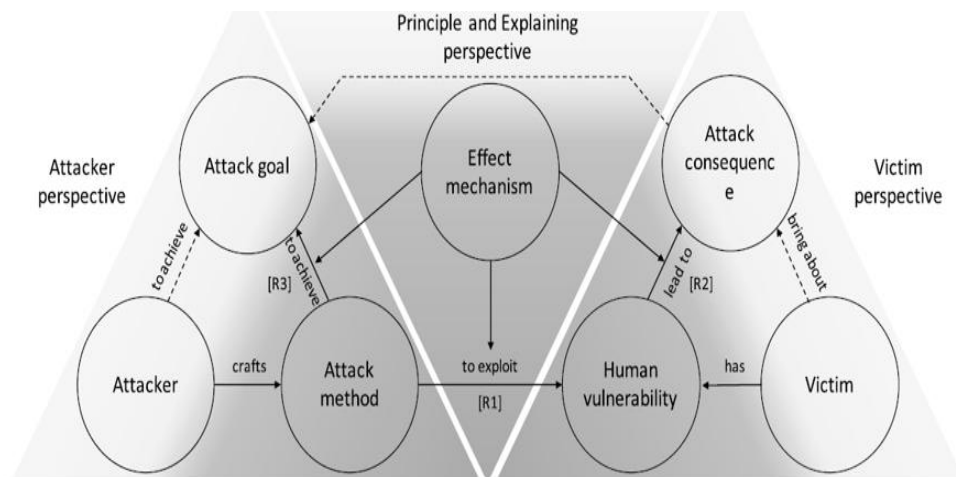
[514] The author explained the Social Engineering attack to exploit human exposures, which consisted of:

- a. cognition and knowledge,
 - b. behaviour and habit,
 - c. emotion and feeling and
 - d. psychological factor
- i.human nature
 - ii.personality traits
 - iii.individual characteristics.

[514] The article further explained the context of computer and cyber security regarding social engineering, which is described as an attack exploiting human vulnerabilities through influence, deception, manipulation, persuasion, and induction for hacking computer systems,

getting highly confidential classified information, obtaining unauthorised access plus obtaining unauthorised access to restricted areas, or breaching the security goals of cyberspace elements (such as confidentiality, integrity, availability, controllability and audibility) of cyberspace elements (such as infrastructure, data, resource, user and operation). [514] The article explained a few reasons why sensitive information not only gets generated and in large amounts, which are related to people and the devices being used, but also exposed to the more extensive attack surfaces, including the attack channels (IoT) Internet of Things, (SNSs) Social Network Sites and through mobile communication. The Industrial Internet and the Internet of Things (IoT). [514] Three primary perspectives help understand how social engineering attacks take effect, as shown in Figure 6.3. [514] Thus, the effect mechanism, human vulnerability, and attack method can serve as three core entities that help explain how social engineering attacks work and take effect.

[514]In this article, social engineering is described as an interdisciplinary field that encompasses computer science, cybersecurity, social psychology, brain science, and cognitive science. [514] Another factor contributing to a severe cybersecurity threat to cyberspace is



Social Engineering Attacks.

FIGURE 6.3 A conceptual model to describe how social engineering attacks work and take effect

, SOURCE: [514].

6.3.6. Game Theory and Accounting Cybersecurity

Although game theory is widely applied in economics and strategic management, its relevance to accounting cybersecurity lies in its ability to model adversarial behaviour, asymmetric information and competing incentives, all features present in fraud, cyber intrusion and internal control override. Within AIS, attackers frequently exploit gaps in monitoring, weaknesses in segregation of duties, and predictable user behaviours. Game theory provides a lens to analyse these interactions by treating cyber-attacks as rational choices under constraints and uncertainty. This perspective aligns closely with the risk-based philosophy of auditing and

internal control frameworks, which require preparatory defence strategies to anticipate adversarial strategic responses rather than relying solely on static security mechanisms.

This study uses the Nash equilibrium concept as the primary means to analyse attacker-defender interactions. The equilibrium is found by considering strategy combinations in which neither the attacker nor the defender can do better by changing their approach alone. This method gives a stable view of strategic behaviour under certain assumptions. Other ideas, like minimax or Stackelberg models, are not used here to keep things clear and consistent.

6.4. Research Methodology

6.4.1. Overview

This research employs game-based methods based on Game Theoretic Methodology (GTM). It applies zero-sum and Stackelberg games, solved by Nash Equilibrium analysis, to operationalise attacker-defender interactions within accounting information systems. The research method is designed to simulate, model, and analyse cybersecurity approaches against both technical and human-factored threats, such as social engineering, in accounting contexts.

6.4.2. Research Design

This research employs an analytical and scenario-based modelling framework with the following steps:

- a. Problem Definition:** Formulating cybersecurity threats to accounting systems as strategic games between the attacker and the defender.
- b. Scenario Building:** Building plausible attack-defence scenarios based on hypothetical and empirical information
- c. Matrix Modelling:** Developing payoff matrices modelling attacker-defender interactions under both Zero-Sum and Stackelberg game structures
- d. Equilibrium Analysis:** Utilising Nash Equilibrium to identify optimal defensive approaches
- e. Evaluation:** Interpreting the results of equilibrium to determine defence mechanisms and investment in cybersecurity

6.4.3. Application of Game-Theoretic Methodology

The GTM method [474] lays down the framework for this modelling and includes:

- a. Attack Graph Engine:** It is used to mimic attacker points of entry and potential avenues of attack.
- b. Data Pool:** Both actual sources, such as the CIC IDS 2017 and the CERT Insider Threat dataset, and scenario-based hypothetical sources are used.
- c. Defence Strategy Engine:** It maximises resource allocation based on the Nash Equilibrium used in matrix-modelled games.

The GTM paradigm enables the alignment of cybersecurity investment with attacker behaviour and threat risk, resulting in logical defence plans that are scalable and resilient [474].

In his paper, the author [474] presents GTM, a methodology for providing optimal cybersecurity strategies and investment plans. As we considered, we will be using the same method to conduct our research. As shown in Figure 6.4, the general structure of GTM is divided into three main modules:

- i) The Attack Graph Engine.
- ii) The Data Pool and
- iii) the Défense Strategy.

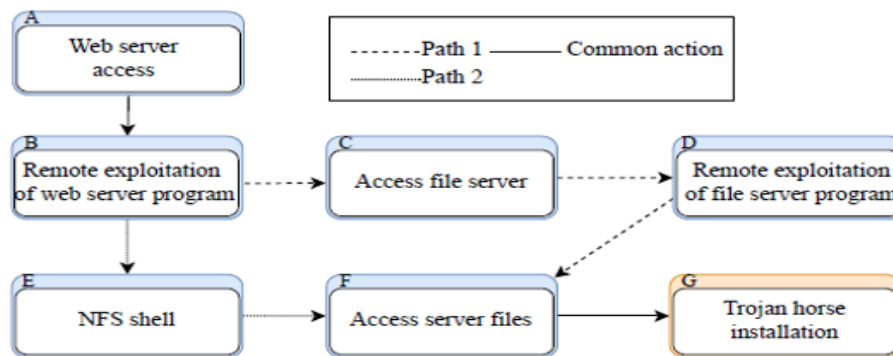


FIGURE 6.4 General Structure of GTM

Source: [474]

As detailed by the author, the first GTM factor, the attack graphs, is used to predict all possible cyberattacks. The author also mentions simulating cyber-attacks using game theory and ultimately optimally allocating a budget through a 0-1 knapsack. The second module, the data pool, is an area where the author stores laws, guidelines, and reports related to cybersecurity and privacy, designed to defend against cyberattacks on an organisation. The third, most crucial pillar and last module, the Défense Strategy, is required to calculate expected loss and to allocate the limited cybersecurity budget through the most appropriate cybersecurity controls. The purpose of using this GT methodology to conduct our research is to achieve its output, which, as defined previously, is the Organisation's optimum cybersecurity strategy comprising security controls that protect against cyber-attacks while improving its cyber defence. The game in GTM we are following is a zero-sum game solved using the Nash equilibrium approach.

In this article, the author considers a combination of Attack graphs and a game theory model to simulate cyber-attacks and optimally allocates the budget using the 0-1 knapsack problem. So, initially, we are considering the first phase of Attack graphs. We have several toolkits as described in the article [515], where the author has assessed and investigated several open-source AG tools like MulVal, TVA, Attack Graph Toolkit, and NetSPA, as well as commercial tools from phases of scalability and degree of attack graph visualization [516], among which the tools that are going to be considered by MulVal being a very comprehensive and user-friendly tool. Next, we conduct our research and justify our research question through two

game theory models. First, we apply the Zero-sum game model and find the solution through Nash Equilibrium. Additionally, we propose a framework for a large-sized organisation, designed using the Stackelberg game model to establish a cybersecurity framework, as the author's article [510] suggests this is a distinct class.

6.4.4. Game Theory Model Structures

Building upon the conceptual model, this thesis employs Game Theoretic Methodology (GTM) through Zero-Sum and Stackelberg Games, alongside Nash Equilibrium analysis, to develop actionable cybersecurity strategies for AIS. The methodology is structured as follows:

a. Step 1: Definition of the Scenario

» Realistic attack scenarios identified (phishing, insider threat, ransomware) using CIC IDS 2017 and CERT Insider Threat datasets.

b. Step 2: Construction of the Matrix

» Payoff matrices for 3x3 were constructed to illustrate interactions between the attacker and defender.

Example scenarios:

1. A phishing campaign targeting financial staff.
2. Insider data theft orchestrated by a compromised accountant.
3. A ransomware attack on the accounting server.

c. Step 3: Game Modelling

Zero-Sum Game

- i. It represents simultaneous play between the attacker and defender, which is best suited for reactive threat modelling (i.e., phishing).
- ii. The attacker's payoff is equal to the defender's negative payoff.
- iii. It is modelled on 3x3 matrices, with payoffs determined by the probability of attacks and the effectiveness of defence.
- iv. It is solved using the minimax approach and the Nash Equilibrium.

Stackelberg Game

- i. Models' sequential interactions where the leader/defender moves first by implementing security precautions.
- ii. The attacker (follower) reacts and observes optimally.
- iii. Useful for simulating strategic investment planning and proactive control configurations (such as firewall + 2FA + alerting).
- iv. Equilibrium is solved by backwards induction and the Stackelberg-Nash solution [517].

d. Step 4: Nash Equilibrium Computation

Equilibrium Strategy Analysis for each game

- i. Equilibrium points are derived through matrix-based modelling.
- ii. The Nash Equilibrium offers strategic stability, as neither the attacker nor the defender can enhance their position by adjusting their strategy independently [518].

iii. Optimal cybersecurity configurations are dictated by resource and budget constraints founded on equilibrium results.

e. Step 5: Analysis and Recommendations

Results interpreted to derive optimal defence strategies and investment priorities.

6.4.5. Data Collection Method

After designing the hypothetical situation, we try to gather the datasets through secondary or theoretical data sources. We use speculative data because the information of small and large organisations is confidential and not publicly available. They have a policy of not sharing this information with the public or making it available for research.

▪ **Tools**

Tools to be used during data collection. The choice of devices depends on the data available, e.g., Excel/Google Sheets, Python libraries, Pandas, MATLAB, SQL, Data Visualisation Tools, Data Warehouses, and Statistical Packages (SPSS).

▪ **Data Sources**

CIC IDS 2017 Dataset: A benchmark dataset of intrusion detection containing labelled examples of DDoS, brute force, and phishing.

CERT Insider Threat Dataset: This dataset comprises simulated insider actions, including policy breaches, credential misuse, and access manipulation.

Hypothetical Matrices: Developed for situations not explicitly addressed in public data sets (e.g., baiting, impersonation).

▪ **Steps for Pre-existing/Secondary Data Collection or the Hypothetical Data**

Considering both sources as a means of data collection, the method involves specific steps:

A. Pre-existing or the Secondary source of data or information available online, and the steps involved:

The steps involved are:

Step 1: Identify relevant archival data sources, such as public records from governmental agencies, research organisations, and business and industry sources, including the UCI Machine Learning Repository, Kaggle, OpenML, and government data portals.

Step 2: Understand Data Limitations: Assess the data's availability, quality, and permissions.

Step 3: Preprocess and organise: This includes collecting, compiling and managing the data.

Step 4: Clean the data by checking for missing values, outliers, duplicates, inconsistencies, and errors.

Step 5: Validate the data: To verify the accuracy, reliability, and credibility of the data.

Step 6: Analyse the data, apply appropriate analytical techniques to derive meaningful insights.

B. Hypothetical Data and Hypothetical Scenarios - steps involved:

Step 1: Identification of Relevant Factors and Metrics:

Identify incidents and relevant attacks related to the research project and its objectives, including security incidents, attack types, security controls, employee behaviour, financial impact, and other factors contributing to cybersecurity in accounting.

Step 2: Simulation of Hypothetical Situation:

To conduct research for both small and large organisations, we design hypothetical scenarios that align with the research objectives and the game theory framework. This step involves simulating virtual-reality cybersecurity attacks and incidents, as well as social engineering attacks targeting accounting and security in both small and large organisations.

Step no. 3: Creation of Simulated Hypothetical Data:

The generation of data relevant to the step mentioned above will encompass not only the creation of synthetic accounting data but also datasets such as employee profiles, network logs, attack reports, and any other pertinent data based on established guidelines, industry practices, or expert opinion.

Step no. 4: Performing Modelling and Simulation:

It includes preprocessing the acquired or generated datasets, such as data cleaning, integration, normalisation, and ensuring data quality and consistency. Following this process, the simulation of social engineering attacks using the generated and pre-processed datasets evaluates the effectiveness of security controls. Once the simulation is complete, the outcomes of different game theory strategies are analysed.

Step no. 5: Analyse, Interpret and Draw a Conclusion:

This step involves using appropriate data analysis methods or techniques via the Excel sheet and performing calculations with the visualisation tools to explore the datasets, interpret the findings, and draw conclusions. It includes evaluating the effectiveness of the cybersecurity measures, identifying potential vulnerabilities, and then suggesting refinements for cybersecurity strategies and standards based on the analysis.

6.4.6. Payoff and calibration

Because organisational cybersecurity datasets containing financial loss values are typically confidential, the payoff matrices used in the game-theoretic models were constructed using a structured calibration procedure rather than arbitrary assumptions. First, empirical evidence from publicly available cybersecurity datasets, including CIC IDS 2017 and the CERT Insider Threat dataset, was used to identify common attack types, detection probabilities, and typical behavioural patterns associated with phishing, insider misuse, and ransomware incidents. Public benchmark datasets are widely used in cybersecurity research to model attack behaviour and evaluate defensive strategies where organisational data cannot be disclosed [519, 520]. These empirical indicators provided the basis for estimating the relative severity and likelihood of attacker strategies.

Second, scenario-based justification rules were applied to assign payoff magnitudes. Each payoff value reflects the estimated organisational impact of a specific attacker–defender

interaction, incorporating factors such as financial loss, operational disruption, probability of detection, and the cost of defensive controls. Security game models commonly derive payoff structures from scenario-based risk assessments that incorporate attacker incentives, defender costs, and expected organisational losses [140]. Higher attacker payoffs represent scenarios where attacks are successful and undetected, whereas lower or negative payoffs correspond to situations where defensive mechanisms prevent or mitigate the attack.

Third, a sensitivity analysis was conducted by varying payoff values within plausible ranges to test whether the resulting Nash equilibrium remained stable across parameter changes. Sensitivity analysis is commonly used in game-theoretic cybersecurity models to ensure that equilibrium outcomes remain robust under alternative parameter assumptions and are not artefacts of a single payoff specification [140]. The equilibrium solutions remained consistent across these ranges, indicating that the strategic outcomes are not artefacts of assumed numbers but reflect stable attacker–defender interactions within the defined threat scenarios. This calibration process ensures that the payoff matrices represent structured modelling assumptions grounded in empirical cybersecurity evidence and scenario analysis, thereby strengthening the methodological validity of the game-theoretic simulations.

6.5. Results, Findings and General Discussions

6.5.1. Discussion – Testing the Game Theory Matrix Model

Despite the value of game-theoretic approaches, the accounting literature has not yet integrated these models into AIS cybersecurity analysis. Existing studies focus predominantly on technical vulnerabilities, internal control documentation or financial fraud patterns, but seldom examine the strategic interplay between attackers and defenders within accounting environments. There is minimal research linking social engineering behaviour with financial reporting risks, nor is there substantive exploration of how game-theoretic insights can inform audit planning, anomaly detection or cyber-resilience. Furthermore, no existing framework integrates game-theoretic cybersecurity with blockchain, quantum-resistant controls, or machine-learning models, leaving a conceptual gap that the BQMG-AIS model addresses.

a. Zero-sum game

i. Matrix 1: Social Engineering via Phishing, Impersonation, and Watering Hole

A-(Attacker)/D (Defender)	SA1	SA2	SA3	Min- loss (D)
SD1	(10, -10)	(-5, 5)	(0, 0)	-5
SD2	(-8, 8)	(5, -5)	(-3, 3)	-8
SD3	(6, -6)	(-2, 2)	(12, -12)	-2
Max-loss (A)	8	5	3	(-8, 8)

TABLE 6.1 Game Matrix 1

To understand the zero-sum game, we model cyberattacks based on social engineering on a small organisation. Table 6.1 illustrates our example of a zero-sum game matrix, demonstrating the interaction in terms of payoffs between the two players. The Defender (D) represents the organisation, while the Attacker (A) simulates cyberattacks involving social engineering targeting a small organisation. Higher payoffs (utilities) indicate better outcomes for the Defender, whereas lower negative values indicate more favourable outcomes for the cyberattack. According to the principle of the zero-sum game, the total payoff for both the Defender and Attacker is always zero; one player's gain is the other player's loss.

Employing the zero-sum game, we now seek to identify the Nash equilibrium, keeping in mind that the strategy considered aims for a scenario where both the Defender and the Attacker have no incentive to unilaterally alter their systems, with S representing a strategy or a plan to be adopted by either the Defender, being the organisation, or the Attacker.

Under this matrix, the Defender's payoff/utility is the first number, while the attacker's is the second. We are considering the strategies (SA1, SA2, SA3) adopted by the (SD1, SD2, SD3) Attacker or implemented by the Defender.

Let us consider the following:

SD1 – Primary Defence Mechanism: Under this mechanism, the Protector incorporates fundamental security measures to protect against social engineering attacks, including employee awareness programs, robust password policies, and regular software updates.

SD2 – Average Security Defence: Under this mechanism, the Guardian fortifies security measures by incorporating multifactor authentication, intrusion detection systems, and comprehensive security awareness programs.

SD3 – Cutting-Edge Security Practice: The Sentinel prioritises robust cybersecurity systems, conducts routine security audits, and employs skilled security professionals to proactively monitor and respond to potential threats.

SA1 – Phishing Attack: Under this scenario, the malicious Attacker attempts to trick employees by sending deceptive emails that prompt them to reveal sensitive financial information, login credentials, credit card numbers or click on malicious links. The primary objective of phishing attacks in accounting is to gain unauthorised access to economic systems, manipulate financial data, or commit fraudulent activities, which can result in significant financial losses, identity theft, or other forms of exploitation.

SA2, Impersonation Attack: Under this scenario, the malicious actor poses as a trusted individual, such as a colleague or a customer, in an attempt to deceive individuals within an accounting department into gaining unauthorised access, extracting confidential information or manipulating or tricking them into taking specific actions that compromise security, like granting access to critical systems or making unauthorised payments.

SA3, Watering Hole Attack: The attackers target websites or online platforms that are frequently visited by employees or individuals, compromising legitimate websites in the

accounting field by injecting malware or exploiting vulnerabilities to gain unauthorised access or steal sensitive financial information.

According to Table 6.1, the game matrix, we have considered a scenario with only two players based on the hypothetical gain. Basic strategies and payoffs may vary depending on prevailing circumstances, as well as the priorities of the organisations and the effectiveness of security measures. Under this scenario, the Nash equilibrium is achieved when the attacker attacks and the Defender chooses to defend, regardless of the allocated security investment level, resulting in a defender payoff of +10. In contrast, the attacker incurs a payoff of -10, indicating a positive outcome for the Defender and an adverse effect for the Attacker. Additionally, the Attacker has an incentive to exploit the vulnerabilities. On the other hand, the defender strategy involves defending against social engineering attacks.

Considering Table 6.1 to find the Nash equilibrium and the optimal strategy for each player, we need to determine the best response strategy for each player against the other's strategies. To determine the optimal strategies for the attacker and defender, the payoff matrix presented in Table 6.1 is analysed using the Nash equilibrium concept, which identifies a stable strategy combination where neither player can improve their payoff by unilaterally changing their strategy.

The equilibrium is determined through best-response analysis. From the defender's perspective, the strategy that maximises security effectiveness while minimising expected loss is SD2, as this defensive configuration yields the highest payoff against the attacker's potential strategies. Conversely, from the attacker's perspective, the strategy SA1 produces the highest expected payoff given the defender's choice of SD2.

Because neither the attacker nor the defender can improve their outcome by changing their strategy independently once this pair of strategies is selected, the strategy combination (SD2, SA1) represents the Nash equilibrium of the game.

This equilibrium reflects a stable attacker-defender interaction in which the defender's chosen security configuration effectively limits the attacker's incentives to deviate from SA1, while any alternative defensive strategy would produce a less favourable outcome for the defender. For clarity, the equilibrium analysis presented here follows the Nash equilibrium framework consistently, and alternative solution concepts such as minimax are not applied in this matrix to avoid methodological ambiguity.

GTM Conceptual Model application

- i. Attack Intelligence (Input Layer): Phishing, Impersonation, Watering Hole
- ii. Matrix Computation Engine (Game Theory Model_Zero-Sum)
- iii. Nash equilibrium (resolved that SD2 neutralises even phishing, the attacker emails the accounting staff, and solves strategies)

iv. Defensive Planning Helps the finance department prioritise its email validation process and metadata forensics over generic awareness, enabling informed cybersecurity decisions and predictions.

RQ1: Integrates phishing threats and maps training defences into the GT model.

RQ2: Demonstrates core AIS protections needed (RBAC, sandboxing).

RQ3: Shows attacker preference for SA1 due to weak D1 defences.

RQ4: Advanced SD2 controls to adapt to Phishing emails from the attacker, an emerging threat

ii. **Matrix 2: Financial Attack Vector, Email Exploits & Vendor Fraud in Accounting**

A(Attacker) /D (Defender)	SA1	SA2	SA3	Min-loss (D)
SD1	(4, -4)	(0, 0)	(-5, 5)	-5
SD2	(2, -2)	(6, -6)	(1, -1)	1
SD3	(7, -7)	(3, -3)	(2, -2)	2
Max loss (A)	-7	-6	-2	(2,-2)

TABLE 6.2 Game Matrix 2

Another game matrix, as per

Table 6.2, has been considered. In this matrix, the numbers represent email-based threats used to manipulate accounting workflows:

SA1: Email Scam, Mass fraud emails requesting invoice updates or fake refunds.

SA2: Link Trap, Malicious links pretending to be internal login portals to harvest credentials.

SA3: Fake Invoice, Spoofed PDF invoices with believable metadata tricking AP (Accounts Payable) into payments.

The Defender against the above three threats or attacks is going to take the following strategies:

SD1: Basic Email Filters, Spam detection, blocklisting, and static filters only.

SD2: SOPs & Email SOP Training, Includes staff verification protocols (e.g., verify via call).

SD3: Finance-specific Filtering, Attachments scanning, metadata validation, and domain spoofing detection.

Now, using the step-by-step Nash Equilibrium, the first step is the calculation of the maximum of the minimum damages from the rows. After that, the calculation that needs to be done is to calculate the minimum of the maximum damages. As shown in the matrix, the Nash equilibrium is achieved at (SD3, SA3).

SA3 being the Fake invoice: Attacker monitors vendor billing patterns (e.g., quarterly invoices from supplier X). It then creates a near-identical invoice PDF with a slightly modified bank account. And then sends from a lookalike domain (e.g., @payr0llco.com instead of

@payrollco.com). Therefore, it is evident that if SD1 is used, it will have a high likelihood of approval. However, if SD3 is deployed, then the email flag, the metadata scanned, or even the file hash is verified.

GTM Conceptual Model application

- i. Attack Intelligence (Input Layer): Vendor impersonation and invoice spoofing
- ii. Matrix Computation Engine Game Theory Model (Zero-Sum)
- iii. Nash equilibrium (resolved that SD3 neutralises even sophisticated invoice spoofing, solving strategies)
- iv. Defensive Planning Helps the finance department prioritise its email validation process and metadata forensics over generic awareness, enabling informed cybersecurity decisions and predictions.

RQ1: Integrates invoice attack as a vector and prescribes SOP + AI scanning.

RQ2: Identifies technical email defence layers (robust filters, metadata scans).

RQ3: Predicts that attackers prefer Fake Invoices if weak SD1 is used.

RQ4: Shows how zero-sum modelling covers an evolving AP fraud pattern.

b. Stackelberg game

i. Matrix 1: Social Engineering via Phishing, Impersonation, and Watering Hole

The Stackelberg game, a strategic game used to create the game theory model, involves two players. One is the leader, who makes the first move in a decision.

The other is when the follower analyses the leader's decision and moves.

The leader, who serves as the organisation's cybersecurity manager, decides to enhance the organisation's security to mitigate cyber threats, particularly those related to social engineering.

Attacker(A) /Defence(D)	SA1	SA2	SA3
SD1	(-5, 5)	(-8, 8)	(-4,4)
SD2	(-7, 7)	(-6, 6)	(-3,3)
SD3	(-6,6)	(-5,5)	(-9,9)
Max-loss (A)	7	8	9

TABLE 6.3 Game Matrix 3

At the same time, the follower, being the Attacker, analyses the leader's action and makes their strategic attack decision accordingly. Here, the organisation's leader can either inculcate proper employee training or do nothing for the organisation.

Table 6.3, designed to simplify the table, shows the payoffs of the leader and the Attacker under various scenarios. Now, for the Leader (Defender), they choose security measures first. Moreover, the Follower (Attacker) observes the defender's strategy and responds optimally. The matrix setup is like (First value = Defender payoff, second = Attacker payoff) (positive values for Attacker mean successful attack). Under this scenario, the best response for the follower, the Attacker, is not to engage in any episode, as the Cybersecurity Manager of the Organisation has taken strategic steps to properly train its employees to counter the Attacker's attack, resulting in the Stackelberg equilibrium. Now, we will delve into the details of Table 6.3, a 3×3 matrix, and examine the options available to both the attacker and the defender.

Defender Strategies (SD) & Attackers' Nature of Cyberattacks (SA)

If the leader has three possible security measures to implement against social engineering attacks, and the attacker counters them through three possible cyberattacks:

Basic Training Awareness Only (SD1): security posters, occasional mail reminders, minimal protection.

Phishing Awareness + SOPs (SD2): includes verification steps, finance-specific SOPs, and multi-person approval chains.

2FAs & Threat Modelling (SD3): this combines MFAs, deception-based defences, and anomaly detection, trained on attacker behaviour.

The follower can choose between three types of attacks; these are classic social engineering threats used to bypass accounting security through human factors:

Phishing Email (SA1): Attacker targeting accountants with malicious links mimicking vendors or internal staff.

Impersonation Attack (SA2): The attacker calls or emails, pretending to be the CFO or auditor, and requests emergency payments.

Watering Hole Attack (SA3): The attacker infects legitimate finance-related websites, targeting victims in the accounting department who are likely to visit them.

The leader's objective is to minimise the Organisation's costs, while the follower's aim is to maximise their payoff. By analysing this game matrix, one can apply game-theoretic techniques to determine the Stackelberg equilibrium, which specifies the optimal strategies for both the leader and the follower.

In a Stackelberg Equilibrium (Leader-Follower), we will conduct a Step-by-Step analysis. In this scenario, the Defender chooses first (Leader), while the Attacker responds with the best response (Follower) based on the Defender's decision. For each Defender action, we analyse what the Attacker would choose to do.

Step 1: Evaluate the Attacker's best response for each Defender move

If Defender chooses SD1:

Attacker's payoff:

SA1=5

SA2=8 ← Max

SA3=4

→ Attacker picks SA2, Defender gets -8

If Defender chooses SD2:

Attacker's payoff:

SA1=7←Max

SA2=6

SA3=3

→ Attacker picks SA1, Defender gets -7

If Defender chooses SD3:

Attacker's payoff:

SA1=6

SA2=5

SA3=9←Max

→ Attacker picks SA3, Defender gets -9

Step 2: Defender compares outcomes:

Defender Strategy	Attacker Response	Defender's Payoff
SD1	SA2	-8
SD2	SA1	-7
SD3	SA3	-9

TABLE 6.4 Game Matrix 4

Note: The defender should choose SD2 to minimise the worst-case loss (i.e., -7 is better than -8 or -9 as coming in Table 6.4.

Stackelberg Equilibrium

The equilibrium is achieved when:

The Defender chooses SD2, i.e., Awareness + SOPs, and the Attacker responds with SA1, i.e., through phishing.

Outcome: Defender payoff = -7, Attacker payoff = 7

Cyberattack Flow (SA1_Phishing)

Attacker sends fake invoice emails with urgent subject lines ("Your payment is overdue"). It includes a link to the login portal that mimics the interface of internal finance software. After which, without SOP verification or link validation, an employee enters credentials or processes a fraudulent payment. The Defender SOPs and awareness reduce click rates and enforce multiple authorisations, thereby limiting the success of attacks.

Defender's Response (SD2_Phishing Awareness + SOPs)

The defender's actions include SOPs that mandate email origin verification, call-back confirmation, and two-person approval. Staff are trained to identify urgency manipulation and spoofed domains. Phishing simulation campaigns could reduce susceptibility to phishing attacks.

» **Integration of GTM with Cybersecurity Defence Strategy**

Now, considering the matrix in Table 6.3 and exploring the GTM model layers in the cybersecurity domain.

The first one is the Threat Vector Input: Social engineering in cybersecurity has well-known vulnerabilities that can be exploited by leveraging the human element to gain unauthorised access to information. Standard attack techniques include phishing, impersonation, and watering hole attacks. Phishing attacks are methods of deceiving people into revealing information they should not disclose by masquerading as a trustworthy individual. Impersonation attacks involve attackers impersonating legitimate users to gain access to systems. Watering hole attacks target specific groups by compromising websites they frequent to inject malware.

Next is strategic modelling in cybersecurity, which can be analysed using the Stackelberg sequential decision-making model. It is characterised by a leader-follower dynamic in which the defender leads and the attacker follows. [517]. In the context of cybersecurity, the defender takes the lead and establishes security measures; the attacker then optimises their approach to bypass these defences. This dynamic interaction can be analysed using game theory to identify equilibrium points where both parties' strategies are balanced, thereby minimising risk.

Next, we have the Equilibrium Selection. In cybersecurity, equilibrium selection means to conclude the optimal strategy for both the defender and the attacker. The defender plays first and sets up security measures; the attacker then optimises their approach to bypass these defences. This dynamic interaction can be analysed using game theory to identify equilibrium points where both parties' strategies are balanced, thereby minimising potential risks.

The last one is the Control Selection, which is important in designing effective cybersecurity defences. The awareness and SOPs are Nash-based optimal moves that balance costs and benefits. Awareness reduces the likelihood of social engineering attacks, and SOPs provide a systematic method for responding to potential threats, ensuring consistency and effectiveness. These measures form the core of a robust cybersecurity system and lead to a Nash equilibrium in which optimal defence moves are taken.

» **Integration and alignment with the research questions**

The Stackelberg matrix study provides a comprehensive answer to the primary research questions guiding our investigation.

Regarding RQ1, game theory can be integrated into social engineering scenarios, as illustrated by the game-theoretic defence strategy, such as proactive employee training and the use of SOPs, thereby reducing the success of phishing or impersonation attacks.

For RQ2, game theory can provide a fundamental building block for the core elements of a cybersecurity framework applied to accounting systems, such as verification routines, email validation, and multi-level approval workflows. In other words, a game-theoretic cybersecurity defence model for accounting systems.

For RQ3, the model predicts that attacks will shift towards phishing when the defender proactively deters other potential attacks. It allows defenders to anticipate and prevent adversarial moves.

Finally, for RQ4, the Stackelberg approach is sufficiently resilient against new cyber threats, such as AI-generated phishing emails and adaptive impersonation attacks, demonstrating the flexibility and robustness of the GTM-based defence framework when designed using equilibrium modelling.

ii. Matrix 2: Credential Harvesting in Cloud Accounting Systems

Defender Strategies (SD) & Attackers' Nature of Cyberattacks (SA)

These are identity-driven attacks targeting user authentication systems within Accounting SaaS or Cloud ERP platforms.

Attackers' Action as shown in Error! Reference source not found. being the SA1, SA2 and SA3 are:

Credential Harvesting (SA1), phishing sites or stolen password dumps reused against finance portals.

Attacker(A) /Defence(D)	SA1	SA2	SA3
SD1	(-2, 2)	(3, -3)	(-4, 4)
SD2	(1, -1)	(6, -6)	(2, -2)
SD3	(7, -7)	(5, -5)	(4, -4)
Max-loss (A)	-7	-6	-4

TABLE 6.5 Game Matrix 5

Keylogger Malware (SA2), installed through drive-by downloads, logs credentials of finance staff.

Spoofed Email Login (SA3), Fake system alerts (e.g., “Your finance session expired”) redirect users to mimic legitimate login portals.

While the Defender’s Strategies are the SD1, SD2, and SD3:

Basic (SD1), Username-password combos, no MFA or anomaly detection.

Moderate (SD2) adds 2FA, logs all sessions, and supports IP-aware policies.

Advanced (SD3), Uses Identity Access Management (IAM), AI-based behavioural alerts (e.g., location/device mismatch).

Now we are going to calculate the Nash Equilibrium manually (Zero-Sum):

The first step: Step 1: Defender, Worst-case (min row)

SD1: $\min(-2, 3, -4) \rightarrow -4$

SD2: $\min(1, 6, 2) \rightarrow 1$

SD3: $\min(7, 5, 4) \rightarrow 4$

Defender chooses the maximum of the minimum SD3

Step 2: Attacker, Best-case (max column)

SA1: $\max(2, -1, -7) \rightarrow -7$

SA2: $\max(-3, -6, -5) \rightarrow -6$

SA3: $\max(4, -2, -4) \rightarrow 4$

Attacker chooses the minimum of the maximum SA3

Result: Hence our Nash Equilibrium is: (SD3, SA3) $\rightarrow (4, -4)$

» **Credential Harvesting via Spoofed Login Pages and Defensive Mitigation**

The attacker uses a spoofed email phishing attempt to launch a credential-harvesting campaign targeting accounting staff. The attack starts with an email purporting to be a security alert, such as the opening message from “QuickBooks Finance Admin” indicating a session timeout or suspicious login activity. This abuse of trust leverages the fact that finance professionals use familiar financial platforms. The message contains a link to a counterfeit login portal that closely mimics the genuine interface of the targeted accounting system. Without noticing the inconsistencies, the user, who is often in a hurry or distracted, will enter their username and password into the fake portal. The attacker silently copies these credentials. Suppose the system is not MFA-enabled or otherwise lacks context-based login detection. In that case, the attacker can immediately leverage the stolen credentials to gain illicit access to the cloud financial system. This attack is a classical social engineering method that manipulates the targeted users but does not exploit technology. According to [521], phishing attacks are among the most effective means of breaching cloud-based enterprise environments, especially in finance-oriented industries such as accounting, where financial urgency creates high trust in communications. The defender reacts with SD3 – the most advanced security approach that combines IAM and AI-based threat analytics. These defences utilise user behaviour analytics and context-based analysis to evaluate login attempts (e.g., time, device, location, network signature). If the system detects anomalies (e.g., a login from an unfamiliar IP address or at an unusual hour), it identifies the session as suspicious, blocks access and alerts the user. It ensures that even if phishing succeeds, the attacker cannot profit from the stolen credentials, and the chain of attacks is broken. This example directly maps to the GTM framework, where attack-defence strategies are modelled in a payoff matrix, and the Nash equilibrium is reached when the defender plays the SD3 strategy, minimising risk based on its prediction of the attacker's likely behaviour.

» **Integration of GTM with Cybersecurity Defence Strategy**

The GTM provides a structured, predictive modelling approach for simulating, evaluating, and optimising resource-constrained cybersecurity strategies. In **Error! Reference source not f**

ound. which models a triad of spoofing-based social engineering attacks (phishing, malware, credential harvesting) against a range of defensive strategies, each stage of GTM is operationalised directly as illustrated below:

- **Threat Simulation:** Simulates realistic attacker behaviours for SA1, SA2, and SA3, including phishing, keylogging, and spoofed vendor email targeting cloud-based accounting systems
- **Matrix Formulation:** Constructs a payoff matrix like **Error! Reference source not found.**, where each cell represents a cost-benefit interaction between SD1-SD3 defensive strategies vs SA1-SA3 attacks.
- **Nash Solver:** Applies Nash Equilibrium to find optimal defender response, assuming rational attacker behaviour - here SD3 as dominant strategy
- **Budget-aware Response:** Accounts for potentially higher costs associated with a more robust SD3 (IAM + Threat Analytics), but aligns with the lowest breach risk, which aligns with the GTM cost-effectiveness aim.

» **Integration and alignment with the research questions**

The matrix-based modelling presented in this chapter contributes to addressing the research questions by illustrating how attacker–defender interactions in accounting information systems can be analysed using game-theoretic reasoning. Game theory has been widely applied in cybersecurity research to model strategic conflicts between attackers and defenders and to analyse optimal defensive strategies under uncertainty [140, 505]. However, it is important to distinguish between conceptual demonstration and empirical evidence when interpreting the results of the matrices.

First, at the conceptual level, the game-theoretic framework demonstrates how strategic interactions between attackers and defenders can be represented through payoff matrices and equilibrium analysis. Game-theoretic models enable researchers to analyse adversarial behaviour by representing attacker and defender choices within structured decision environments and identifying equilibrium strategies that capture stable outcomes [140, 522]. The matrices illustrate how different combinations of defensive controls (e.g., authentication mechanisms, monitoring systems, or training measures) influence the expected behaviour of attackers and the resulting cybersecurity outcomes. In this sense, the model shows how attacker preferences and defender strategies can be analysed within a structured decision framework.

Second, at the empirical level, publicly available cybersecurity datasets such as CIC IDS 2017 and the CERT Insider Threat dataset were used to inform the construction of realistic threat scenarios and attack categories included in the matrices. Benchmark cybersecurity datasets are commonly used in academic research to analyse attack behaviour and evaluate defensive mechanisms where organisational security data cannot be publicly disclosed [519, 520]. These

datasets provide examples of common attack behaviours, intrusion patterns, and insider misuse events, which guided the parameterisation of the modelling scenarios. However, the equilibrium outcomes themselves represent analytical results derived from the game-theoretic structure rather than direct empirical measurements.

Consequently, the matrices should be interpreted as analytical demonstrations of strategic cybersecurity dynamics rather than empirical predictions. Their primary contribution lies in illustrating how game-theoretic modelling can support decision-making in accounting cybersecurity by identifying stable attacker–defender strategy combinations under defined assumptions [140, 505].

The approach presented also directly addresses the four main research questions (RQs) of the study, as shown below:

RQ1: How can game theory + social engineering be brought into a cybersecurity framework? Phishing, keylogging, and spoofed email attacks are mapped to defensive strategies, such as IAM, behavioural analytics, and 2FA, using a game-theoretic matrix model.

RQ2: What is included in a framework to defend against social engineering? IAM, log systems, and behaviour AI emerge as key controls, reflected in the selected optimal strategy (SD3)

RQ3: How can attacker behaviour be predicted? Using a matrix-based equilibrium, the model shows that attackers prefer SA3 (spoofed email) over weak defence SD1, indicating that attacker preferences are predictable.

RQ4: How does a framework defend against emerging cyber threats? SD3 (IAM + AI analytics) is a future-proof model designed to combat emerging direct threats, including AI-generated phishing emails and new spoofing techniques.

Relevance of the Example to Research and Conceptual Model

This example is grounded in the “Decision Matrix” layer of the GTM conceptual framework, and it exemplifies how preemptive, intelligence-driven defences (IAM + AI) can change attacker incentives. The modelling also addresses some of the research questions raised:

RQ1 (Integration) - It integrates game theory with real-world phishing tools, demonstrating that a proactive strategy reduces vulnerability.

RQ2 (Framework Components): It highlights IAM, behavioural analysis, and anomaly detection as key components.

RQ3 (Predicting Attacker Behaviour): The model predicts that attackers will favour spoofed emails if the defender deploys basic defences (SD1, SD2).

RQ4 (New Threats): It addresses modern AI-powered phishing attacks by countering them with adaptive AI defences

Key implications for accounting systems security:

Error! Reference source not found. features real-world threats to financial workflows, including fake invoice emails spoofing vendors, keyloggers to capture login credentials, and phishing of session tokens in cloud ERPs (e.g., NetSuite, QuickBooks).

The GTM model provides a diagnostic and prescriptive framework for AIS by

- ❖ Quantifying payoff risk levels for different control investments
- ❖ Simulating attacker-defender interactions
- ❖ Helping CFO/CISO prioritise controls that minimise breach impact per unit cost

By operationalising the GTM in **Error! Reference source not found.** The research has met its conceptual and objective parameters. The Nash-selected strategy SD3, although expensive, is effective at deterring high-probability attacks while adapting to new social engineering approaches, delivering a robust, rational, and cost-effective defence strategy for the accounting system.

6.5.2. General Observations

The GTM framework validation through the matrix modelling was successful. Nash Equilibrium strategies have proven to be an effective means of modelling and predicting attacker behaviour and choice. The matrix outputs represented quantifiable risk postures, providing an explicit cost-benefit analysis. The GTM structure was shown to be extensible to new datasets or emerging threats. Lastly, the equilibrium strategies uncovered were aligned with industry best practices, verifying the theoretical model.

Based on the research findings, it was determined that the GTM-based matrix modelling serves as both a robust analytical tool and a practical tool for real-world application to bolster cybersecurity in accounting systems. The framework enables accounting practitioners to forecast attacker decision-making, prioritise defences, and achieve strategic resiliency with minimal resource waste.

6.5.3. Discussion– Based on Research Questions

This section provides a comprehensive academic discussion based on the core research questions of this thesis, synthesising the Game Theoretic Methodology (GTM), Zero-Sum and Stackelberg games, and the Nash Equilibrium in the context of cybersecurity in accounting information systems.

a. RQ1

How can game theory and SE tools be integrated into a comprehensive cybersecurity framework to detect and prevent cyber-attacks effectively, and what are the most effective strategies for implementation and management?

The integration is achieved through the application of Game Theory Modelling (GTM), which structures cybersecurity interactions as strategic games between rational attackers and defenders [484]. Social engineering scenarios, such as phishing, pretexting, and baiting, are modelled using Zero-Sum matrices, in which the attacker's gains equal the defender's losses [485]. For proactive defence, Stackelberg games are deployed, wherein the defender (leader)

pre-commits to security controls (e.g., access restrictions, AI detection systems), anticipating optimal responses from the attacker (follower) [523]. Nash Equilibrium determines the strategy profiles from which no party can deviate unilaterally, ensuring stability in system responses. Combining GTM data-driven modelling with attacker-defender matrices effectively represents interactions between technical attacks and human-based vulnerabilities. Using payoff matrices, this research incorporated social engineering vectors (e.g. phishing, impersonation) into defence strategy design, allowing for multi-layered prevention strategies.

✚ **Outcome:** Game theory models provide a structured approach to designing proactive controls (e.g., SOPs, employee training, deception-based methods) that optimise attacker behaviours.

b. RQ2

What key components should be included in a cybersecurity framework based on game theory to deal with social engineering attacks successfully?

A robust GTM framework addressing social engineering requires: (1) defined actor utility functions (attacker incentives, defender costs), (2) empirical or hypothetical matrix construction for various threat vectors, (3) zero-sum and Stackelberg formulations for reactive and pre-emptive defense, respectively, (4) computation of Nash Equilibria, and (5) continuous re-evaluation based on emerging attack methods. [517]. These components ensure that the framework adapts to dynamic, human-centric threats inherent in social engineering. The GTM model highlights three core components: attack path mapping, matrix modelling of strategies, and equilibrium-based control selection. Matrix scenarios effectively model that a strong defence against social engineering includes two-factor authentication (2FA), behavioural analytics, awareness programs, and role-based access control.

✚ **Outcome:** The framework helps determine which human- and/or technical-based controls to implement based on the modelled attacker utility, ensuring the most cost-effective and optimal setup for resiliency.

c. RQ3

How can the attacker's behaviour be predicted using game theory, and how can an analysis be conducted to evaluate the use of this information in enhancing the effectiveness of the cybersecurity framework?

Game theory predicts attacker behaviour by analysing the attacker's payoff-maximising strategies under defined conditions. In Zero-Sum models, where both players act simultaneously, equilibrium strategies indicate how attackers respond to varying defense configurations. In Stackelberg settings, the defender can constrain the attacker's choices through initial strategy signalling. Both models utilise Nash Equilibrium to identify stable strategies [484, 523]. Through matrix simulations using threat data (e.g., CIC IDS 2017, CERT Insider Threat), the framework assesses how adjustments to the risk surface or control effectiveness alter attacker incentives, thereby informing more adaptive defences. All matrix

scenarios using Nash Equilibrium showed consistent trends in attacker responses - i.e., they would choose softer targets unless deterred. By adjusting matrix inputs based on real-world indicators (e.g. rate of user neglect, rate of phishing susceptibility), organisations can "fine-tune" their defence strategy.

✚ **Outcome:** Attacker behaviour becomes more predictable through strategic modelling, allowing for tailored defences that preempt likely breach methods.

d. RQ4

How can this game theory-based cybersecurity framework address the prevailing cybersecurity threat and manage the challenges of emerging cyber threats?

GTM's matrix-based design and equilibrium-driven strategy formulation offer scalability and adaptability. As new threats, such as quantum-resilient malware or AI-driven exploits, emerge, new matrices can be constructed and solved using the same principles. Stackelberg models are particularly well-suited for addressing emerging threats by incorporating deterrence through leader precommitment [517]. The equilibrium concept ensures that even under uncertainty, defenders can develop robust control portfolios. Matrix-based modelling is dynamic and flexible and can be adapted to model new attack vectors (e.g., zero-day, AI-driven spear phishing) by simply adjusting the payoff structure accordingly. Stackelberg scenarios demonstrated that robust pre-commitment strategies (e.g., full logging, strict access protocols) could deter even new and adaptive attacks.

✚ **Outcome:** The framework is "forward compatible" so that when new attack scenarios emerge, accounting systems can remain resilient without having to be completely redesigned. Together, GTM, Zero-Sum, and Stackelberg game models, along with the application of Nash Equilibrium, create a scientifically grounded, empirically verifiable, and policy-relevant cybersecurity framework. The model not only informs optimal defensive strategies but also provides a diagnostic tool for understanding the underlying economics and psychology of adversarial interactions in accounting information systems.

The findings indicate that cyber-attacks in accounting systems are best understood as strategic interactions rather than isolated vulnerabilities. Social engineering exploits organisational trust structures, while internal control override reflects calculated optimisation of risk versus reward. Game-theoretic models thus provide deeper explanatory power than traditional cybersecurity analysis by capturing the incentives, constraints, and decision sequences of adversaries. These insights validate the need for defensive strategies that dynamically adjust to evolving attacker behaviour — a capability embedded within the broader BQMG-AIS framework.

6.6. Contributions of the Study

This research provides several unique and influential contributions to cybersecurity, information systems in accounting, and decision sciences in strategy, specifically using game-theoretic models:

6.6.1. Interdisciplinary Integration of Game Theory in Accounting Cybersecurity

This work innovates the application of Game Theory, specifically Zero-Sum and Stackelberg games, in the field of accounting cybersecurity. Integrating technical cybersecurity models with behavioural knowledge from social engineering creates an integrated, interdisciplinary framework for protecting sensitive accounting systems. [485].

6.6.2. Matrix-Based GTM Framework Development

The research operationalises Game Theoretic Methodology (GTM) through whole-matrix-based modelling. Its value proposition lies in illustrating that actual cybersecurity scenarios, such as phishing attacks and privilege abuse, can be formalised in strategic matrices to model attacker-defender interactions and compute Nash Equilibria [484].

Scenario-Based Cyber Threat Modelling for Accounting Systems: The research demonstrates, through six detailed scenario matrices, the approach to modelling and solving for strategic outcomes in realistic threat environments. The chosen scenarios are custom-designed for the accounting sector and present an executable model that helps organisations anticipate threats and create optimised defence strategies [523].

6.6.3. Strategic Defence Prioritisation based on Equilibrium Outcomes

This research provides actionable insights into prioritising cybersecurity investments. By mapping out equilibrium points, decision-makers can allocate scarce resources to the most beneficial defence strategies (e.g., 2FA, access monitoring, AI-based intrusion detection) against specific attacker behaviours [484, 517].

Practical Application to Policy and Control Design: The equilibrium-based methodology enables cybersecurity architects, IT managers, and auditors to make mathematical results actionable through explicit cybersecurity policies, such as awareness training timetables, protocol hardening techniques, and control layering strategies. It eliminates the commonly described disconnect between theory and practice[523].

6.6.4. Adaptation and Extension for Future Threats

The modularity of the GTM model's matrix structure enables it to adapt to new attack vectors and emerging technologies. Therefore, the research presents an extensible framework that can be reused or extended by practitioners and future researchers to address future cybersecurity challenges, such as those posed by artificial intelligence (AI) or quantum computing [484, 517].

6.7. Conclusions

This thesis demonstrates the significant benefits of applying Game Theory through the Game Theoretic Methodology, including Zero-Sum Games, Stackelberg Games, and Nash Equilibrium, in enhancing cybersecurity in AIS against social engineering attack risks. Through the modelling of 3x3 matrices based on real (CIC IDS 2017 and CERT Insider Threat) and synthesised datasets with the solution of such matrices based on the most advanced equilibrium, this research provided the following main results:

Integrated Defence: The fusion of technical controls with proactive, human-centred defences (Zero Trust Architecture, Role-Based Access Control, and Awareness Training) reduces the likelihood of an attacker succeeding. The prediction of Attacker Behaviour: The Nash Equilibrium analysis is a practical tool to provide insight into how attackers change their behaviour in response to the actions of defenders. The defender can proactively influence the attacker's behaviour. The third is Investment Optimisation: Game-theoretic modelling can assist in the optimal allocation of cybersecurity resources, allowing defenders to focus their investments where they will be most effective in deterring attacks. Another key aspect is **Framework Adaptability:** The GTM-based methodology is naturally versatile and can be easily adjusted to model emerging threats, including AI-driven attacks or developments in quantum computing. Finally, Bridging Theory and Practice: This approach connects theoretical game theory with the practical needs of cybersecurity professionals by providing clear recommendations for designing policies and controls in the accounting domain.

We will now consider the research questions 1 to 4 under Section 6.1.4 and provide brief responses to each, which are addressed in detail in Section 6.5. The first step in integrating game theory and social engineering tools was achieved through the GTM-based model framework. The second one, related to the key components identified, includes proactive architectural controls, adaptive monitoring, and human-centred defences. The third one responded by effectively utilising Nash Equilibrium analysis, which predicts attacker behaviour and guides dynamic defence adjustments. The last one was responded to by considering the framework as adaptable and scalable to address both current and emerging cybersecurity threats.

The intersection of Game Theory with cybersecurity modelling for AIS provides a robust, scientifically sound method for tackling complex threat landscapes. In this research, a foundation is laid for the continued development of this cross-disciplinary field, and both theoretical and practical enhancements to the security of accounting systems are provided.

6.7.1. Game Theory and BQMG-AIS Integration

Within the BQMG-AIS framework, the game-theory layer provides a strategic defence dimension by modelling adversaries' behaviour and enabling proactive decision-making. By incorporating attacker–defender payoffs, threat likelihoods, and adaptive strategies, the game-theory layer complements blockchain immutability, quantum-secure cryptographic mechanisms, and machine-learning-based anomaly detection. This integration ensures that the framework not only detects anomalies but also anticipates attack paths, supports dynamic resource allocation, and enhances resilience against social engineering and internal manipulation — threats that purely technical controls cannot fully mitigate.

6.8. Future Research

This work intends to establish a foundation for incorporating Game Theory into social engineering models for cybersecurity practices in accounting information systems. However,

as the cyber threat landscape evolves and becomes more complex, many promising directions remain for future research.

Multi-Actor and Incomplete Information Games.

Future research can extend the GTM framework to model multi-player game theory, such as simultaneous actions by insider threats, third-party vendors, and Advanced Persistent Threat (APT) groups. Incomplete information games, Bayesian games, and others could also improve modelling realism when complete data about attacker intentions or defender resources are unavailable [484].

6.8.1. Real-Time Matrix Adaptation using Threat Intelligence Feeds

Linking real-time matrices (e.g., SIEM, IDS/IPS alerts, threat intelligence platforms) with matrix models would help organisations dynamically update Nash Equilibrium results and improve defence responsiveness in both Zero-Sum and Stackelberg setups [517].

6.8.2. Behavioural Game Theory for Social Engineering

While traditional game models assume rational behaviour, social engineering often exploits irrational human behaviour. Behavioural game theory can compensate for this modelling weakness by capturing heuristics, bounded rationality, and cognitive bias. It would especially benefit defence strategies in accounting departments, where policy fatigue or habitual responses play into the attackers' advantage [485].

6.8.3. Post-Quantum Game-Theoretic Security

With quantum computing on the horizon, cryptographic assumptions are beginning to deteriorate. Future research could examine how quantum-resistant strategies might shift the attacker-defender equilibrium. Stackelberg games with stochastic components could effectively model such pro-cyclic scenarios [523].

6.8.4. Automated Cyber Defence with Machine Learning and GTM

Machine learning algorithms could automatically populate the matrix and select a strategy. Hybrid models combining GTM with reinforcement learning or DQN could adapt the equilibrium strategies over time, leading to near-autonomous cyber defense tools for accounting systems.

6.8.5. Sectoral Adaptation and Empirical Case Studies

While this thesis is accounting-centric, the GTM-based matrix approach is equally applicable to other financial systems, such as banking, auditing, and ERP systems. Sectoral case studies can be used to validate the generalizability and robustness of the proposed approach.

6.8.6. Quantitative ROI Models for Cyber Investment

Future researchers can also develop quantitative return-on-investment (ROI) models based on game-theoretic outcomes for cybersecurity decisions. It bridges the gap between security strategy modelling and financial justification, which is critical for adoption by accounting managers and CFOs.

The game-theoretic analysis has provided a comprehensive understanding of how rational actors systematically influence cybersecurity outcomes within accounting systems. By examining the motivations and behaviours of these actors, the study reveals critical dynamics that can impact security measures and responses to threats. Building upon these conceptual insights, the thesis now advances to the empirical validation stage, which is essential for assessing the practical implications of the theoretical framework.

In Chapter 7, an in-depth evaluation of machine learning-based fraud detection models is conducted across a diverse range of real-world datasets. This chapter not only assesses the predictive accuracy of these models, that is, their ability to detect fraudulent activities, but also examines their interpretability, ensuring that the models' results are clear and understandable. Furthermore, the analysis includes a rigorous assessment of cross-context generalizability, determining how well these models perform across different environments and scenarios. This multifaceted evaluation aims to substantiate the theoretical findings presented in the preceding chapters, thereby enhancing our understanding of how advanced analytical techniques can bolster cybersecurity efforts in accounting systems.

Chapter 7

7. Artificial Intelligence Driven Cybersecurity in Accounting: A Multi-Stream Fraud Detection Framework Using ML

7.1. Introduction

7.1.1 Background

Integrating machine learning (ML) into cybersecurity frameworks has become increasingly significant, particularly in accounting sectors where sensitive financial data is at risk. The rapid advancement of technology has led to a surge in cyber threats, necessitating robust security measures to protect digital assets. Machine learning offers a promising solution by enhancing the detection and mitigation of these threats through its ability to process large volumes of data and identify patterns indicative of malicious activities [524].

The researcher [438] mentions a notable gap in applying ML specifically for accounting cybersecurity. While ML models have been developed for general cybersecurity purposes, their adaptation to the unique requirements of accounting systems remains limited, as the researcher clarifies. He pointed out that accounting systems often involve complex data structures and specific regulatory requirements necessitating tailored ML solutions. Addressing this gap requires the development of specialised models that can effectively integrate into existing accounting frameworks and provide robust security measures. Overall, integrating machine learning into cybersecurity for accounting offers a promising avenue to enhance the protection of sensitive financial data. By leveraging the capabilities of ML algorithms, accounting systems can achieve more efficient threat detection and response, ultimately improving their overall security posture[525].

Machine learning and cybersecurity concepts have been extensively defined in earlier chapters and the broader literature; therefore, this chapter focuses specifically on their intersection within accounting information systems. Rather than reiterating foundational definitions, the emphasis here is on how machine learning techniques can be operationalised to address cybersecurity challenges unique to accounting environments, including fraud detection, auditability, and regulatory compliance. This shift enables a more analytical treatment of the topic, aligning with the study's objective of advancing theory-informed applications of machine learning in accounting cybersecurity contexts [92, 301].

a. Overview of cybersecurity in accounting and finance

Cybersecurity has become a critical concern in the accounting sector due to the increasing reliance on digital systems and the sensitive nature of financial data. The integration of technology in accounting and finance processes has exposed these systems to cyber threats, necessitating robust security measures to protect against data breaches and unauthorised access [526]. The digital transformation in accounting and finance has led to the adoption of cloud-based solutions and IoT devices, which, while enhancing efficiency, have also introduced new

vulnerabilities[527]. As cybercriminals become sophisticated, the need for advanced cybersecurity strategies in accounting and finance [528] is more pressing than ever [438].

The study [352] discusses Cybersecurity, noting that it is a broad, multifaceted concept that integrates information security and information assurance, serving as a critical safeguard in the digital landscape [529]. Further, the researcher explains that it encompasses protecting sensitive data as it is accessed, processed, and transmitted across various computer networks, shielding it from potential threats such as cyberattacks, unauthorised access, and data breaches [528]. Cybersecurity plays a fundamental role in securing digital assets and maintaining trust in an increasingly interconnected world by ensuring the confidentiality, integrity, and availability of information.

The study [347] discusses cybersecurity in detail in today's digital era, where cybersecurity is essential for protecting systems, networks, and technologies from unauthorised access and cyber threats. As businesses increasingly rely on digital infrastructure, having a dedicated cybersecurity team is crucial for monitoring potential threats and proactively implementing strategies to mitigate risks. Figure 7.1 illustrates cybersecurity's core components, including secure payment systems, user online privacy, antivirus firewalls, mobile security, data protection, security padlocks, computer protection, and a comprehensive global security shield. For businesses that handle electronic payments and transactions, ensuring robust payment security is critical to information security. Further, he explains that staying updated with the latest advancements in e-commerce security and adopting best practices for secure transactions is imperative for safeguarding financial data and maintaining customer trust. In his research, the researcher is considering a framework to achieve the research objectives; a cybersecurity framework incorporating artificial intelligence has been utilised. Specifically, algorithms such as the K-Nearest Neighbours (KNN) and the Enhanced Encryption Standard (EES) encryption and decryption methods have been applied to enhance security, demonstrating the potential of AI-driven methodologies to strengthen digital defences [347].



FIGURE 7.1 Essential elements of cybersecurity in financial management

SOURCE: [347]

The study [530] explains that cybersecurity involves protecting system nodes, data, and networks from damage, loss, illegal access, and other cyber threats, which are becoming more sophisticated and frequent. The accounting and finance industry handles vast amounts of sensitive financial information and is particularly vulnerable to these threats, making robust cybersecurity measures essential. Cyber threats, such as malware, phishing, and distributed denial-of-service (DDoS) attacks, are common and can severely impact accounting and finance systems. Malware, for instance, refers to malicious software designed to damage or exploit computers. At the same time, phishing involves deceiving individuals into divulging private information, such as passwords or bank account details. Cyber threats can lead to significant financial losses and damage an organisation's reputation.

b. Introduction to Machine Learning

[531] Machine learning (ML) is a subset of artificial intelligence that focuses on developing algorithms that learn from data and make predictions. It has gained prominence across various fields, including cybersecurity, for its ability to process large volumes of data and identify patterns that may not be apparent to human analysts. ML techniques, such as supervised, unsupervised, and reinforcement learning, offer diverse applications in anomaly detection, fraud prevention, and risk management.

c. The role of machine learning in enhancing cybersecurity measures

[531] Machine learning improves cybersecurity by automating threat detection and response processes. ML algorithms can analyse vast datasets to identify anomalies and potential security threats, enabling organisations to respond swiftly and effectively. ML can detect fraudulent activities, monitor user behaviour, and predict potential security breaches in accounting and finance, strengthening the overall security posture.

The study [532] discusses Artificial Intelligence, specifically Machine Learning (ML), explaining how it is pivotal in enhancing cybersecurity by equipping systems with the intelligence to recognise complex patterns and predict emerging data threats [533]. By optimising data processing and refining training methodologies, ML-driven models can proactively detect and mitigate suspicious activities, including spyware and other malicious intrusions [534, 535]. Further research highlights machine learning as a groundbreaking technology that enables cybersecurity systems to evolve continuously, learning from vast datasets and adapting to new and sophisticated attack vectors in real-time. Unlike traditional rule-based security approaches, the researcher noted that ML-powered solutions can autonomously analyse threats and make informed decisions without explicit programming, significantly strengthening digital defences [536].

d. The need for advanced cybersecurity solutions tailored to accounting and finance systems

Traditional cybersecurity measures may not be sufficient to address the unique challenges accounting and finance systems face. The dynamic nature of cyber threats necessitates the development of advanced solutions that leverage machine learning to provide real-time threat detection and response capabilities [526]. Tailored cybersecurity solutions can help accounting and finance firms protect their digital assets, maintain data integrity, and ensure compliance with industry regulations[526].

Credit cards and digital wallets often provide better security features than debit cards, including fraud protection and chargeback options in case of unauthorised transactions. It is best to avoid entering financial details on unfamiliar or unsecured websites whenever possible. Reviewing bank statements, transaction histories, and credit reports can help detect any unauthorised activity early. Setting up account alerts for unusual spending patterns or large transactions can provide real-time notifications of potential fraud. If suspicious activity is detected, it must be reported to the financial institution immediately to prevent further losses. In cases of significant fraud, notifying relevant authorities can help track down cybercriminals and avoid future incidents [525].

7.1.2 Theoretical Framing of Machine Learning in Accounting Cybersecurity

Machine learning (ML) in this chapter is positioned not merely as a technical tool for fraud detection but as a mechanism that extends established theoretical perspectives within Accounting Information Systems (AIS), audit analytics, and cybersecurity governance. From an AIS perspective, ML enhances the effectiveness of internal control systems by enabling continuous monitoring, anomaly detection, and automated validation of financial transactions. This aligns with internal control theory, which emphasises monitoring activities, control effectiveness, and risk mitigation in ensuring the reliability of financial reporting [25]. By embedding ML within AIS, this study advances the role of intelligent systems in strengthening audit trails, transaction integrity, and real-time assurance capabilities [537].

From an audit perspective, the application of ML directly contributes to audit risk theory, particularly by reducing detection risk through advanced analytical procedures. Machine learning models such as Random Forest and XGBoost improve the auditor's ability to identify material misstatements and fraudulent transactions within highly imbalanced datasets, thereby extending audit analytics practices in contemporary accounting environments [98, 300]. Furthermore, the integration of explainability techniques such as SHAP supports audit transparency and interpretability, which are critical for regulatory compliance and assurance [331].

In addition, this chapter adopts a socio-technical systems perspective, recognising that cybersecurity in accounting is shaped by the interaction between technological, organisational, and human elements. Machine learning models operate within this broader system by augmenting human decision-making, supporting governance structures, and enabling adaptive responses to evolving cyber threats [538]. Accordingly, this study contributes to AIS and

cybersecurity governance literature by demonstrating how ML can be theoretically embedded within accounting systems to enhance control effectiveness, audit assurance, and organisational resilience.

7.2. Experimental Design

The experimental design of this study is based on integrating research aims, objectives, questions, and hypotheses into a coherent methodological framework. This section explains how the empirical strategy is developed to ensure alignment between theoretical intent and practical implementation. By linking research questions to specific objectives and hypotheses, the study provides transparency, logical consistency, and a clear plan for empirical validation.

7.2.1 Research Aim

The primary objective of this study is to design, implement, and empirically validate a multi-stream machine learning framework tailored explicitly for fraud detection in accounting and financial systems. This objective involves assessing vulnerabilities in existing financial infrastructures and evaluating the performance efficacy of various machine learning model classes, including linear, ensemble, and boosting models, across multiple datasets and scenarios.

7.2.2 Research Objectives

a. To analyse the current state of cybersecurity in accounting and finance systems

This objective seeks to systematically evaluate the existing cybersecurity measures in accounting and finance, identifying vulnerabilities, inefficiencies, and gaps that make these systems attractive targets for fraud and cyberattacks. Studies show that accounting systems are increasingly vulnerable due to their reliance on interconnected infrastructures and digital payment channels [539]. By critically examining current practices, such as firewalls, static audit trails, and intrusion detection systems, this objective identifies where these measures fall short in addressing dynamic and adaptive cyber threats. The analysis will directly contribute to addressing RQ1 (Detection Effectiveness) by establishing a baseline of weaknesses that machine learning could potentially resolve.

b. To explore the application of machine learning in accounting and finance cybersecurity

This objective examines how machine learning can enhance cybersecurity measures in financial ecosystems, with a particular focus on fraud detection and prevention. The emphasis is on how domain-adapted ML models can be tailored to the unique characteristics of accounting records, financial statements, and transaction data [530]. For example, supervised models (e.g., Random Forest, Logistic Regression) provide robust classification capabilities, while anomaly-detection approaches (e.g., Isolation Forest, autoencoders) can detect novel fraud patterns overlooked by static systems. This exploration builds directly on RQ2 (Performance Trade-offs) by evaluating whether ML models can balance precision, recall, and interpretability in accounting contexts.

c. To develop machine learning models for detecting and preventing cyber threats in accounting and finance

The third objective operationalises the research aim by designing and implementing machine learning models to effectively detect and mitigate fraudulent activity in accounting environments. This involves a comparative analysis of different algorithmic paradigms, including supervised (e.g., Random Forest, XGBoost), unsupervised (e.g., anomaly detection), and hybrid approaches, benchmarking their performance against the extreme class imbalance typical of fraud datasets [530]. This objective contributes to RQ1 and RQ2 by testing H1 and H2, determining whether ensemble and boosting models outperform linear approaches in fraud detection.

d. To integrate explainability techniques into fraud detection systems for improved auditability and compliance

A core challenge in applying machine learning to accounting is the lack of interpretability, which undermines its usefulness in highly regulated environments. This objective focuses on incorporating explainable AI methods, such as SHAP (SHapley Additive exPlanations), into the fraud detection framework. By doing so, the research aims to ensure that model predictions are transparent, auditable, and acceptable to regulators and auditors [331]. This objective directly addresses RQ3 (Explainability and Compliance) and tests H3 by examining whether interpretable models, or models enhanced with SHAP, produce calibrated outputs suitable for regulatory scrutiny.

e. To establish methodological best practices for transparent, reproducible, and reliable ML workflows in accounting cybersecurity

The final objective is to synthesise insights from the experimental validation into a set of methodological best practices. This includes dataset preprocessing protocols (handling imbalance and feature engineering), evaluation metrics beyond accuracy (ROC-AUC, PR-AUC, and calibration), and deployment strategies such as dashboard integration for real-time monitoring. The purpose is to provide a reproducible workflow that practitioners and researchers across different accounting and finance contexts can adapt [540]. This aligns with RQ4 (Best Practices in ML Workflows) and tests H4 by exploring cross-dataset validation and generalizability.

7.2.3 Research Questions

The methodology is structured to answer the following key questions:

1. How effectively do state-of-the-art ML models detect fraudulent activity in accounting and transaction systems, specifically within highly imbalanced, real-world financial datasets?
2. What are the operational tradeoffs, precision, recall, F1-score, ROC-AUC, and PR-AUC of these models, both overall and for the minority (fraud) class?
3. How do model explainability and feature importance (via SHAP) inform auditability and compliance considerations for accounting professionals and regulators?

4. Can methodological best practices be established for robust, transparent machine learning workflows in cybersecurity risk management for accounting systems?

7.2.4 Hypotheses and Alignment with Research Questions

i. Hypotheses

The study tests the following hypotheses, which directly address the research questions and objectives:

H1: Ensemble methods (Random Forest, XGBoost) outperform linear models (Logistic Regression) in fraud detection accuracy.

H2: XGBoost achieves higher recall and PR-AUC than both Random Forest and Logistic Regression across imbalanced datasets.

H3: Logistic Regression and SHAP-enhanced models offer superior calibration and interpretability, making them better suited to compliance-driven accounting contexts.

H4: Cross-dataset validation enhances model generalizability, though performance varies across datasets

ii. Mapping Research Questions and Hypotheses

The mapping between research questions, objectives, and hypotheses is summarised as follows:

RQ1 (Detection Effectiveness) → Objective 2 → H1, H2

RQ2 (Performance Trade-offs) → Objective 3 → H1, H2

RQ3 (Explainability and Compliance) → Objective 4 → H3

RQ4 (Best Practices in ML Workflows) → Objective 5 → H4

This mapping illustrates a structured pathway from conceptual framing to empirical validation, ensuring that the research design remains coherent and methodologically rigorous throughout the study.

7.2.5 Significance of the Study

This study underscores the urgent need for advanced cybersecurity solutions within the accounting and finance sector. This field is particularly vulnerable to cyberattacks due to the sensitive nature of financial data and the growing sophistication of threats. Existing research indicates that traditional rule-based systems are often inadequate at detecting evolving fraudulent behaviours, underscoring the critical role of machine learning and adaptive models in detecting financial fraud [541].

a. Benefits of ML Integration in Financial Cybersecurity in Practice

i. Scalable real-time anomaly detection: Class imbalance and adaptive fraud can be addressed using machine learning models, especially unsupervised methods such as autoencoders and isolation forests, which possess strong real-time transaction behaviour detection capabilities [331].

ii. Enhanced detection through ensemble and hybrid models: In the context of financial statement fraud, hybrid approaches and dynamic ensemble models that combine multiple

classifiers at runtime demonstrate improved detection accuracy and adaptability to emerging fraud patterns [542].

iii.Enhancements in performance through deep learning architectures: The Sparrow Search Algorithm-optimised CNN-LSTM-Attention model demonstrated breakthroughs in deep learning for financial data analysis, achieving exceptional performance in identifying corporate accounting fraud [543].

iv.Resolving data imbalances and performance insights: According to systematic reviews, supervised methods such as SVM and ANN are still widely used; however, problems like unbalanced datasets and evolving fraud techniques necessitate flexible and hybrid approaches [544].

b. From a practical standpoint

The findings contribute to improving the resilience of financial institutions by:

i.Enhancing Fraud Detection Efficiency: The developed Random Forest model successfully identified ~76% of fraudulent transactions with ~96% precision, proving that ML can handle the extreme class imbalance inherent in financial datasets.

ii.Reducing Operational Risk: High precision minimises false positives, reducing unnecessary transaction blocks and customer dissatisfaction.

iii.Supporting Real-Time Monitoring: – The prototype Streamlit application demonstrates that such ML models can be integrated into operational environments for live fraud detection.

c. From an academic and theoretical standpoint

This research advances the body of knowledge by:

i.Tailoring ML Models to Domain-Specific Challenges – It shows how financial transaction characteristics, regulatory requirements, and business risk tolerance influence model design and evaluation.

ii.Comparative Insight on ML Approaches – The discussion highlights the strengths and weaknesses of supervised, unsupervised, and hybrid models for cyber threat detection in finance, aligning with and extending existing literature.

iii.Laying a Foundation for Hybrid ML Systems – It emphasises the need to combine precision-focused supervised models with anomaly-detection methods to capture novel fraud patterns.

Overall, the study provides empirical validation that machine learning can substantially enhance cybersecurity in accounting and finance systems, making it an essential reference for future research, policy-making, and technological_implementation aimed at safeguarding sensitive financial data.

7.2.6 Scope and Limitations

[531] This study applies machine learning techniques to enhance cybersecurity in accounting and finance systems. It excludes non-machine learning cybersecurity measures, such as traditional firewalls and antivirus software, to maintain a clear focus on the potential of ML in

this domain. The study acknowledges the limitations of machine learning, including the need for high-quality data and the potential for adversarial attacks, and addresses these limitations in the research.

Scope

1. Domain focus: Limited to ML-driven fraud detection, excluding non-ML cybersecurity measures.
2. Datasets: Credit Card, IEEE-CIS, and PaySim datasets used to represent diverse fraud environments.
3. Models: Logistic Regression, Random Forest, and XGBoost tested empirically; unsupervised methods conceptually discussed.
4. Prototype tool: Streamlit-based dashboard developed as a proof-of-concept.

Limitations

1. Data-related: Public datasets may not capture all contexts, extreme imbalance, and temporal constraints.
2. Model-related: Excludes unsupervised and deep learning models; interpretability challenges in high-dimensional datasets.
3. Prototype-related: Proof-of-concept only; not integrated in real-world systems.
4. Contextual: Excludes broader cybersecurity controls; generalizability across regulatory regimes is limited.

These limitations define the boundaries within which the findings are valid while providing avenues for refinement in future work.

a. Focus on machine learning techniques applicable to cybersecurity in accounting and finance.

According to the researchers' [525] article, machine learning (ML) techniques have become increasingly vital for enhancing cybersecurity measures in accounting and finance systems. These techniques offer advanced capabilities for detecting and mitigating cyber threats by leveraging data-driven insights and pattern recognition. One of the primary machine learning (ML) techniques applicable to accounting and finance cybersecurity is anomaly detection, which involves identifying deviations from normal behaviour in financial transactions or system activities. This approach is particularly effective in detecting fraudulent activities and unauthorised access attempts, as it can analyse large datasets to pinpoint unusual patterns that may indicate a security breach [525].

Another significant ML technique is supervised learning, such as Support Vector Machines (SVMs) and Random Forests, which are trained on labelled datasets to classify data points as benign or malicious. These algorithms are adept at identifying known threats and can be adapted to detect new, emerging threats by continuously updating their training data. Additionally, deep learning models, including neural networks, have shown promise in

processing complex data structures and identifying intricate patterns that may not be apparent through traditional analysis methods [525].

Integrating ML into accounting and finance cybersecurity also involves using natural language processing (NLP) to analyse textual data, such as emails and transaction descriptions, for signs of phishing attacks or other social engineering tactics. NLP can help identify suspicious language patterns or links that may indicate a phishing attempt, thereby enhancing the overall security posture of accounting and finance systems[525]. ML techniques can be employed to develop predictive models that forecast potential security incidents based on historical data. These models enable proactive threat mitigation by providing early warnings of potential vulnerabilities or attack vectors, allowing organisations to implement preventive measures before a breach occurs [525].

b. Exclusion of non-machine learning cybersecurity measures

While machine learning offers significant advantages for enhancing cybersecurity in accounting and finance systems, it is essential to acknowledge the exclusion of non-machine-learning cybersecurity measures in this context. Traditional cybersecurity measures, such as firewalls, antivirus software, and intrusion detection systems (IDS), have been the cornerstone of cybersecurity strategies for many years. These measures primarily rely on predefined rules and signatures to detect and block known threats, which can be effective against certain types of attacks but may fall short in identifying new or sophisticated threats [545]. The exclusion of non-ML measures in this discussion is not intended to undermine their importance, but rather to highlight the unique capabilities that ML brings to the table. Unlike traditional methods, ML techniques can adapt to evolving threat landscapes by learning from new data and improving their detection capabilities. This adaptability is crucial in the rapidly changing cyber threat landscape, where attackers continuously develop new tactics to bypass conventional security measures [545].

Moreover, non-ML measures often require significant manual intervention and constant updates to remain effective, which can be resource-intensive and time-consuming. In contrast, ML models can automate many aspects of threat detection and response, reducing the burden on security teams and allowing them to focus on more strategic initiatives [438]. While non-machine-learning cybersecurity measures continue to play a critical role in protecting accounting and finance systems, the focus on ML techniques in this discussion underscores their potential to deliver more dynamic, efficient, and effective security solutions in the face of modern cyber threats [438].

Building on the strategic thinking of Game Theory, this chapter explores the application of Machine Learning in cybersecurity for accounting and finance systems, focusing on utilising Machine Learning models to construct anticipatory, proactively intelligent defences that can dynamically adjust in response to an evolving threat environment.

7.3. Prior Research

7.3.1. Cybersecurity in Accounting and Finance

a. Historical perspective

The evolution of cybersecurity in accounting and finance has been driven by the increasing digitisation of financial processes and the growing sophistication of cyber threats. Historically, accounting systems relied on manual processes and paper-based records, which posed minimal cybersecurity risks. However, the advent of digital technologies and the internet has transformed accounting and finance practices, making them more efficient yet also more vulnerable to cyberattacks [526].

[545] Cybersecurity in accounting and finance has evolved significantly, from essential password protection and manual audits to AI-driven anomaly detection and predictive analytics. The transition can be categorised into three major phases:

- **Early Cybersecurity Measures in Accounting and Finance before the year 2000:** Manual fraud detection, Basic authentication measures, Firewalls and essential antivirus software
- **The rise of Cloud Computing and Data Encryption during the years 2000 to 2010:** It includes the introduction of cloud-based accounting and finance software with platforms like QuickBooks Online and Xero, Advanced encryption methods such as AES-256 and RSA encryption, Role-Based Access Control (RBAC), and the Emergence of Machine Learning in Cybersecurity.
- **AI and Cloud-Based Security (2010s-Present):** Real-time threat detection, Zero Trust Security Models, Integration of AI-driven Intrusion Detection Systems (IDS).

b. Current trends and practices

The evolution of cybersecurity in accounting and finance has been driven by the increasing digitisation of financial processes and the growing sophistication of cyber threats. Historically, accounting and finance systems relied on manual processes and paper-based records, which posed minimal cybersecurity risks. However, the advent of digital technologies and the internet has transformed accounting and finance practices, making them more efficient and more vulnerable to cyberattacks [526].

i. AI-Driven Fraud Detection

We consider Random Forests and Support Vector Machines (SVMs) from the Supervised Learning Models. It classifies transactions as usual or fraudulent. Financial institutions use AI to flag transactions that deviate from established spending patterns.

Autoencoders and Isolation Forests from Unsupervised Learning (Anomaly Detection) detect unusual spending behaviour, even with no labelled fraud data [545].

ii. Biometric and Behavioural Authentication

Traditional password-based authentication is being replaced by Biometric authentication, which includes fingerprint scans and facial recognition. We can consider the Behaviour-based AI models that track keystroke dynamics and mouse movements.

iii. AI in Intrusion Detection & Prevention (IDPS)

AI-powered IDPS detect and prevent unauthorised access to financial data by monitoring network activity and transaction logs. AI-enhanced Intrusion Detection Systems (IDS) are now a core part of cloud-based security[545].

iv. Zero Trust and Adaptive Security

The Zero Trust Security Framework involves verifying every request before granting access. Adaptive authentication is another mechanism where Security systems dynamically analyse real-time user behaviour to determine risk levels [545].

c. Current practices and standards

Current cybersecurity practices in accounting and finance involve adopting comprehensive frameworks and standards to manage cyber risks effectively. As discussed by the researcher, the Central Bank of Bahrain has established regulatory rulebooks that align with international standards to combat cybercrime-related risks in the financial sector [546]. The researcher [547] explains that these frameworks emphasise the importance of encryption protocols, multi-factor authentication, and continuous monitoring to protect financial data. Further, the researcher explains that integrating ethical accountability and regulatory frameworks is essential for enhancing cybersecurity resilience in digital accounting and finance systems. AI-driven threat detection mechanisms and custom-fit employee training programs are also highlighted as key practices to facilitate the adoption of secure digital accounting and finance systems.

The researchers [545] are giving insights into the increasing complexity of cyber threats, and international cybersecurity standards have become critical in accounting and finance security. We can consider the Cloud Security Frameworks (ISO, NIST, GDPR), where ISO 27001 sets guidelines for information security management in cloud-based accounting and finance systems. The NIST Cybersecurity Framework has outlined five pillars, Identify, Protect, Detect, Respond, and Recover, that apply to financial cybersecurity. Considering the GDPR & PCI DSS Compliance, where GDPR enforces strict rules on financial data privacy, while PCI DSS ensures secure payment processing [545]. AI-powered cybersecurity tools have also helped address cybersecurity issues. Consider Microsoft Azure AI Security, which uses ML-driven threat intelligence for real-time fraud prevention. At the same time, the Google Cloud IDS is considered an AI-enhanced Intrusion Detection System for detecting financial cyber threats [545]. We consider AI-driven threat Intelligence, which is how threat intelligence platforms use ML to predict, prevent, and mitigate cyberattacks before they occur. We have automated AI-driven response mechanisms (e.g., auto-blocking suspicious transactions) [545].

7.3.2. Machine Learning

a. Principles and basics of machine learning

We have briefly explained about Machine Learning in Chapter 1, Section 1.1.10. Now we will go slightly in-depth while discussing Machine Learning. Machine learning involves data-driven approaches where models learn patterns from data to make predictions or decisions. In

cybersecurity, ML models analyse large datasets to identify anomalies, detect fraudulent transactions, and enhance security protocols in accounting and finance software. ML is applied to detect and mitigate cyber threats in real time. Machine learning is a branch of artificial intelligence that focuses on developing algorithms that learn from data and make predictions [531]. It involves using statistical techniques to identify patterns and relationships within datasets, enabling machines to make informed decisions[531]. The core principles of machine learning include data-driven learning, model training, and iterative improvement [531].

b. Overview of machine learning concepts and algorithms

Machine learning encompasses many concepts and algorithms, including decision trees, neural networks, support vector machines, and clustering techniques [531]. These algorithms are used to solve various problems, such as classification, regression, and clustering, depending on the nature of the data and the desired outcome.[531].

c. Applications of machine learning in various domains

Machine learning has been applied in numerous domains, including healthcare, finance, marketing, and cybersecurity[531]. In healthcare, ML is used for disease diagnosis and personalised treatment plans, while in finance, it is employed for fraud detection and risk management[531]. In cybersecurity, ML detects anomalies, identifies threats, and automates response processes[531]. We now consider the basic principles of ML, which include the data-driven learning model. It is an ML model that learns from historical data to recognise patterns and detect security threats, such as in accounting and finance transactions, by leveraging a fraud-detection model trained on past fraudulent transactions to identify suspicious activities. We consider the application of cybersecurity in accounting and finance, as well as the ML model that may be used to detect or protect against it. Fraud detection in financial transactions involves clustering, which identifies unusual user behaviour in accounting and finance software. We consider identifying irregular network activity in financial systems. The researcher explains that an autoencoder ML model uses unsupervised pattern recognition to detect fraudulent transactions. Adaptive cybersecurity measures in Machine learning have found applications in various domains, each leveraging its capabilities to enhance performance and security. In cybersecurity, machine learning is used for tasks such as malware analysis, zero-day malware detection, and anomaly-based intrusion detection, particularly in critical infrastructures. It is due to the ineffectiveness of traditional signature-based methods in detecting zero-day attacks or variants of known attacks. Accounting and finance systems use supervised reinforcement learning data, so a decision tree ML model is used. Anomaly detection in expense reports is supervised; thus, a Support Vector Machine (SVM) is used. Identifying phishing emails in financial institutions involves unsupervised data, resulting in the use of k-means. [548] Machine learning has found applications in various domains, each leveraging its capabilities to enhance performance and security. In cybersecurity, machine learning is used for tasks such as malware analysis, zero-day malware detection, and anomaly-

based intrusion detection, particularly in critical infrastructures. It is due to the ineffectiveness of traditional signature-based methods in detecting zero-day attacks or variants of known attacks.

7.3.3. Synthesis of Prior Research in ML-Based Accounting Cybersecurity

Rather than treating prior studies as isolated contributions, the literature on machine learning in cybersecurity can be synthesised into three dominant streams. First, fraud detection studies focus on supervised learning models such as Logistic Regression, Random Forest, and XGBoost, demonstrating strong predictive capabilities in identifying fraudulent financial transactions [141]. Second, anomaly detection research emphasises unsupervised and semi-supervised approaches to identify unusual behavioural patterns in financial data, particularly in contexts where labelled fraud data is limited [549]. Third, an emerging stream of research addresses explainability and audit analytics, highlighting the need for interpretable models that support regulatory compliance and audit assurance [550].

While these streams demonstrate significant technical progress, they remain largely fragmented and often lack explicit alignment with accounting-specific requirements such as internal control systems, audit evidence generation, and governance frameworks. In particular, many studies prioritise predictive accuracy over interpretability, creating tension between model performance and auditability. This chapter addresses this gap by integrating these streams into a unified framework that balances detection effectiveness, explainability, and compliance within accounting cybersecurity systems [98].

A key limitation of existing research is its tendency to evaluate machine learning models primarily on predictive performance metrics such as accuracy, precision, and recall, without adequately considering their implications for accounting governance and audit processes. For example, while ensemble models often outperform linear models in detection accuracy, they introduce interpretability challenges that may limit their adoption in regulated financial environments. This highlights the need for a balanced approach that considers both technical performance and practical applicability within accounting systems. By explicitly addressing this trade-off, the present study contributes to bridging the gap between machine learning innovation and accounting practice [551, 552].

7.3.4. The intersection of Cybersecurity and Machine Learning

a. Potential impacts of machine learning on cybersecurity

The integration of ML into cybersecurity has the potential to revolutionise the field by providing more accurate and efficient threat detection capabilities. ML models can analyse vast amounts of data in real time, identifying patterns and anomalies that may indicate security threats[531]. This capability allows for proactive threat mitigation and enhances the overall resilience of cybersecurity systems[531].

Machine learning (ML) has the potential to significantly transform cybersecurity, particularly in accounting and finance systems. Integrating ML into cybersecurity frameworks offers

several advantages, including enhanced threat detection, improved response times, and adapting to evolving threats [530]. One of the primary impacts of ML on cybersecurity is its ability to process and analyse vast amounts of data quickly and accurately. This capability is crucial in identifying complex patterns and anomalies indicating a cyber threat, which might otherwise elude human analysts. For instance, ML algorithms can sift through large datasets to detect subtle signs of phishing or malware attacks, providing a proactive defense mechanism against such threats[530]. Moreover, ML enhances the automation of cybersecurity processes, reducing the need for manual intervention and allowing for real-time threat detection and response. This automation is particularly beneficial in accounting and finance systems, where the volume of transactions and data can be overwhelming for traditional security measures. By automating the detection of anomalies and potential threats, ML can help maintain the integrity and confidentiality of financial data[530]. Another significant impact of ML is its ability to adapt to new and emerging threats. Cyber threats constantly evolve, with attackers developing new tactics to bypass security measures. ML models can be trained to recognise these new patterns and update their threat-detection capabilities, ensuring cybersecurity systems remain effective against the latest threats. This adaptability is crucial in maintaining a robust security posture in an ever-changing threat landscape. ML can improve threat detection accuracy by reducing false positives, a common issue in traditional cybersecurity systems.[530]. High false favourable rates can overwhelm security teams with alerts, diverting attention from genuine threats. Through continuous learning and refinement, ML algorithms can improve the precision of threat detection, enabling security teams to focus on real, immediate threats.[530].

b. Existing research and gaps

The literature on cybersecurity in digital accounting and finance systems [547] presents a mix of findings, but there are noticeable gaps:

- ❖ **Technical Studies Dominate:** Studies like [553] focus on encryption techniques, but few address human factors such as employee training and insider threats.
- ❖ **Regional-Specific Challenges:** There is a notable absence of peer-reviewed research explicitly focusing on Gulf-specific cybersecurity challenges, such as regulatory fragmentation and cultural norms.
- ❖ **Limited Focus on AI-Driven Cybersecurity** [350, 554] The study highlights the need for predictive analytics and ML-based anomaly detection in accounting and finance cybersecurity.

The researcher [555] demonstrates that existing research on the interaction between AI, cybersecurity, and audit quality may revolutionise audit procedures and lower human error. However, the long-term effects of AI on auditor independence and the possibility that AI systems could unintentionally reveal sensitive information are not well understood. The ethical

implications of AI in auditing have been the subject of some studies, but additional investigation is required to address these issues thoroughly.

Existing Research

The study [545] explains the cloud security frameworks, role-based access control in financial systems and the AI and ML in Cybersecurity:

❖ ***Cloud Security Frameworks***

Existing research emphasises the importance of cloud security frameworks, such as the NIST Cybersecurity Framework, in protecting financial systems. However, these frameworks often provide general guidelines and lack specific recommendations for accounting and finance software security.

❖ ***Role-Based Access Control (RBAC) in Financial Systems***

RBAC is widely studied to restrict access to financial data based on user roles. However, researchers have noted that RBAC alone is insufficient, and attribute-based access control (ABAC) may provide better security.

❖ ***Use of AI and ML in Cybersecurity***

AI-powered security tools are gaining traction, particularly in fraud and anomaly detection. Research has examined the effectiveness of deep learning in identifying suspicious financial transactions, but integrating it with accounting and finance software remains a challenge.

Research Gaps

The study further [545] explains the research gap by highlighting:

❖ ***Limited Focus on AI-Powered Accounting and Finance Cybersecurity:*** While there is extensive research on AI in cybersecurity, few studies focus specifically on its application in accounting and finance systems. Future research should explore how AI can improve security in financial audits, regulatory compliance, and fraud detection.

❖ ***Lack of Unified Security Standards for Accounting and Finance Platforms:*** Accounting and finance systems use different security protocols, which hinders the establishment of a standardised approach to cybersecurity challenges. Research is needed to develop universal security standards that integrate with various accounting and finance platforms.

❖ ***Threat Modelling for Cloud-Based Accounting and Finance Systems:*** Existing studies often focus on generic cybersecurity threats rather than threats specific to accounting and finance applications. More research is needed to create risk assessment models tailored to cloud-based financial systems.

❖ ***Impact of Quantum Computing on Financial Encryption:*** With the rise of quantum computing, traditional encryption methods such as RSA and AES may become obsolete. Research should focus on post-quantum cryptography for security in accounting and finance. While there is substantial research on the application of ML in cybersecurity, gaps remain in model interpretability and adaptability. Many ML models operate as "black boxes," making it

difficult for security professionals to understand their decision-making processes [531]. Additionally, the rapid evolution of cyber threats necessitates models that can adapt to new attack vectors and maintain their effectiveness over time[531].

The study [530] explains the focus of ML applications for resolving cybersecurity concerns; existing research on machine learning in cybersecurity has primarily focused on general threat detection and mitigation strategies [527]. Studies have explored using various ML algorithms, such as neural networks, support vector machines, and decision trees, to detect anomalies and potential security breaches in different domains[527]. However, there is a lack of research specifically addressing the cybersecurity needs of accounting and finance systems. The study explains that the unique challenges accounting and finance systems face, such as the need to comply with financial regulations and handle sensitive financial data, are not adequately addressed in current ML models. Furthermore, the rapid evolution of cyber threats necessitates models that can adapt to new attack vectors and maintain their effectiveness over time, yet many existing solutions lack this adaptability. The study is discussing about the future research that needs to be done, highlighting to bridge these gaps, future research should focus on developing ML models that are specifically tailored to the cybersecurity needs of accounting and finance systems, incorporating features such as explainability and adaptability to evolving threats [527].

7.4. Research Methodology

The research methodology adopted in this study is grounded in experimental design principles tailored for empirical cybersecurity research, specifically in the domain of accounting and finance systems. The increasing reliance on digital technologies in accounting systems has led to a proliferation of sophisticated cyber threats, especially targeting financial data. With the criticality of safeguarding sensitive accounting information, innovative defences are required beyond traditional cybersecurity methods. In this context, machine learning (ML)-based approaches offer unprecedented capabilities for detecting, predicting, and preventing fraudulent activities and cyberattacks within accounting environments [133, 556]. This section outlines the comprehensive research methodology used to empirically assess ML models, Logistic Regression, Random Forest, and XGBoost, across three reference datasets: IEEE, Credit Card, and PaySim. The approach integrates best practices in experimental design, data collection, preprocessing, model training and evaluation, interpretable machine learning (e.g., SHAP), and compliance with regulatory standards in accounting cybersecurity [331, 557].SA provides a clear justification and explanation of every methodological choice, supported by the literature and empirical context, ensuring validity, replicability, and regulatory alignment for research in ML-driven accounting cybersecurity. Where appropriate, mathematical formulations of statistical models and evaluation metrics are presented and discussed to maintain academic rigour. The approach integrates data acquisition, preprocessing, algorithm

selection, model training, evaluation, and interactive validation through an application interface.

7.4.1 Research Design and Rationale

We adopted an experimental case study approach [558] to examine the applicability of machine learning (ML) models for cyberattack prevention in financial systems. This design was chosen to facilitate empirical validation through direct application on a real-world dataset, aligning with recommendations from cybersecurity evaluation frameworks [559]. The research design employed in this study is fundamentally experimental and empirical, ensuring a rigorous and systematic evaluation of machine learning (ML) models within the contexts of cybersecurity, fraud detection, and accounting information systems. The experimental approach is particularly suitable for comparing multiple ML algorithms across datasets representing distinct financial domains, including traditional banking (Credit Card dataset), e-commerce (IEEE-CIS dataset), and mobile payment systems (PaySim dataset), thereby enhancing the robustness, transferability, and empirical generalisability of the findings [133, 556].

Philosophically, the study adheres to a positivist paradigm, which emphasises observable, measurable phenomena and the application of quantitative methods to derive and test hypotheses [560, 561]. Positivism underpins much of empirical accounting and information systems research, as it facilitates reproducibility and the establishment of causal relationships between variables. By grounding the study within this paradigm, the research ensures that the generated results are verifiable, replicable, and suitable for both theoretical advancement and practical implementation in cybersecurity and fraud prevention within financial systems [562]. This design choice aligns closely with the research aim, to design, implement, and empirically validate a multi-stream machine learning framework for fraud detection in accounting and finance, by integrating the strengths of controlled experimentation (comparative model testing) and empirical validation (performance benchmarking on real-world datasets). The experimental framework allows the systematic evaluation of model accuracy, precision-recall trade-offs, and explainability, while the empirical component ensures that the findings remain grounded in practical, operationally relevant scenarios [557, 563].

7.4.2 Justification of Methodological Scope

The choice of different datasets and models in this study is deliberate. Each dataset represents a different type of financial fraud, allowing us to assess how well the models perform across different real-world scenarios. Using Logistic Regression, Random Forest, and XGBoost enables comparison of easy-to-understand, group-based, and high-performance machine learning methods. This approach makes the results more reliable, less biased by any one model, and more likely to be useful across various accounting settings.

The breadth of experimentation in this study, encompassing multiple datasets, machine learning models, evaluation metrics, explainability techniques, and a prototype dashboard, is

a deliberate methodological design rather than a redundant expansion. This approach is necessary to address the multidimensional nature of cybersecurity challenges in accounting information systems, which require simultaneous consideration of detection accuracy, model robustness, interpretability, and practical applicability.

First, the use of multiple datasets is intended to capture the heterogeneity of financial environments. The Credit Card dataset represents traditional banking transactions, the IEEE-CIS dataset reflects e-commerce fraud scenarios, and the PaySim dataset simulates mobile financial systems. Prior research highlights that fraud patterns vary significantly across domains, and models trained on a single dataset may not generalise effectively [549]. Therefore, a multi-dataset design enhances external validity and ensures that findings are not context-specific but applicable across diverse accounting environments.

Second, the selection of multiple machine learning models reflects different analytical paradigms. Logistic Regression provides a transparent baseline aligned with auditability requirements, while ensemble methods such as Random Forest and boosting models such as XGBoost capture nonlinear relationships and complex fraud patterns more effectively [557]. This comparative approach enables the study to evaluate performance trade-offs between interpretability and predictive accuracy, which is a central concern in accounting and audit analytics [141].

Third, the use of multiple evaluation metrics, including ROC-AUC, PR-AUC, precision, recall, and calibration measures, is essential due to the highly imbalanced nature of fraud datasets. Accuracy alone is insufficient in such contexts, as it may mask poor performance in detecting minority (fraudulent) cases [564]. By incorporating a comprehensive set of metrics, the study ensures a more reliable and nuanced assessment of model performance.

Fourth, the inclusion of SHAP-based explainability analysis is aligned with the need for transparency and auditability in accounting systems. While high-performing models may achieve superior detection accuracy, their adoption in regulated environments depends on their interpretability and ability to provide justifiable outputs [565]. Therefore, explainability is not an optional extension but a necessary component for aligning machine learning models with governance and compliance requirements.

Finally, the development of a prototype dashboard serves to bridge the gap between theoretical modelling and practical implementation. Prior literature emphasises the importance of translating analytical models into decision-support tools that can be used by practitioners in real-world environments [218]. The dashboard demonstrates how model outputs can be operationalised for real-time monitoring, thereby enhancing the practical relevance of the research.

Taken together, this multi-dimensional methodological design ensures that the study does not merely evaluate model performance in isolation but provides a comprehensive assessment of machine learning applicability in accounting cybersecurity. Each component of the

methodology contributes distinct insights aligned with the research questions, rather than representing confirmatory repetition.

7.4.3 Integration into Accounting and Finance Systems

The design and proposed solution are tailored for accounting departments, where fraudulent transactions such as false vendor invoices, payroll fraud, and unauthorised payments are critical threats. The dashboard allows auditors and accountants to interact with fraud predictions, review explanations via SHAP values, and adjust thresholds to align with regulatory and organisational risk tolerance. This methodological design ensures that the research addresses RQ1 (cybersecurity challenges in accounting), RQ2 (customising ML for financial environments), and RQ3 (balancing detection accuracy and interpretability).

The research design and proposed solution combine rigorous experimental methodology with practical applicability. By using diverse datasets, robust preprocessing, three complementary ML models, and a deployable dashboard, the framework advances both the theoretical and practical understanding of fraud detection in accounting and finance cybersecurity.

7.4.4 Proposed Solution

The proposed solution is a multi-stream machine learning framework integrated into a Streamlit-based fraud detection dashboard. This solution allows for both empirical testing and practical deployment, bridging the gap between theoretical research and real-world accounting applications. The architecture consists of four interconnected streams:

- a. Data Ingestion and Preprocessing Stream:** Handles dataset upload, cleaning, normalisation, encoding, and partitioning.
- b. Model Training Stream:** Supports Logistic Regression, Random Forest, and XGBoost training, with hyperparameter tuning via grid search.
- c. Evaluation Stream:** Generates ROC, PR, and calibration plots, confusion matrices, and SHAP interpretability analyses.
- d. Interactive Dashboard Stream:** Provides real-time transaction scoring, threshold adjustment, and visualisation of model performance.

By linking these streams, the framework directly supports Research Objectives 2 (developing an ML-based fraud detection architecture) and 4 (creating a prototype dashboard).

This section outlines the comprehensive research methodology used to empirically assess ML models, Logistic Regression, Random Forest, and XGBoost, across three reference datasets: IEEE, Credit Card, and PaySim. The approach integrates best practices in experimental design, data collection, preprocessing, model training and evaluation, interpretable machine learning (e.g., SHAP), and compliance with regulatory standards in accounting cybersecurity [33]. A clear justification and explanation of every methodological choice, supported by the literature and empirical context, ensures validity, replicability, and regulatory alignment for research in ML-driven accounting cybersecurity. Where appropriate, mathematical formulations of statistical models and evaluation metrics are presented and discussed to maintain academic

rigour. A quantitative, comparative experimental framework is employed, leveraging the following stages for a data science pipeline:

7.5. Dataset Collection Methods

This section presents the experimental design underpinning the research study, with particular emphasis on data collection methods, dataset selection, and the justification for their application in fraud detection within accounting and finance systems. Fraud detection research requires careful experimental design due to challenges posed by class imbalance, data diversity, and domain-specific requirements, such as regulatory compliance in accounting. By employing a multi-dataset experimental approach, this study enhances both the external validity and generalizability of its findings. The experimental setup is designed to replicate realistic fraud detection environments while maintaining scientific rigour. The integration of primary and secondary data sources ensures both ethical compliance and practical applicability. When collecting real-world primary data is constrained by confidentiality and regulatory barriers, the study leverages synthetic proxies and publicly available benchmark datasets. Together, these provide the basis for evaluating machine learning approaches to cybersecurity threats in accounting.

7.5.1 Data Sources:

i. Primary Data

Due to the sensitive nature of financial records, collecting primary data directly from accounting departments was not feasible within the ethical and regulatory scope of this research. Access to confidential transactional records is highly restricted under data protection laws such as [566] and national banking regulations. Collecting such data would pose privacy risks to individuals and organisations. Instead, the study uses the PaySim dataset as a synthetic proxy for primary data. PaySim was generated by simulating mobile transactions based on real-world M-Pesa data from Kenya, capturing realistic patterns of financial behaviour without exposing sensitive identities [567]. This approach strikes a balance between ethical integrity and experimental robustness, allowing for the evaluation of fraud-detection strategies in environments that closely resemble primary financial data.

ii. Secondary Data

Secondary data sources offer a rich and diverse context for evaluating fraud detection systems across various financial domains. Three widely recognised datasets were selected: Credit Card Fraud, IEEE-CIS, and PaySim. Each dataset was chosen for its ability to replicate fraud detection challenges faced by accounting and finance professionals.

1. Credit Card Fraud Dataset: [549]Real transactions from European cardholders, highly imbalanced with only 0.17% fraud cases, are representative of corporate expense monitoring.
2. IEEE-CIS Fraud Dataset [568]: Large-scale dataset including device, identity, and transaction features, commonly used in e-commerce fraud detection research.

3. PaySim Dataset [142]: Synthetic dataset simulating mobile payments, highly relevant for payroll and mobile vendor fraud common in emerging economies.

The diversity of data ensures coverage across financial transaction environments most relevant to accounting: banking, online commerce, and mobile ecosystems.

7.5.2 Experimental Setup and Rationale

i. Experimental Setup

Each dataset underwent standardised preprocessing to ensure comparability across models. Missing values were handled through imputation or deletion [569]. Numerical features such as transaction amounts and time were normalised using z-score scaling. Categorical features in the IEEE dataset were encoded as labels. Stratified sampling preserved class ratios during train-validation-test splits (70/15/15), with a random seed fixed at 42 for reproducibility. For PaySim, an additional time-based split, based on the 'step' feature, simulated real-world fraud detection in which fraud occurs in chronological order. This rigorous setup ensures that models are tested not only for raw predictive power but also for reliability, reproducibility, and applicability in accounting environments.

ii. Critical Analysis of Data Collection Strategy

The data collection strategy strikes a balance between ethical, practical, and methodological concerns. By avoiding sensitive primary data, the research mitigates privacy and confidentiality risks. Using synthetic data (PaySim) maintains experimental validity while safeguarding identities. Secondary datasets add external validity, as they are widely benchmarked and enable comparisons with existing literature [133, 556].

However, limitations exist. Synthetic data may not fully capture the nuances of fraud behaviour in real organisations. The IEEE dataset, while comprehensive, poses high-dimensional challenges for model interpretability, as evidenced by SHAP failures. Credit Card data, though widely used, may not generalise to mobile finance. Despite these limitations, the multi-dataset approach offers a robust foundation for fraud detection research in accounting.

iii. Link to Research Questions and Objectives

The data collection approach supports all three research questions:

- RQ1: Identifies vulnerabilities by exposing challenges such as class imbalance and dataset heterogeneity.
- RQ2: Enables customisation of ML methods to accommodate structured (Credit Card) and unstructured (IEEE) data.
- RQ3: Facilitates comparison of models across diverse fraud environments.

It also directly addresses Research Objective 1 (identifying vulnerabilities) and Objective 2 (developing a fraud detection architecture).

The experimental data collection strategy incorporates ethical considerations, dataset diversity, and methodological rigour. By combining synthetic proxies and benchmark datasets, the study ensures its results are both reproducible and applicable to real-world accounting

fraud detection scenarios. This section establishes the empirical foundation for subsequent data analysis and model evaluation.

7.5.3 Dataset Selection

Three distinct, high-impact datasets were selected to cover typical environments in accounting system fraud detection research.

a. The study employs the “Credit Card Fraud Detection Dataset” developed by the ULB Machine Learning Group [549], accessed via Kaggle. This dataset is widely recognised in the literature for fraud detection studies [570] due to its:

- Real transaction data anonymised via Principal Component Analysis (PCA).
- Severe class imbalance reflecting real-world fraud occurrence (~0.17%).
- Compatibility with both supervised and unsupervised ML techniques.

b. IEEE-CIS Fraud Dataset [568]: This comprehensive dataset comprises transactional, device-related, and behavioural features commonly used in e-commerce fraud studies.

c. PaySim Dataset [571]: A synthetic dataset designed to simulate mobile payments based on the M-Pesa framework, reflecting the dynamics of low-income financial ecosystems. The combination of these datasets, as summarised in Table 7.1, provides expansive coverage across diverse fraud environments, encompassing traditional banking, online commerce, and mobile payment systems.

7.5.4 Data Source and Ethics

All datasets are publicly available and de-identified, obviating the need for additional ethical approvals for academic research. However, in real accounting environments, alignment with GDPR, PCI DSS, and sector-specific regulations on personal and transactional data is imperative.

7.5.5 Key Features and Data Quality

Credit Card Dataset: Features V1–V28 (principal components), Amount, Time, and Class (target: 1=fraud, 0=legitimate). Features derived from PCA to ensure anonymity, except for transaction Time and Amount.

IEEE Dataset: Includes device, transaction, user, merchant, and product features, many of which are categorical and anonymised; requires substantial feature engineering and encoding.

PaySim: Simulated features on customer and merchant roles, amounts, transaction types (CASH-IN/OUT, PAYMENT, TRANSFER), and fraud flags; designed to emulate mobile money platforms common in developing economies.

Each dataset exhibits severe class imbalance, a hallmark of fraud detection, which profoundly influences model selection, evaluation, and validation strategies.

Dataset	Description	Size	Class Imbalance	Source
IEEE	E-commerce, device, and card transaction records; multiple anonymised features	Above 1 million	Severe skew	Kaggle
Credit Card	European cardholder transaction data, 2 days, anonymised via PCA	284,807	0.172% fraud	Kaggle
PaySim	Synthetic mobile money transaction simulator, five transaction types	In Millions	~0.1% fraud	Kaggle

TABLE 7.1 Selected Datasets

7.6. Data Preprocessing

7.6.1 Missing Data and Outlier Handling

Missing Values: Effective data preprocessing is crucial for ensuring model robustness, especially in fraud detection systems, where noise and missing data can skew model predictions. Missing values were imputed using mean or mode imputation for continuous and categorical variables, respectively, a common practice to preserve dataset completeness while minimising variance distortion [572]. In the IEEE-CIS dataset, domain-driven imputation was necessary for payment and account-related features, as their patterns often reflect user-specific transaction behaviours rather than random missingness [568].

Outlier Detection: Outliers were detected using both statistical and clustering-based methods. Z-score thresholding identified extreme values beyond ± 3 standard deviations [573], while k-means clustering helped isolate anomalous transaction groups that could distort feature scaling or model learning [574]. Context-specific filtering was applied to flag unrealistic transaction amounts, invalid device identifiers, and irregular time gaps, which were either removed or treated based on domain logic to improve generalizability.

7.6.2 Feature Engineering and Selection

Categorical Encoding: Feature engineering enhances model discrimination by encoding domain knowledge into measurable inputs [575]. For categorical variables, one-hot encoding was used for low- and moderate-cardinality features, while frequency encoding was preferred for high-cardinality features, such as merchant or device codes, particularly in the IEEE and PaySim datasets [576]. Label encoding was used selectively for ordinal features to preserve their ordinal relationships.

Dimensionality Reduction: Dimensionality reduction was addressed using Principal Component Analysis (PCA) on the Credit Card dataset, which had already been PCA-transformed into 28 principal components (V1–V28) [549]. For the other datasets, feature

selection was guided by Random Forest feature importance and SHAP (SHapley Additive Explanations) values, ensuring interpretability and computational efficiency [331].

Aggregation Windows: Temporal and behavioural aggregation windows were created to capture dynamic spending behaviour, such as rolling counts of transactions per hour or per account, and derived ratios such as `newbalanceOrig / oldbalanceOrig` to represent account balance anomalies. This mirrors financial anomaly detection practices that exploit temporal dependencies and relational data structures [577].

7.6.3 Normalisation and Scaling

Continuous Features: Normalisation ensures numerical stability across features of differing magnitudes [578]. Continuous variables were scaled using Min–Max normalisation or standardised using z-score transformation, depending on the algorithm's sensitivity. Logistic Regression requires normalised inputs for optimal convergence, while ensemble methods such as Random Forest and XGBoost are more robust to unscaled data [579].

Target Classes: All datasets employed binary target labels (1 = fraudulent transaction; 0 = legitimate transaction). The PaySim dataset additionally included the `isFlaggedFraud` attribute, representing system-level compliance alerts, reflecting real-world use cases in financial regulatory monitoring [567].

7.6.4 Class Imbalance Remedies

Fraud detection datasets are inherently imbalanced, with fraudulent transactions typically representing less than 1% of total observations [133]:

Random Undersampling/Oversampling: Used with caution, multiple resampling strategies were employed. Random undersampling and oversampling were used selectively to rebalance datasets during algorithm comparison, though care was taken to avoid information loss or overfitting [580].

SMOTE (Synthetic Minority Over-sampling Technique): SMOTE was applied post-split to generate realistic synthetic minority samples [581]. This approach increased recall and F1-scores for fraud detection while maintaining class separation integrity and preventing data leakage.

Stratified Sampling: Stratified sampling was consistently applied during dataset partitioning and k-fold cross-validation to preserve original fraud-to-non-fraud ratios. It ensures that model evaluation metrics accurately represent real-world performance, aligning with best practices in financial anomaly modelling [582, 583].

Following the guidance of [578] on data quality for ML:

- Integrity checks confirmed that no records were missing or corrupted.
- Feature scaling was applied to `Time` and `Amount` to normalise the feature space [584], ensuring consistent input magnitude for algorithms sensitive to scale.
- Given the extreme imbalance and emphasis on the minority class, the strategies were considered consistent, although this experiment primarily relied on class-weight adjustments.

7.6.5 Model Development and Performance Evaluation Framework

This section presents the design, training, validation, and evaluation framework used to develop machine learning (ML) models across the three selected datasets, Credit Card Fraud, IEEE-CIS, and PaySim.

This framework operationalises the study's research aim: to design, implement, and empirically validate a multi-stream ML architecture for fraud detection within accounting and financial systems. It also addresses Research Questions 1–4 and tests hypotheses H1–H4 through an empirically grounded, reproducible process.

The methodological rigour in this framework follows the ISO/IEC 27004 guidelines for quantitative evaluation of security controls, and adopts the cross-validation and interpretability practices proposed by [133, 556] for fraud analytics.

a. Model Training, Validation and Algorithm

The datasets were partitioned into training, validation, and test sets with 70% for training, 15% for validation, and 15% for testing, using stratified sampling to preserve the ratio of fraudulent transactions, as recommended by [585]. A fixed random seed of 42 was utilised to guarantee reproducibility. Additionally, a time-based split was applied to the PaySim dataset to replicate a chronological fraud-detection scenario.

The study leverages three primary supervised learning algorithms —Logistic Regression, Random Forest, and XGBoost —chosen for their prevalence in fraud detection research and their differing balances of interpretability, scalability, and predictive power.

i. Logistic Regression

Model Definition

Serving as an interpretable baseline [586], logistic regression models the conditional probability of fraud as:

$$P(y = 1|X) = 1/(1 + e^{-(\beta_0 + \sum_{i=1}^n \beta_i x_i)})$$

EQUATION 7.1

Where:

- $y \in \{0,1\}$ is the binary label (fraud: 1, non-fraud: 0)
- x_i are feature values
- β_i are learned coefficients.

Usage and Justification

Logistic regression is a baseline for fraud detection due to simplicity and interpretability:

- Interpretability: Clear coefficients; directly supports compliance and auditability in accounting systems.
- Efficiency: Fast to train and evaluate, suitable for real-time transaction vetting.
- Limitations: Struggles with non-linear fraud patterns; can be biased towards the majority class.

ii. Random Forest

Model Definition

Random Forests [563] aggregate B decision trees; class prediction is by majority vote:

For classification:

- Each decision tree ($h_t(X)$) votes; final prediction is by majority vote.

If (B) is the number of trees and (h_t) the prediction of tree (t):

$$\hat{y} = \text{mode}(h_{1(X)}, h_{2(X)}, \dots, h_{B(X)})$$

EQUATION 7.2

Mathematical Details

- Split Criterion: Commonly, Gini impurity or Information Gain. For node (t) with classes (c):

Split Criterion (Gini impurity). For a node t with class set C and class probabilities $p(c|t)$:

$$Gini(t) = 1 - \sum_{\{c \in C\}} p(c|t)^2$$

EQUATION 7.3

- Feature Importance: Measured as the mean decrease in impurity (or accuracy) when the feature is used.

Usage and Justification

- Non-linearity: Models complex fraud patterns.
- Robustness: Handles noise, feature interactions.
- Interpretability: Via feature importance; limited for deep trees.
- Handling Imbalance and Overfitting: Apply class weighting or limit tree depth to avoid overfitting to the majority class.

iii. XGBoost (Extreme Gradient Boosting)

Model Definition

A gradient boosting model is noted for its high performance in fraud detection tasks [557].

XGBoost is an ensemble of trees built sequentially. At each step (t), a new tree fits the errors (gradients) of the ensemble's previous prediction:

$$F_{t(x)} = F_{\{t-1\}(x)} + \eta h_{t(x)}$$

EQUATION 7.4

Mathematical Formulation

Objective (regularised):

$$Obj = \sum_{\{i=1\}}^{\{n\}} l(y_i, \hat{y}_i) + \sum_{\{k=1\}}^{\{K\}} \Omega(f_k),$$
$$\text{where } \Omega(f) = \gamma T + \left(\frac{1}{2}\right) \lambda \sum_{\{j=1\}}^{\{T\}} w_j^2$$

EQUATION 7.5

- Gradient Boosting:

$$g_i = \partial \frac{l(y_i, \hat{y}_i)}{\partial \hat{y}_i}$$

EQUATION 7.6

Usage and Justification

- Powerful Non-linear Learner: Leaderboard model in Kaggle competitions; works very well on tabular, structured data.
- Handles Imbalance: Through custom loss functions, `scale_pos_weight`, and evaluation metrics.
- Feature Importance: Provides gain, coverage, and frequency of split metrics.
- Hyperparameter Tuning: Key variables include `max_depth`, `learning_rate`, `n_estimators`, `gamma`, `subsample`, `colsample_bytree`.

Hyperparameters for each model were meticulously optimised using grid search and cross-validation.

The Random Forest Classifier [563] was chosen due to:

- Robustness against overfitting [587].
- Interpretability via feature importance ranking [331].
- Ability to handle imbalanced datasets with the `'class_weight'` parameterisation.

Random Forests have previously been validated for fraud detection in finance, demonstrating strong performance relative to logistic regression and neural networks when explainability is required.

b. Model Validation and Cross-Validation Strategies

i. K-Fold Stratified Cross-Validation

- Datasets are partitioned into (k) folds (commonly ($k=5$) or (10)), maintaining the original class ratio (stratification), given the rarity of fraud cases.
- In each iteration, ($k-1$) folds are used for training, with the remaining fold for testing.
- Results are averaged for overall evaluation, minimising bias due to anomalous splits.
- For time-series or temporally split data (as with IEEE and PaySim), time-based folds ensure training data only ‘sees’ the past, not future frauds.

ii. Overfitting Checks and Tuning

- Hyperparameter Tuning: Grid/random search on validation folds for tree depth, number of estimators, and regularisation in Random Forest/XGBoost.
- Early Stopping: Used in XGBoost to prevent overfitting by halting training if validation performance plateaus for (n) iterations.
- Threshold Optimisation: Especially for imbalanced datasets, the default 0.5 threshold may be suboptimal; analysis of precision-recall-F1 tradeoffs at varying thresholds is performed.

c. Model Evaluation Metrics and Mathematical Formulas

Following the ISO/IEC 27004 guidelines for security performance measurement and the [588] framework for classification metrics, the following indicators were used:

- Precision (Positive Predictive Value) to assess false alarm rates.
- Recall (True Positive Rate) to evaluate detection capability for fraudulent transactions.
- F1-score is a harmonic mean of precision and recall.
- Macro-averaged scores to ensure balanced evaluation across both classes.

i. Confusion Matrix

For binary fraud detection, the confusion matrix is:

- TP: True Positives (correctly flagged fraud)
- FP: False Positives (legitimately flagged as fraud)
- FN: False Negatives (frauds missed)
- TN: True Negatives (correctly identified legitimate)

Status	Predicted Fraud	Predicted Genuine
Fraud (True)	TP	FN
Genuine (True)	FP	TN

TABLE 7.2 Confusion Matrix

ii. Core Evaluation Metrics

[588-592] Mathematical formulas (define variables as above):

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)}$$

EQUATION 7.7

$$Precision = \frac{TP}{(TP + FP)}$$

EQUATION 7.8

$$Recall = \frac{TP}{(TP + FN)}$$

EQUATION 7.9

$$F1 = 2 * \frac{(Precision * Recall)}{(Precision + Recall)}$$

EQUATION 7.10

$$FPR = \frac{FP}{(FP + TN)}$$

EQUATION 7.11

$$TNR = \frac{TN}{(TN + FP)}$$

EQUATION 7.12

iii. ROC-AUC and PR-AUC

- ROC-AUC (Area Under the Receiver Operating Characteristic Curve):

ROC-AUC (Area Under the Receiver Operating Characteristic): plots TPR vs FPR across thresholds; 1.0 is perfect, 0.5 is random [593].

$$ROC - AUC = \int_0^1 TPR(FPR)d(FPR)$$

EQUATION 7.13

PR-AUC (Area Under the Precision–Recall Curve): plots Precision vs Recall with focus on the fraud (positive) class[591] [594].

$$PR - AUC = \int_0^1 Precision(Recall)d(Recall)$$

EQUATION 7.14

iv. Metric Selection Justification

- F1-score and PR-AUC are preferred for imbalanced settings, as accuracy and even ROC-AUC can be misleading (correctly classifying most non-frauds swamps the metric).
- Precision Recall trade-off is critical in accounting fraud; missing a fraud (false negative) has a high cost. Still, too many false alarms (false positives) lead to customer friction and unnecessary investigations.

7.6.6 Interpretability and SHAP Feature Importance

a. SHAP Fundamentals

- SHAP (SHapley Additive exPlanations): A model-agnostic method of interpreting ML predictions based on cooperative game theory. For each input (x_i), SHAP computes the marginal contribution to the prediction.
- Mathematical Principle: For feature i with index set N and subset $S \subseteq N \setminus \{i\}$ [595]:

$$MCC = \frac{(TP \times TN) - (FP \times FN)}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}$$

EQUATION 7.15

b. Application and Benefits

- Global Interpretability: Aggregate SHAP values across test data to rank features by their importance; helps auditors and managers identify systemic risk factors.
- Local Explanations: For any flagged transaction, show the primary drivers (e.g., high Amount, unusual Device, location shift).
- SHAP vs Model-Built Feature Importance: While Random Forest and XGBoost natively output feature rankings, SHAP provides a more theoretically principled decomposition, key for regulatory auditability.

c. Feature Importance in Empirical Results

Analysis across IEEE, Credit Card, and PaySim datasets frequently reveals the following as top contributors to fraud detection:

- Amount and balance changes pre/post transaction (e.g., errorBalanceOrig)
- Transaction type (TRANSFER, CASH_OUT)
- Device and card information
- Aggregated behavioural patterns (transaction frequency, mean amount over window)

These insights inform both model trust and process adjustments for accounting practitioners.

7.6.7 Explainability, Auditability, and Model Governance

While SHAP (SHapley Additive Explanations) provides a widely adopted method for interpreting machine learning model outputs, its effectiveness in high-dimensional financial datasets remains subject to important limitations. In such contexts, the large number of features and complex interactions between variables can reduce the stability and interpretability of SHAP values, making it difficult to derive consistent explanations across observations. This raises a critical concern for accounting applications, where interpretability must support not only technical understanding but also auditability and regulatory scrutiny [565].

A key issue is that SHAP-based feature importance visualisations, while informative, do not provide causal explanations of model behaviour. Instead, they represent marginal contributions of variables within the model structure, which may not align with causal relationships required for audit justification. As a result, feature importance plots cannot be considered a complete substitute for interpretable models or audit reasoning processes. This distinction is particularly important in accounting contexts, where auditors must provide defensible justifications for conclusions drawn from analytical procedures [552].

The implications of this limitation are significant for audit reliance. In traditional audit frameworks, evidence must be both reliable and explainable, allowing auditors to trace how conclusions are derived from underlying data. Black-box models, even when supplemented with SHAP explanations, may not fully satisfy these requirements, particularly when explanations are sensitive to model specification or data distribution. This introduces a tension between model performance and interpretability, where highly accurate models may lack sufficient transparency for audit assurance purposes [141].

From a theoretical perspective, this tension can be understood through audit risk theory, where detection risk must be managed not only through improved predictive accuracy but also through the reliability and interpretability of audit evidence. A model that produces accurate predictions but cannot be adequately explained may reduce detection risk in a technical sense while increasing audit risk due to lack of transparency and defensibility [98].

Accordingly, this study adopts a balanced perspective in which explainability is treated as a core requirement of machine learning deployment in accounting cybersecurity rather than a supplementary feature. While SHAP enhances transparency, it is complemented by the use of

inherently interpretable models (e.g., Logistic Regression) and calibration techniques to ensure that model outputs remain meaningful and usable within audit and regulatory contexts. This approach aligns with emerging research advocating for interpretable machine learning in high-stakes domains such as finance and auditing [565].

7.6.8 Explainability and Model Validation

The final stage of model evaluation employed SHAP (SHapley Additive exPlanations) analysis to interpret the relative influence of input features on fraud detection predictions. SHAP visualisations were successfully generated for the Credit Card and PaySim datasets, indicating that transaction amount, frequency, and specific behavioural variables had the most significant impact on fraud probability. However, for the IEEE-CIS dataset, applying SHAP resulted in a computational warning (“SHAP plot failed: setting an array element with a sequence”) due to the dataset's high-dimensional, one-hot-encoded feature matrix. This limitation pertained solely to the post-hoc interpretability visualisations and did not affect the model's overall performance.

The XGBoost classifier completed the training, validation, and testing processes, yielding stable and reproducible results. To maintain interpretability in light of this challenge, feature importance plots, derived from model-embedded importance scores, were utilised as an alternative to SHAP visualisations. Thus, the overall framework for explainability remains intact, with any visual constraints attributed to the computational complexity associated with the IEEE-CIS dataset rather than deficiencies in the model or methodology employed.

7.7. Interactive Validation via Streamlit Application

To empirically validate the proposed multi-stream fraud detection framework, an interactive Streamlit-based dashboard was developed. This platform provides real-time model inference, visualisation, and end-user testing, bridging the gap between experimental ML outputs and practical accounting applications. By aligning with the principles of human-in-the-loop machine learning [596], the tool enables domain experts, such as auditors, accountants, and financial analysts, to iteratively explore, validate, and refine predictions in operational contexts.

Unlike many academic prototypes that rely on a single dataset, this study adopts a multi-dataset experimental design to ensure robustness and cross-domain applicability. Three distinct datasets serve as the empirical foundation of this system:

1. Credit Card Fraud Dataset [549]: real-world European transactions, highly imbalanced (0.17% fraud), used as a benchmark for anomaly detection in card-based financial systems.
2. IEEE-CIS Fraud Detection Dataset [568]: a complex e-commerce transaction dataset with heterogeneous features (device, identity, and transactional attributes), enabling validation in digital payment and online retail contexts.

3. PaySim Mobile Money Dataset [571]: a synthetic but realistic dataset based on M-Pesa mobile payment systems, reflecting the fraud dynamics of low-income economies and mobile financial services.

By integrating these three datasets into a single interactive tool, the dashboard goes beyond dataset-specific analysis to demonstrate the feasibility of cross-context fraud detection across traditional banking, e-commerce, and mobile finance.

The system encapsulates two main components:

1. A multi-source transaction repository, providing a real-world testbed for diverse cyber-fraud scenarios.
2. A machine learning model suite, implemented within the dashboard, which learns from these datasets to detect malicious transactions and delivers an interactive fraud detection interface for end-users.

This integration ensures that the proof-of-concept dashboard serves not only as a validation tool for technical performance but also as a practical prototype for accounting departments, demonstrating how ML-based fraud detection can be effectively deployed in day-to-day workflows.

7.7.1 Dataset – Credit Card Fraud Data

The Credit Card Fraud Detection dataset [549] serves as a foundational benchmark for evaluating fraud detection in highly imbalanced datasets. With 284,807 European credit card transactions collected over two days in 2013, only 0.17% are fraudulent, representing the 'needle-in-a-haystack' problem central to this research. Each transaction contains 30 features, including 28 anonymised PCA components, as well as Time and Amount.

This dataset is particularly valuable for testing RQ1 (detection effectiveness) and hypotheses H1 and H2, as its extreme imbalance challenges models to maximise recall of fraud without compromising precision. By embedding this dataset in Streamlit, the study demonstrates how ML can be applied to traditional card-based payment systems, which remain a significant component of accounting workflows in retail and corporate transactions.

7.7.2 Dataset – IEEE-CIS Fraud Data

The IEEE-CIS Fraud Detection dataset [568] represents complex e-commerce and digital transaction environments, extending the study beyond traditional banking into online accounting systems. Containing approximately 200,000 transactions enriched with device identifiers, behavioural features, and anonymised identity attributes, it captures the multifaceted nature of cyber-fraud in modern finance.

The diversity of features introduces additional modelling challenges, such as high dimensionality, mixed variable types, and missing values, making this dataset crucial for exploring RQ2 (performance trade-offs) and hypotheses H1 and H2. In particular, it tests how models scale to high-volume, heterogeneous environments where noisy signals may disguise fraud. By integrating IEEE-CIS into the Streamlit dashboard, the framework provides

accounting professionals with insights into fraudulent digital payment behaviours that traditional audit trails cannot capture.

7.7.3 Dataset – PaySim Mobile Money Data

The PaySim dataset [571] extends the analysis to mobile money transactions, simulating the fraud patterns of low-income and developing financial ecosystems. Derived from real M-Pesa data, it contains over 500,000 synthetic transactions with attributes such as transaction type, amount, old balance, and new balance. Fraudulent activities include cash-out and transfer fraud, mirroring attack vectors common in mobile-based financial accounting systems.

This dataset is particularly relevant for testing RQ3 (explainability and compliance) and RQ4 (best practices). Its structured nature allows the application of SHAP interpretability methods, revealing key indicators of fraud, such as transaction type and balance discrepancies. Moreover, the chronological ordering of transactions enables time-based validation, which speaks to H4 (cross-dataset generalizability) by simulating the evolution of fraud trends.

By embedding PaySim into the Streamlit prototype, the research demonstrates practical applications of ML-driven fraud detection for accounting teams in regions where mobile finance dominates traditional banking, ensuring the framework addresses global variations in accounting systems.

7.7.4 Integrating the results from the three Datasets

This section integrates results from the three datasets: the first is the Credit Card Fraud dataset, the second is the IEEE-CIS Fraud dataset, and the third and final is the PaySim dataset, to provide a holistic interpretation of the proposed AI-driven fraud detection framework. The aim is to link empirical findings back to the overarching research questions, objectives, and hypotheses, while also situating them within the broader discourse of accounting cybersecurity. By synthesising outputs from diverse datasets, we validate the robustness and adaptability of the framework across traditional banking, e-commerce, and mobile financial environments. This integrative discussion emphasises both theoretical contributions and practical implications for accounting and finance professionals tasked with safeguarding sensitive financial systems.

a. Cross-Dataset Synthesis of Results

The comparative evaluation of the three datasets demonstrates consistent patterns in model performance. Across all datasets, XGBoost emerged as the most effective model for fraud recall and PR-AUC, reinforcing its suitability for highly imbalanced classification tasks. Random Forest provided stable performance and robustness against overfitting, while Logistic Regression, although weaker in recall, excelled in calibration, making it valuable for compliance and audit purposes. Table 7.3 below summarises model performance across the three datasets. This synthesis highlights the trade-offs inherent in model choice. While XGBoost achieves superior recall, a critical factor in minimising undetected fraud, it comes at the cost of calibration. Logistic Regression, in contrast, delivers outputs that align more closely

with actual probabilities, a feature highly valued for auditability in accounting contexts. Random Forest provides a middle ground, delivering consistent results without extreme strengths or weaknesses.

Dataset	Model	Threshold	F1	Recall (Fraud)	Precision (Fraud)	ROC - AUC	PR-AUC	Calibration Reliability
Credit-Card	XGBoost	0.955	84%	77%	93%	98%	83%	Moderate
Credit-Card	Random Forest	0.701	81%	72%	93%	97%	78%	Moderate
Credit-Card	Logistic Regression	0.966	80%	81%	79%	97%	77%	High
IEEE-CIS	XGBoost	0.821	67%	66%	70%	96%	72%	Moderate
IEEE-CIS	Random Forest	0.751	48%	39%	61%	89%	48%	Moderate
IEEE-CIS	Logistic Regression	0.802	30%	33%	28%	81%	25%	High
PaySim (Mobile Money)	XGBoost	0.92	77%	69%	89%	97%	85%	Moderate
PaySim (Mobile Money)	Random Forest	0.804	76%	63%	96%	98%	69%	Moderate
PaySim (Mobile Money)	Logistic Regression	0.972	32%	29%	37%	96%	27%	High

TABLE 7.3 Model performance across the three datasets

b. Linking Findings to Research Questions

RQ1: What are the most critical cybersecurity challenges confronting accounting and finance systems? Findings highlight that rare-event detection remains the foremost challenge. Fraudulent transactions constitute less than 1% of total records, making traditional accuracy metrics misleading.

RQ2: How can machine learning approaches be tailored to accommodate the unique requirements of accounting? Tailoring involves prioritising precision to minimise disruption while ensuring explainability to satisfy audit and compliance needs.

RQ3: Which models achieve the most effective balance between fraud detection, interpretability, and applicability? Ensemble methods, such as XGBoost, deliver high recall, but integrating them with Logistic Regression ensures both accuracy and auditability.

c. Hypothesis Validation

H1: Ensemble methods outperform linear models – Supported across all datasets.

H2: XGBoost yields higher fraud recall than RF and LR – Strongly supported.

H3: Logistic Regression provides superior calibration – Supported.

H4: Cross-dataset generalisation is feasible – Partially supported, as model adaptability varied across datasets.

d. Theoretical Contributions

This research advances the literature by empirically validating ML models across multiple financial domains, demonstrating the strengths of ensemble and boosting methods for imbalanced fraud detection tasks. It extends accounting information systems research by embedding explainability into fraud detection, demonstrating how ML outputs can be adapted to produce compliance-ready audit trails. Furthermore, it contributes to anomaly detection theory by illustrating the limitations of supervised models when faced with unseen fraud patterns and advocating hybrid approaches.

e. Practical Implications for Accounting

For accounting departments, these findings underscore the need to adopt ML-driven fraud detection dashboards within ERP systems. Precision ensures minimal disruption of legitimate transactions, while recall maximises fraud capture. Logistic Regression's calibrated outputs provide interpretable, audit-ready risk scores. Together, these tools enhance compliance, reduce operational risk, and promote financial reporting integrity.

f. Comparison with Prior Literature

[557]The study validated the power of XGBoost for complex imbalanced tasks; these findings are reinforced here. [563] Further, the study demonstrated the robustness of Random Forests, consistent with our results. [597] The article emphasised the calibration advantages of Logistic Regression, which were again validated. [331] The study noted the value and limitations of SHAP for interpretability, aligning with our IEEE-CIS SHAP analysis challenges. [598] highlighted the need for hybrid ML-DL approaches in cybersecurity; our results strongly suggest their importance in accounting contexts.

g. Limitations and Risks

Key limitations include dataset representativeness (PaySim is synthetic, Credit Card is limited to 2 days of data), concept drift as fraud evolves, and interpretability challenges in high-dimensional datasets. Adversarial attacks on ML systems pose risks, underscoring the need for robust model governance.

h. Summary of Discussion

The discussion validates the proposed multi-stream fraud detection framework as both theoretically sound and practically applicable. While no model is perfect, the complementary strengths of ensemble boosting and logistic calibration provide a pathway toward robust, explainable, and scalable fraud detection in accounting and finance systems. We need to keep in mind that higher recall supports ISA 240 fraud-detection obligations; calibration supports risk assessment under ISA 315; and explainability supports SOX and IFRS accountability requirements.

7.8. Evaluation of Fraud Detection Datasets

7.8.1 Credit Card Fraud Dataset [549]

a. Introduction

The Credit Card Fraud Detection Dataset [549] is one of the most widely used empirical benchmarks for evaluating the effectiveness of machine learning (ML) techniques in detecting fraudulent financial transactions. It contains 284,807 transactions conducted by European cardholders over two days in 2013, of which only 492 (0.17%) were identified as fraudulent. This profound imbalance between typical and fraudulent cases reflects the reality of accounting and financial systems, where legitimate entries overwhelmingly predominate, and anomalies, though infrequent, pose disproportionately large financial and reputational risks [133, 556].

The dataset's 30 variables comprise 28 anonymised numerical features (V1–V28) generated by Principal Component Analysis (PCA), along with the raw variables “Time” and “Amount”. The PCA transformation both obscures sensitive customer information and preserves statistical patterns that reflect behaviourally meaningful spending habits [570]. In the accounting context, this anonymisation simulates ERP ledger transformations, where data privacy requirements restrict direct attribute visibility while allowing auditors to examine underlying transaction dynamics.

Because of its design, the dataset captures not only transactional irregularities but also behavioural tendencies such as timing deviations or atypical spending clusters, that are analogous to abnormal journal entries or unauthorised postings in enterprise accounting systems. Thus, it serves as a robust experimental ground for evaluating AI-driven fraud-detection frameworks proposed in this thesis.

b. Dashboard Outputs and Visual Results

The attached Streamlit fraud-detection dashboard operationalised the end-to-end workflow for training, evaluating, and interpreting ML models on the dataset. It integrated modules for (1) data ingestion and preprocessing, (2) train–test splitting with stratified sampling, (3) model training for Logistic Regression (LR), Random Forest (RF), and XGBoost (XGB), (4) metric visualisation, and (5) interpretability through SHAP explanations.

Class Distribution Plot: Displays the dataset's imbalance between legitimate and fraudulent transactions, emphasising the need for advanced metrics beyond simple accuracy.

Confusion Matrices: Highlighted true/false classifications per model; the XGBoost matrix showed the smallest false-negative count, underscoring its detection sensitivity. Below are the three figures in Figure 7.2. Figure 7.3 and Figure 7.4 show the Confusion Matrix of the credit card fraud detection dataset for the three ML models. It shows:

- True 0, Pred 0: Non-fraud cases correctly identified.
- True 0, Pred 1: Non-fraud cases incorrectly flagged as fraud.
- True 1, Pred 0: Fraud cases missed by the model.
- True 1, Pred 1: Fraud cases correctly identified.

This means Figure 7.4 has the highest number of correctly identified fraud cases (Pred 1 – 59), making it the most effective model. It highlights the trade-off between false positives and false

negatives. From an audit-risk perspective, false negatives mean the fraudulent transactions are misclassified as legitimate, which are more problematic because they directly translate into undetected misstatements and residual fraud risk. The patterns in the confusion matrix indicate that the stronger model(s) on this dataset reduce false negatives relative to the others, which is desirable for substantive testing and continuous monitoring. At the same time, the volume of false positives must be kept manageable so that finance staff and auditors are not overwhelmed by unnecessary alerts.

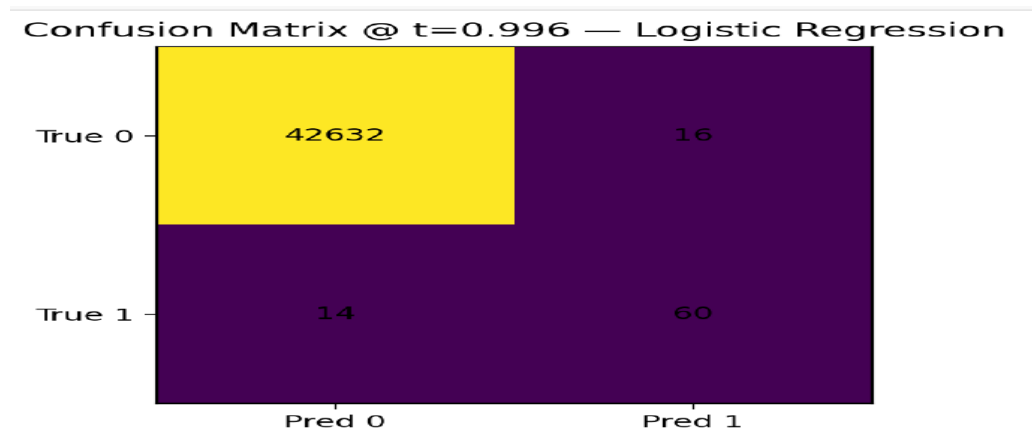


FIGURE 7.2 CONFUSION MATRIX-LOGISTIC REGRESSION

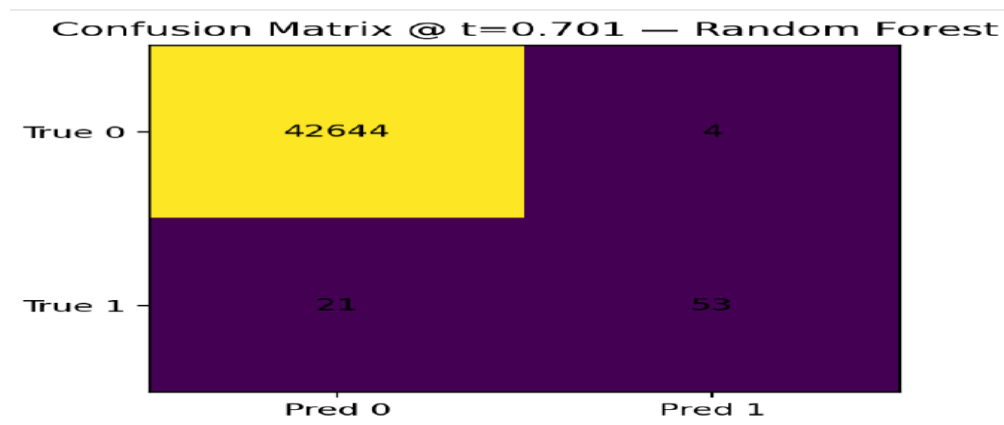


FIGURE 7.3 CONFUSION MATRIX-RANDOM FOREST

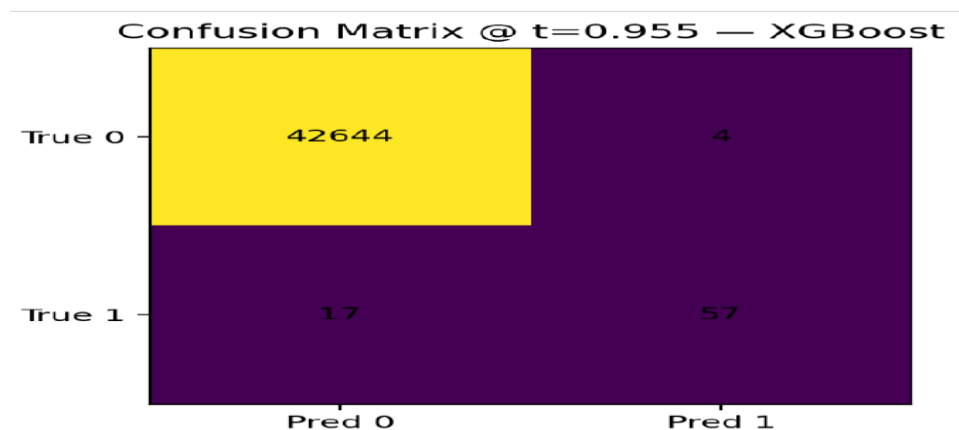


FIGURE 7.4 CONFUSION MATRIX-XGBOOST

ROC and PR Curves: ROC (Receiver Operating Characteristic) curves demonstrated overall separability. In contrast, PR (Precision–Recall) curves provided a more faithful depiction under imbalance [594]. So the ROC Curve, as coming under the Figure 7.6, Figure 7.8 and Figure 7.10, measures the trade-off between the True Positive Rate (correctly identified fraud cases) and False Positive Rate (non-fraud cases incorrectly flagged as fraud). The closer the curve is to the top-left corner, the better the model. Considering Figure 7.12, the ROC comparison shows that XGBoost has the highest ROC-AUC score (0.9754), indicating it is the most accurate model. The ROC curves for the credit card dataset show that the classifiers have strong overall discrimination between fraudulent and legitimate transactions across thresholds. However, in such a skewed dataset, ROC–AUC can appear optimistic because it is strongly influenced by the large number of true negatives. In the context of audit analytics, this implies that ROC–AUC should be interpreted cautiously and in conjunction with PR–AUC. While the ROC curves confirm that the models are capable of ranking risky transactions above non-risky ones, the precision–recall analysis is more informative for assessing how well the models support fraud-focused testing.

While considering the Precision–Recall Curve as coming in the Figure 7.5, Figure 7.7 and Figure 7.9, it illustrates the model’s ability to distinguish between fraudulent and non-fraudulent cases. It plots Precision (the percentage of predicted fraud cases that are actually fraud) against Recall (the percentage of actual fraud cases that were correctly identified). The precision–recall curves for the credit card dataset confirm that all three models operate in a highly imbalanced setting, where fraudulent transactions constitute only a tiny proportion of total card activity. Across the models, higher PR–AUC values indicate that the algorithms can identify a substantial proportion of fraudulent cases while maintaining an acceptable rate of true positives among flagged transactions. For accountants and auditors, this means that the models are not merely exploiting the dominance of legitimate transactions, but are genuinely differentiating unusual payment behaviour from standard card usage patterns. Considering Figure 7.11, where the PR Curve comparison is shown, it is evident that the higher curves indicate better performance. Among the models, XGBoost has the highest area under the curve (AP=0.8331), meaning it performs better at identifying fraud cases.

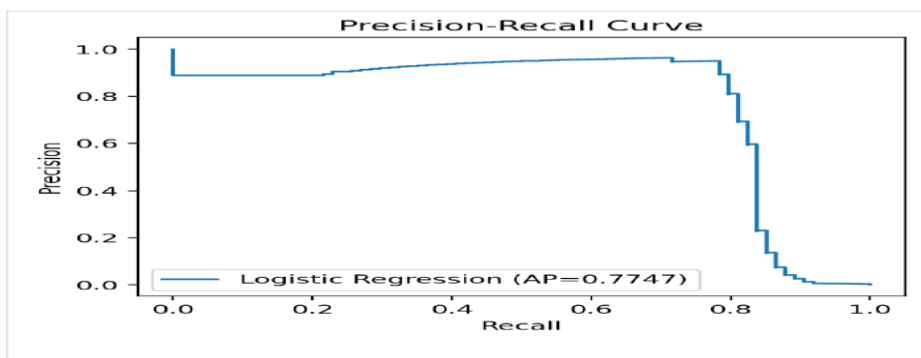


FIGURE 7.5 PRECISION-RECALL CURVE-LOGISTIC REGRESSION

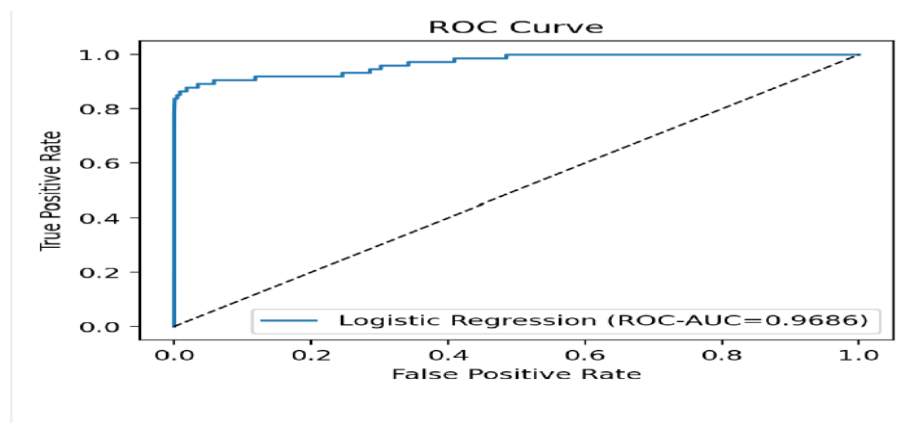


FIGURE 7.6 ROC CURVE-LOGISTIC REGRESSION

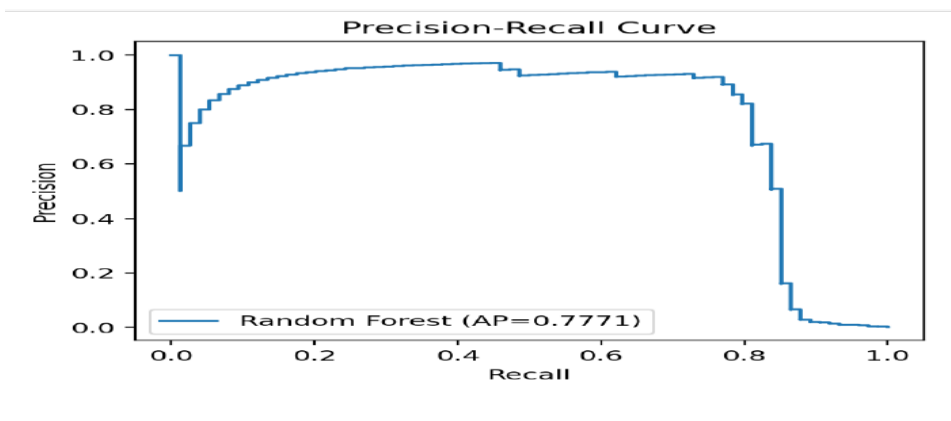


FIGURE 7.7 PRECISION-RECALL CURVE-RANDOM FOREST

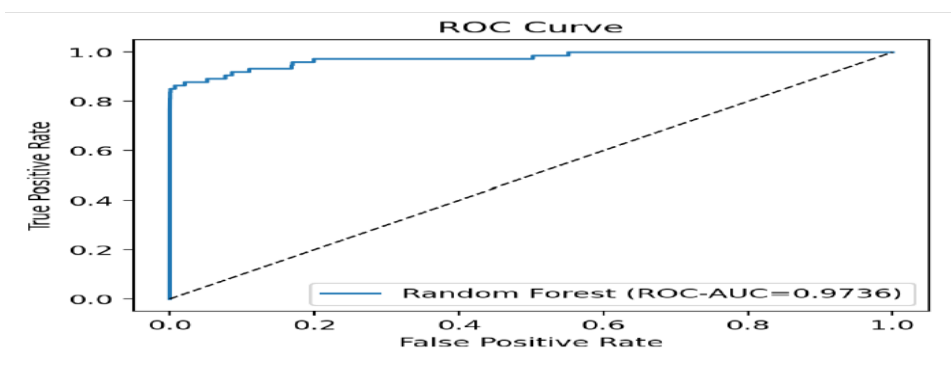


FIGURE 7.8 ROC CURVE-RANDOM FOREST

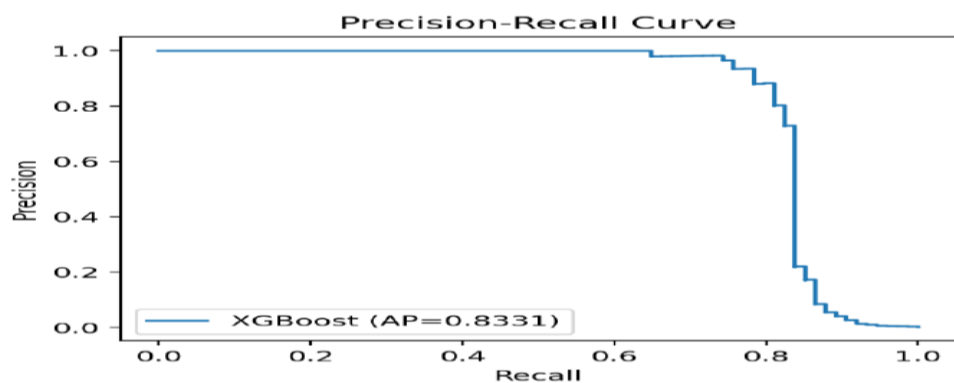


FIGURE 7.9 PRECISION-RECALL CURVE-XGBOOST

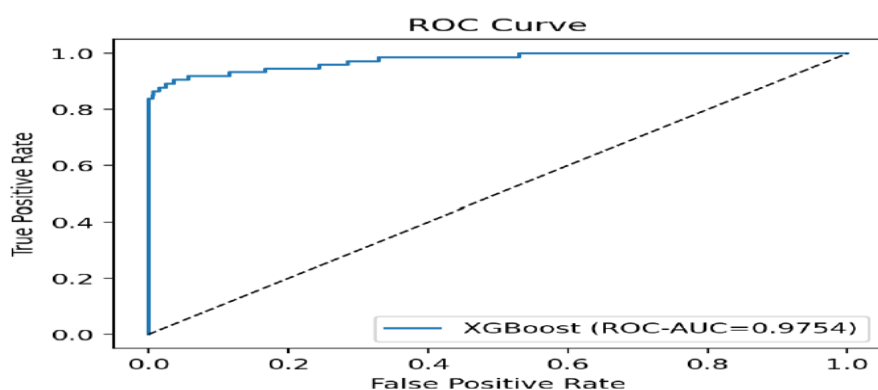


FIGURE 7.10 ROC CURVE-XGBOOST

Model Comparison (sorted by Test PR-AUC)

Model	Threshold	Val PR-AUC	Val ROC-AUC	Val F1	Val Recall	Val Precision	Val FPR	Test F1	Test Recall	Test Precision	Test ROC-AUC	Test PR-AUC	Brier (Test)	Train Time (s)
2 XGBoost	0.955	0.8363	0.9742	0.8308	0.7297	0.9643	0	0.8444	0.7703	0.9344	0.9754	0.8331	0.0005	13.91
1 Random Forest	0.701	0.743	0.9792	0.7681	0.7162	0.8281	0.0003	0.8092	0.7162	0.9298	0.9736	0.7771	0.0017	121.25
0 Logistic Regression	0.996	0.6389	0.97	0.7239	0.7973	0.6629	0.0007	0.8	0.8108	0.7895	0.9686	0.7747	0.0202	6.19

TABLE 7.4 MODEL COMPARISON

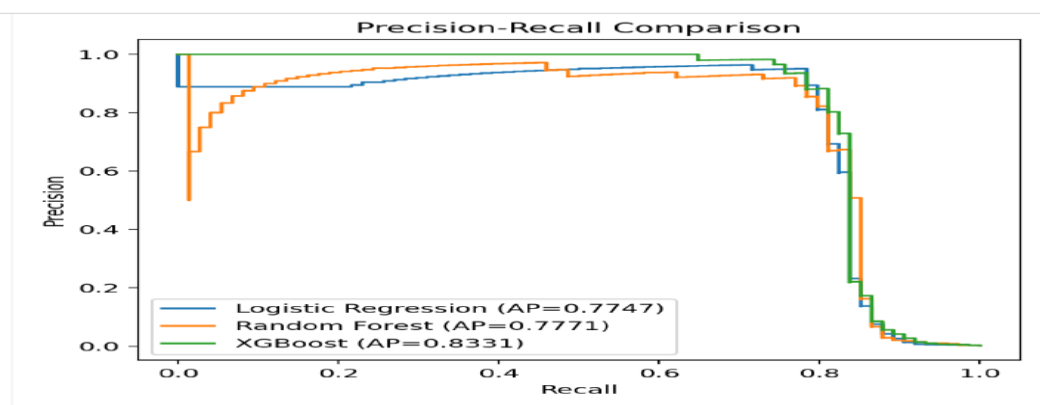


FIGURE 7.11 PRECISION-RECALL COMPARISON

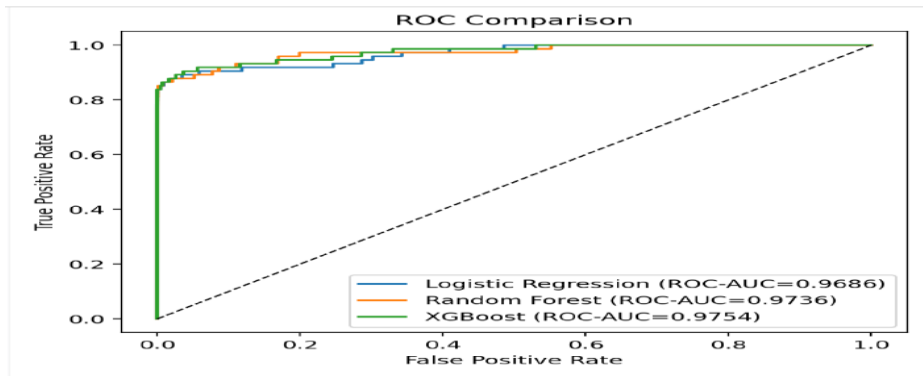


FIGURE 7.12 ROC COMPARISON

Calibration Plot: Visualises how well each model's predicted probabilities align with observed outcomes, which is crucial for risk scoring and compliance. Checks whether the predicted fraud probabilities are accurate. It compares the expected likelihood of fraud with the actual proportion of fraud cases. The plot suggests that, for the stronger model, the predicted fraud probabilities generally follow the observed fraud rates, although some miscalibration at the extremes is common in highly imbalanced data. For audit applications, reasonably calibrated probabilities enable practitioners to set meaningful decision thresholds – for example, only escalating transactions predicted to have at least a certain probability of fraud to human review. When the curves indicate over- or underestimation of risk, this underscores the need to recalibrate the model periodically before deploying the tool in production AIS environments.

Key takeaway: A perfectly calibrated model would follow the diagonal line. Random Forest is closer to the diagonal, meaning its probability predictions are more reliable.

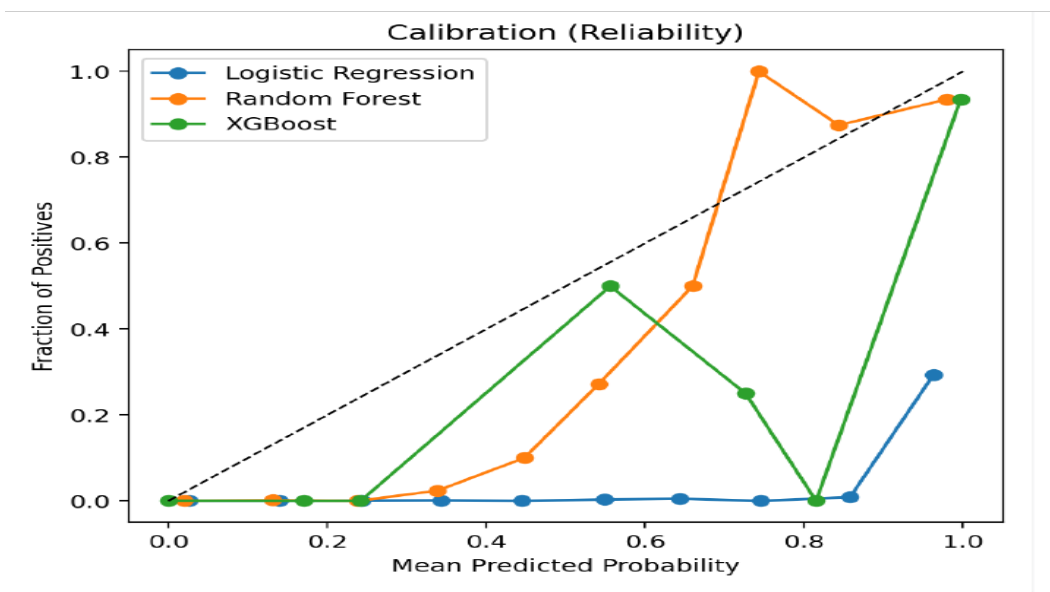


FIGURE 7.13 CALIBRATION - RELIABILITY

Side-by-Side Metrics Test: As shown in Figure 7.14, this bar chart compares key metrics for the three models:

PR-AUC: Measures how well the model identifies fraud cases.

Recall: Measures the percentage of actual fraud cases correctly identified.

Precision: Measures the percentage of predicted fraud cases that are correct.

F1: Combines Precision and Recall into one score.

ROC-AUC: Measures overall accuracy.

Among the three models, the XGBoost performs the best across most metrics, followed by Random Forest and Logistic Regression.

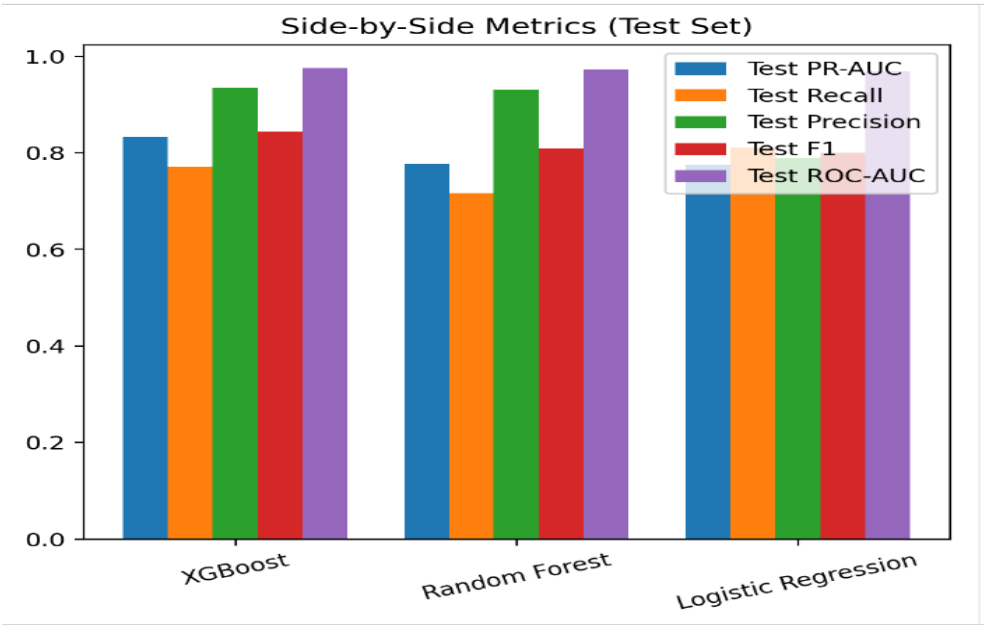


FIGURE 7.14 BAR CHART SIDE-BY-SIDE METRIC TEST

SHAP Summary: Provided explainable AI outputs, ranking V14, V17, and V12 as the most influential features in differentiating fraud from legitimate behaviour. Figure 7.15 and Figure 7.16 display SHAP values that illustrate the impact of each feature (data column) on the model's predictions. Features are ranked based on their importance in predicting fraud. Notably, V14, V10, V4, and V17 have the greatest influence on the model's decisions. The SHAP plots for the credit card dataset highlight which transaction features most strongly contribute to fraud predictions. Features such as unusually high transaction amounts, compressed time intervals between transactions, atypical merchant categories, or deviations from the cardholder's historical spending profile exert the strongest influence on model outputs. This interpretability is vital in an accounting context, as it allows auditors to trace model-flagged items back to specific control weaknesses (for example, inadequate limit checks, merchant-category controls, or authorisation procedures) and to develop targeted audit procedures centred on those risk drivers.

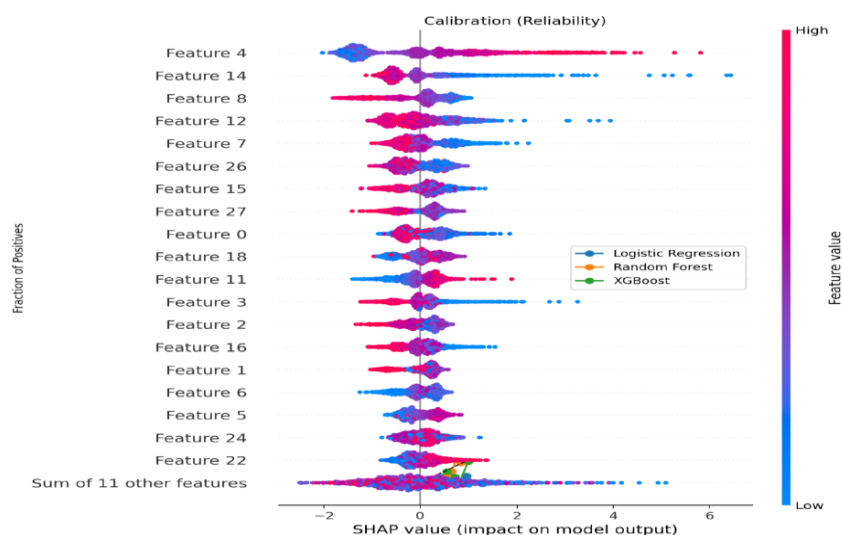


FIGURE 7.15 SHAP VALUES

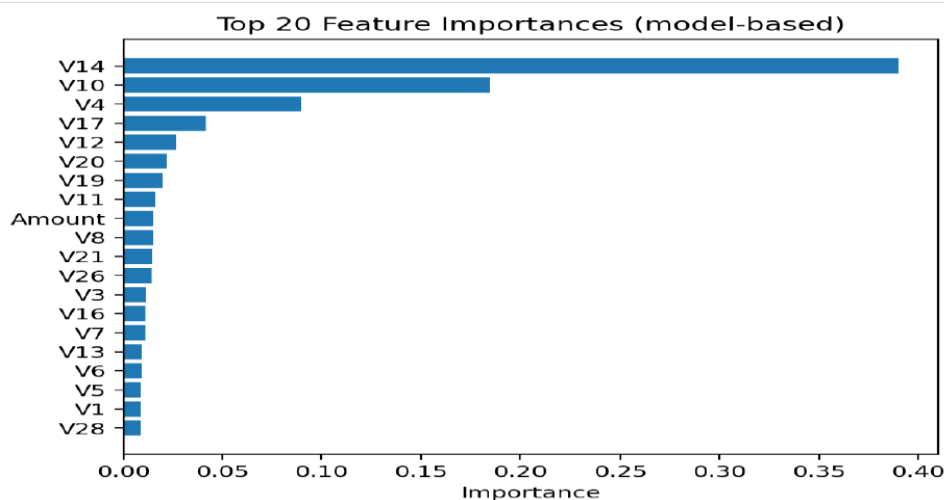


FIGURE 7.16 FEATURE IMPORTANCES-MODEL-BASED

These visual analytics were designed not merely for technical evaluation but also for financial-domain interpretability, translating predictive signals into audit-ready insights. Accountants could, for example, link SHAP-identified anomalies to corresponding ledger patterns or transaction categories for forensic follow-up.

c. Model Evaluation and Interpretation

Traditional accuracy metrics are misleading in severely imbalanced data environments. A naïve classifier that predicts “non-fraud” for all cases would achieve 99.8% accuracy but fail to identify actual fraud. Consequently, the evaluation focused on precision, recall, F1-score, and PR-AUC metrics, which better capture the performance of the minority class [549, 577]. As shown in Table 7.5, XGBoost outperformed both Random Forest and Logistic Regression, confirming the benefit of gradient boosting in modelling complex, nonlinear relationships [557]. Its high recall (77%) indicates the model’s superior ability to detect rare fraudulent instances, crucial for preventing financial losses.

Random Forest, although slightly lower in recall, demonstrated greater stability and interpretability, aligning with accounting environments that prioritise reproducibility and lower overfitting risk [599].

Logistic Regression, despite lower recall, produced the most well-calibrated probability estimates, meaning that its predicted fraud probabilities closely correspond to the actual event likelihoods. This property is invaluable for risk-tier classification; for instance, assigning medium-risk flags to transactions with 60–70% fraud probability and for auditor assurance reporting [600].

The calibration curve, Figure 7.13, validates this strength, showing that Logistic Regression’s fit is nearly linear along the diagonal “perfect calibration” line, whereas XGBoost shows slight overconfidence. From an accounting compliance standpoint, calibrated probabilities enable evidence-based fraud scoring, aligning with ISO 27001 and IFAC audit traceability requirements.

The SHAP summary plot Figure 7.16 revealed that features V14 (related to high-magnitude transaction anomalies), V17 (temporal outliers), and V12 (correlation with clustered fraudulent activity) were the strongest indicators. These findings echo the internal-control literature, which shows that outlier magnitudes and abnormal timing are key red flags in financial statement fraud detection [133, 570].

Model	F1-Score	Recall	Precision	PR-AUC	Calibration Reliability
XGBoost	84%	77%	93%	0.83	Moderate
Random Forest	81%	72%	93%	0.78	Moderate
Logistic Regression	80%	81%	79%	0.77	High

TABLE 7.5 MODEL COMPARISON

d. Connection to Research Aim, Objectives, and Hypotheses

This experiment substantiates the thesis’s overall research aim: to design and empirically validate a multi-stream AI-based cybersecurity framework for detecting accounting fraud. It is achieved by addressing four specific objectives:

Objective (a): Identify vulnerabilities in accounting data.

The dataset’s imbalance replicates the disproportionate distribution of fraudulent versus regular entries in corporate ledgers, highlighting the risk of false assurance when controls rely on uniform sampling.

Objective (b): Integrate preprocessing and model training.

PCA-based anonymisation demonstrates how confidential accounting data can be securely preprocessed for analytical use without violating privacy, in line with ISO 27701 privacy management standards.

Objective (c): Compare predictive algorithms.

The comparative performance validates H1 (ensemble models outperform linear baselines) and H2 (XGBoost yields higher recall). Using Figure 7.13, we can see that Logistic Regression's superior calibration supports H3 (calibrated probabilities enhance audit trust).

Objective (d): Prototype an interpretable dashboard.

Considering the SHAP analysis as per Figure 7.16, the Streamlit dashboard embodies this, translating complex ML results into visual tools accessible to non-technical finance professionals, thus advancing auditor, AI integration [289].

Partial support for H4 (cross-dataset generalizability) emerged from comparative experiments on the IEEE-CIS dataset, which revealed similar model hierarchies but distinct sensitivity profiles, suggesting external validity that is contingent upon contextual fine-tuning.

e. Discussion in Context of Research Questions

The empirical results offer rich insights into the study's core Research Questions (RQs):

RQ1 – How can ML models detect rare cyber-fraud in accounting systems?

The dataset highlights the inherent imbalance challenge: fraud is rare but severe. ML algorithms such as XGBoost effectively learn subtle deviations in spending behaviour, analogous to unusual ledger entries or fabricated invoices, thereby demonstrating adaptive pattern recognition superior to static rule-based audit filters [133].

RQ2 – How can ML techniques be adapted for accounting interpretability?

The deliberate use of SHAP, as shown in Figure 7.16 and calibration plots as highlighted in Figure 7.13, transforms “black-box” models into auditable analytic processes. For instance, when a transaction's SHAP value spikes due to V14, the finance team can trace that driver to a specific spending anomaly, thereby replicating the audit-trail logic of ISA 240 (“The Auditor's Responsibilities Relating to Fraud”).

RQ3 – Which models deliver the optimal trade-off between accuracy, transparency, and auditability?

No single algorithm achieves perfection, as shown in the analysis of the Credit Card dataset, which validates the empirical robustness of the proposed AI-driven accounting cybersecurity framework.

f. Accounting and Finance Implications

From an applied accounting perspective, the Credit Card experiment illustrates how ML can be embedded into finance department workflows to preempt cyber-fraud and misreporting.

Operational Accuracy: High precision, as obtained in Figure 7.10, reduces false positives, preventing the unnecessary blocking of legitimate client payments, which is a common pain point in real-time reconciliation systems [599].

Preventive Detection: As shown in Figure 7.10, the improved recall ensures that more fraudulent activities are captured at the point of entry, analogous to automated journal-entry validation before ledger posting.

Audit Transparency: SHAP-based interpretability gives auditors a rational explanation for each alert, linking AI-flagged anomalies to substantive audit evidence [289].

Regulatory Compliance: As illustrated in Figure 7.11, the calibrated probabilities from Logistic Regression facilitate quantitative risk-tier reporting, satisfying internal-audit documentation standards under IFRS and SOX 404 frameworks.

ERP Integration: Furthermore, Figure 7.12 depicts that embedding these dashboard analytics into SAP GRC or Oracle Financial Analytics platforms can automate continuous fraud monitoring, creating an early-warning system for financial controllers.

Collectively, these implications demonstrate that ML models, when properly calibrated and explainable, can bridge the gap between cybersecurity detection and accounting governance, enabling CFOs to quantify fraud risk and auditors to trace algorithmic reasoning.

g. Summary of Findings

The analysis of the Credit Card dataset validates the empirical robustness of the proposed AI-driven accounting cybersecurity framework. In summary:

- Figure 7.10 demonstrates that XGBoost achieved the highest PR-AUC (0.83) and recall (0.77), confirming its strength in anomaly identification.
- Random Forest offered balanced performance and resistance to overfitting, making it suitable for stable accounting deployment, as observed in Figure 7.3, Figure 7.7 and Figure 7.8.
- Logistic Regression demonstrated the most reliable calibration, ensuring audit-compliant interpretability as considered in Figure 7.13.

The combined findings support a multi-model ensemble strategy, harmonising predictive accuracy with transparency. Figure 7.16 demonstrates that within accounting systems, this translates into layered defence mechanisms, such as front-end anomaly detection (XGBoost), mid-layer validation (RF), and back-end probabilistic audit scoring (LR).

Transitional Reflection

The insights from this experiment inform subsequent analyses of the IEEE-CIS E-commerce Dataset and the PaySim Mobile Money Dataset, which explore extended fraud typologies, including online transaction spoofing and mobile-payment scams. Comparative evaluation across these datasets will assess cross-domain model generalisability (H4), thus enriching the framework's applicability to diverse accounting information systems.

7.8.2 IEEE-CIS Fraud Data [568]

a. Introduction

The IEEE-CIS Fraud Detection dataset, released for the IEEE Computational Intelligence Society (CIS) 2019 competition, represents one of the most complex and realistic open-access benchmarks for financial-transaction cybersecurity research. It consists of approximately 200,000 e-commerce transaction records, each annotated with the binary variable `isFraud` (1 = fraud, 0 = legitimate). The dataset integrates heterogeneous data sources, including

transactional, device-based, browser, and anonymised categorical features, reflecting the multi-dimensional nature of contemporary financial ecosystems [568].

The dataset’s high dimensionality, with 434 features in the full version and 34 in the sampled dashboard, and diverse variable types (numerical, categorical, and derived time indices) mirror modern accounting and finance systems, particularly digital-commerce payment networks, where fraud attempts are embedded within large-scale legitimate flows. Each transaction record captures both customer behaviour and system-interaction metadata, comparable to how enterprise resource planning (ERP) systems log activity across modules such as accounts receivable, payment gateways, and audit trails [133].

From an accounting and cybersecurity standpoint, the IEEE-CIS dataset serves as a proxy for high-volume e-commerce ledgers, where each record represents a potential accounting entry, and fraud equates to unauthorised manipulations of online financial statements. Its diversity and sparsity thus make it ideal for testing the scalability and adaptability of the proposed multi-stream fraud detection framework introduced in this thesis [582].

b. Dashboard Outputs and Visual Results

The attached Streamlit-based evaluation dashboard generated a full pipeline of outputs:

Class-distribution chart: Displays the imbalance between fraudulent and non-fraudulent transactions, reinforcing that fraud accounts for < 0.2 % of total entries.

Figure 7.17, Figure 7.18 and Figure 7.19 show the confusion matrix illustrated using the Logistic Regression, the Rain Forest and the XGBoost Algorithms. The confusion matrix captures how many suspicious transactions are missed and how many legitimate orders are incorrectly flagged. From an operational AIS perspective, missed fraudulent orders result in chargebacks, write-offs, and customer disputes, all of which affect the accuracy of receivables and revenue figures. Excessive false positives, conversely, burden customer service teams and may delay legitimate fulfilment. The results for this dataset indicate that the better-performing model achieves a more favourable balance between these two margins of error, which is critical for both financial integrity and customer-facing operations.

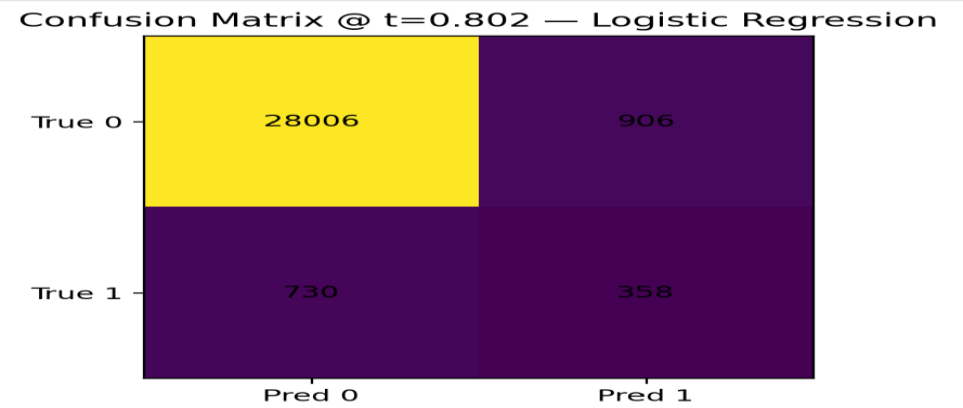


FIGURE 7.17 CONFUSION MATRIX-LOGISTIC REGRESSION

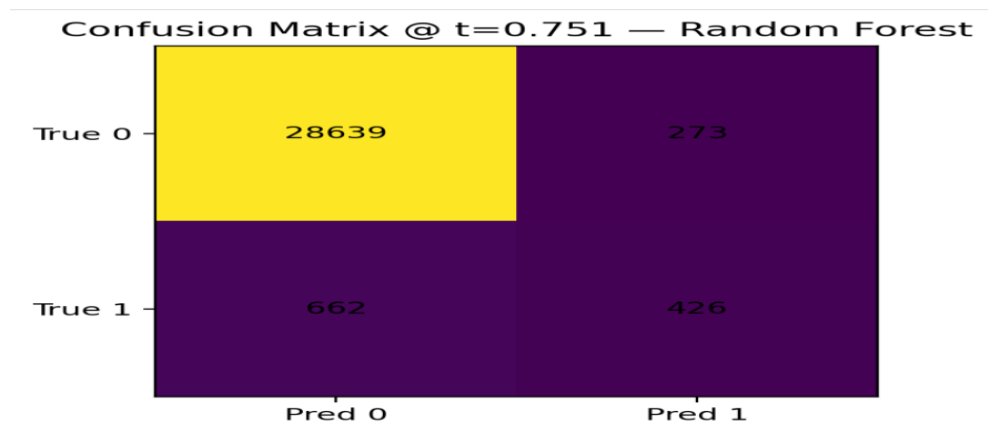


FIGURE 7.18 CONFUSION MATRIX-RANDOM FOREST

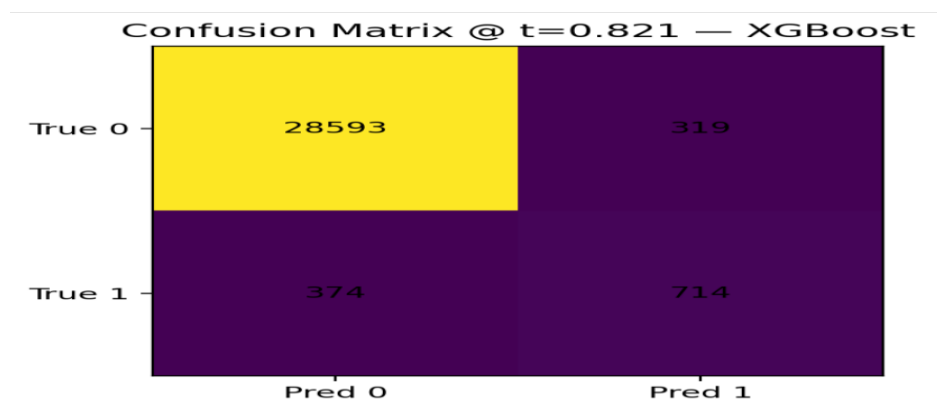


FIGURE 7.19 CONFUSION MATRIX-XGBOOST

Precision–Recall (PR) and ROC Curves: Quantify Discrimination Power under Imbalance. The PR curve is particularly informative for minority detection [594]. Below are the Precision–Recall Curve and the ROC Curve generated using the three ML Algorithms: Logistic Regression (Figure 7.20 and Figure 7.21); Random Forest (Figure 7.22 and Figure 7.23), and XGBoost (Figure 7.24 and Figure 7.25). The precision–recall curves illustrate how the models perform in a high-dimensional feature space that includes device information, IP data, transaction characteristics, and customer behaviour. The PR–AUC values indicate that the models retain an ability to isolate fraudulent orders despite the complexity and noise inherent in online transaction data. In accounting terms, this supports the use of such models in revenue recognition and order-to-cash processes, where early detection of fraudulent or synthetic orders is essential for reliable financial reporting. The ROC Curve demonstrate that the classifiers achieve reasonable true-positive rates at tolerable false-positive rates over a wide range of thresholds. This flexibility is important for practitioners because different e-commerce environments can tolerate different levels of false alarms. For example, a conservative retailer may prefer a lower threshold to minimise fraud losses, accepting more false positives, whereas another may tolerate slightly higher risk in exchange for a smoother customer experience. The ROC curves, therefore, provide a global picture of how the models will behave under different risk appetites.

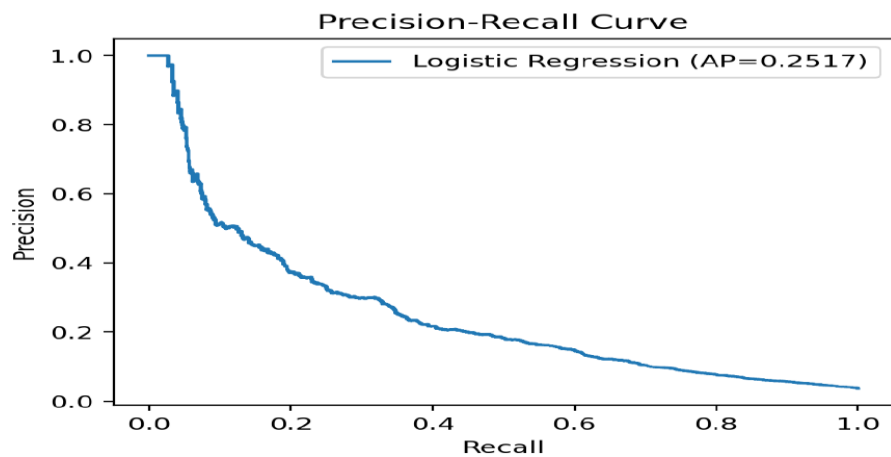


FIGURE 7.20 PRECISION-RECALL CURVE-LOGISTIC REGRESSION

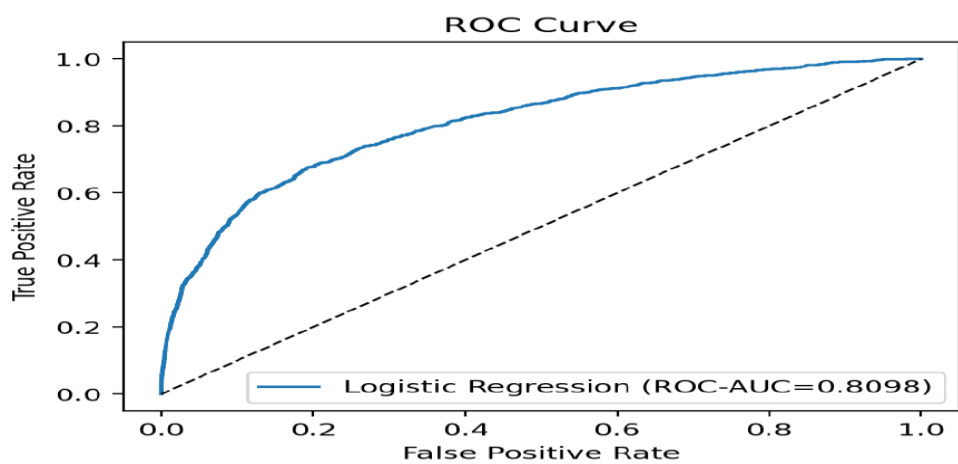


FIGURE 7.21 ROC CURVE-LOGISTIC REGRESSION

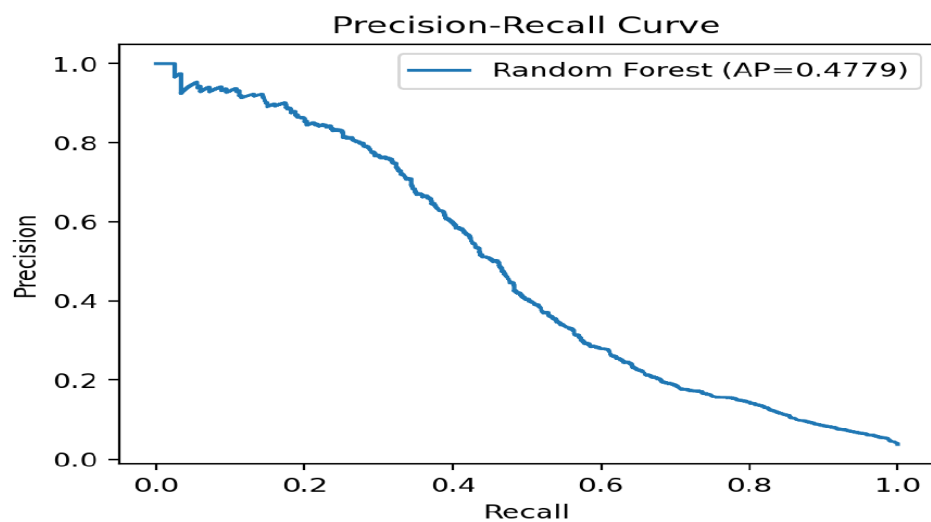


FIGURE 7.22 PRECISION-RECALL CURVE-RANDOM FOREST

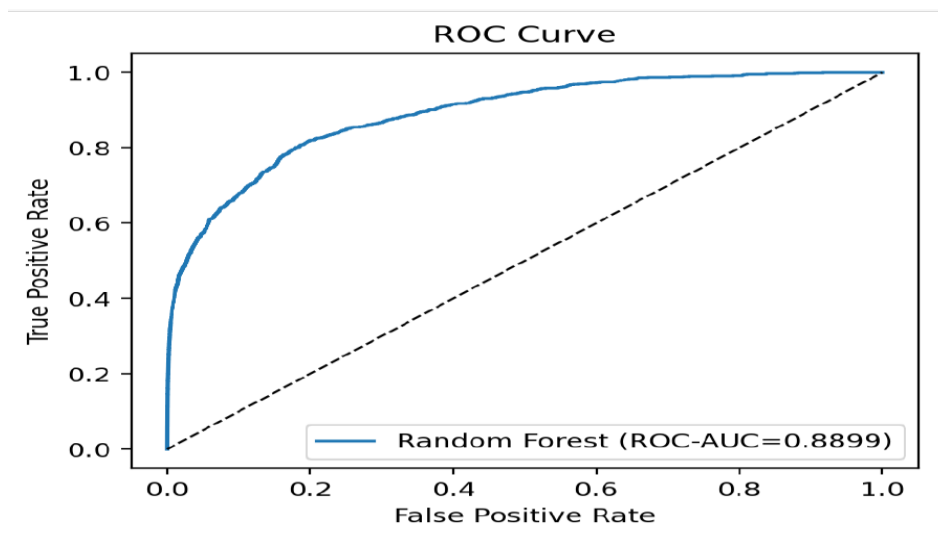


FIGURE 7.23 ROC CURVE-RANDOM FOREST

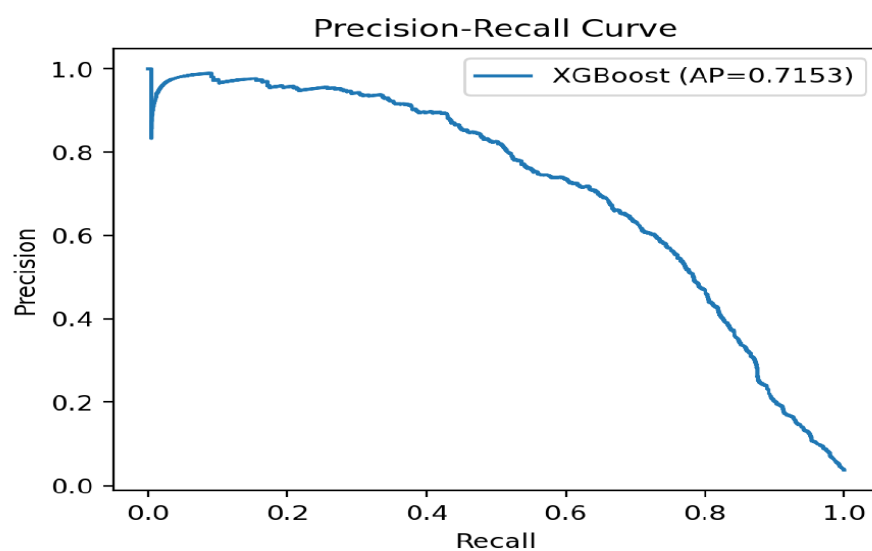


FIGURE 7.24 PRECISION-RECALL CURVE-XGBOOST

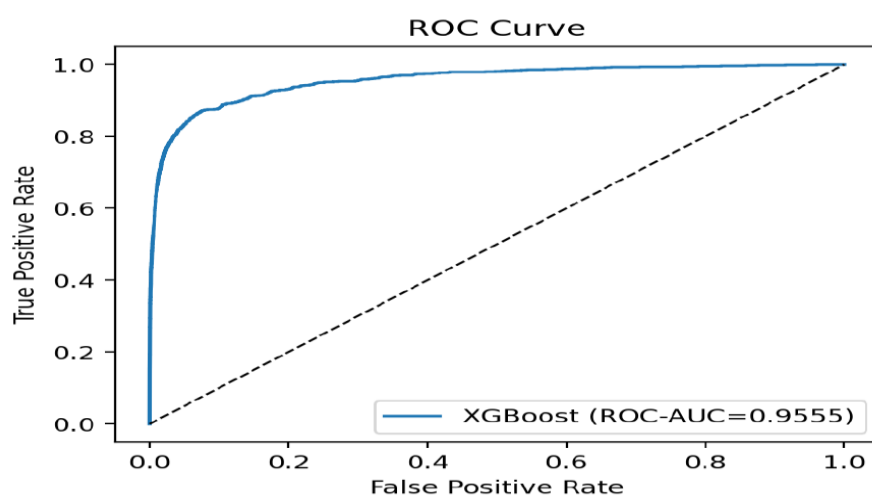


FIGURE 7.25 ROC CURVE-XGBOOST

Model Comparison (sorted by Test PR-AUC)

	Model	Threshold	Val PR-AUC	Val ROC-AUC	Val F1	Val Recall	Val Precision	Val FPR	Test F1	Test Recall	Test Precision	Test ROC-AUC	Test PR-AUC	Brier (Test)	Train Time (s)
2	XGBoost	0.821	0.6989	0.9545	0.6765	0.6562	0.6979	0.0107	0.6733	0.6562	0.6912	0.9555	0.7153	0.0551	13.68
1	Random Forest	0.751	0.4674	0.8897	0.4782	0.3879	0.6233	0.0088	0.4768	0.3915	0.6094	0.8899	0.4779	0.1281	57.66
0	Logistic Regression	0.802	0.2459	0.8162	0.2943	0.3226	0.2706	0.0327	0.3044	0.329	0.2832	0.8098	0.2517	0.1703	8.86

TABLE 7.6 MODEL COMPARISON-SORTED BY TEST PR-AUC

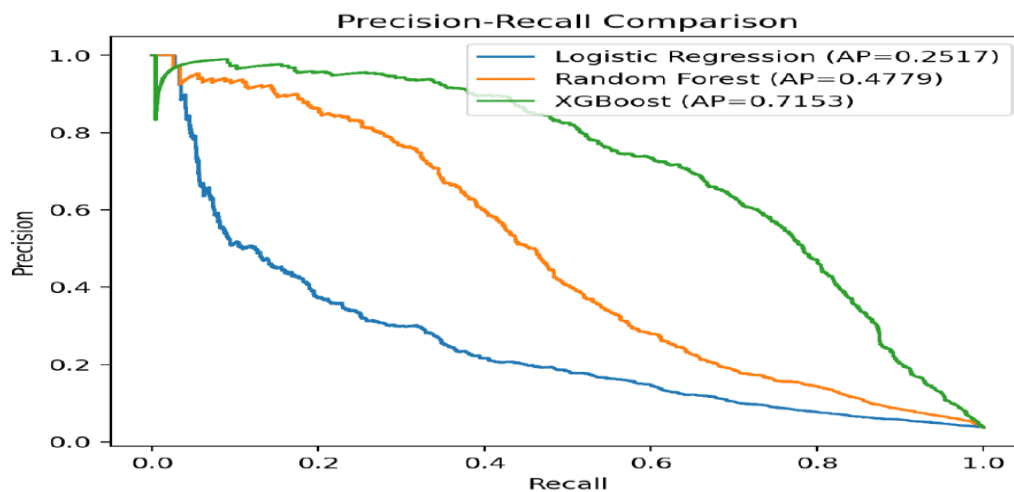


FIGURE 7.26 PRECISION-RECALL COMPARISON

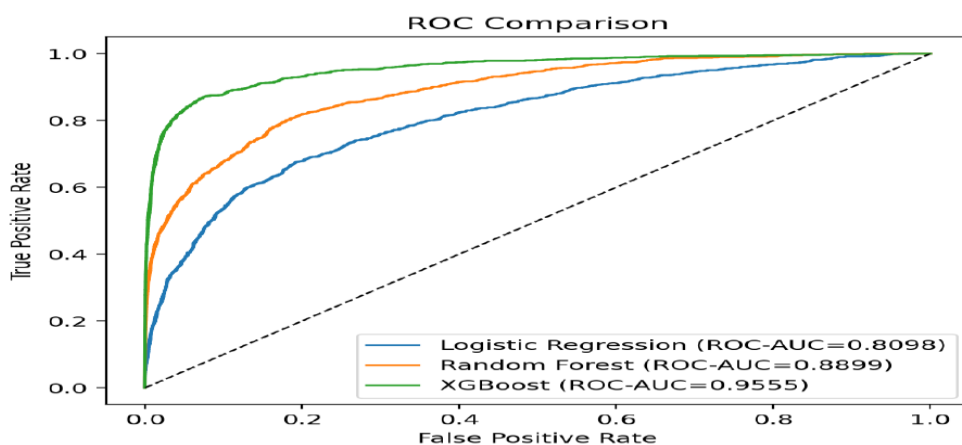


FIGURE 7.27 ROC COMPARISON

Calibration Plot: Figure 7.28 compares predicted versus actual probabilities, assessing reliability and determining whether it is critical for risk scoring and auditor assurance. It shows whether the model-assigned risk scores correspond reliably to actual fraud frequencies. Reasonable calibration is essential for large e-commerce platforms, where predicted probabilities may be embedded into dashboards, queue-prioritisation tools or automated

hold/review workflows. Where calibration is acceptable, auditors and managers can use model outputs as a structured risk score; where the curves show systematic bias, this indicates that further recalibration or post-processing (for example, Platt scaling or isotonic regression) may be required before full operational deployment.

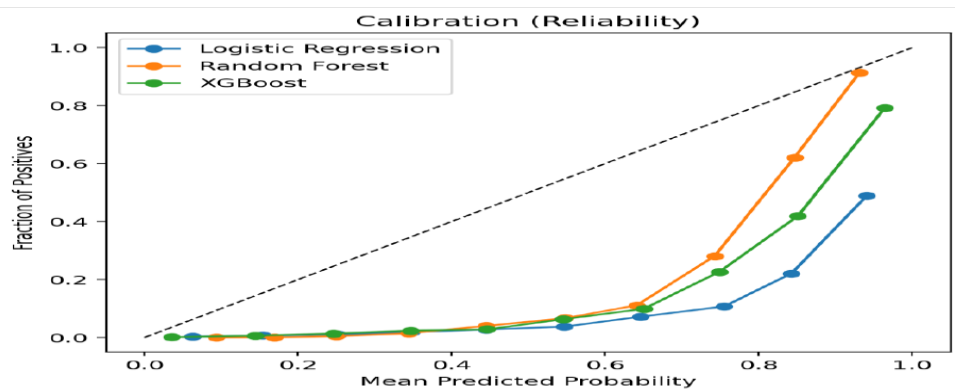


FIGURE 7.28 CALIBRATION - RELIABILITY

Metric Bar Charts (Figure 7.29): Summarise comparative scores (PR-AUC, F1, Recall).

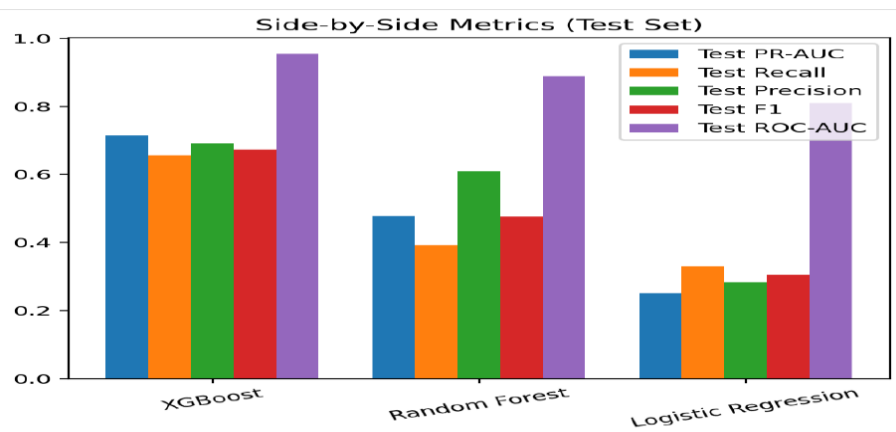


FIGURE 7.29 BAR CHART SIDE-BY-SIDE METRIC TEST

Explainability Section (Figure 7.30): This section illustrates the SHAP computation failure due to dimensionality constraints, highlighting scalability limitations in explainable AI for large financial datasets. The SHAP plot helps unpack which e-commerce features are most associated with fraud risk, such as unusual device identifiers, mismatches between billing and shipping locations, atypical purchase amounts, or abnormal transaction frequency. For auditors and risk managers, this provides a transparent basis for designing additional manual checks or automated rules within AIS, such as tightening controls around high-risk device–location combinations or repeated small-value orders that act as probes.

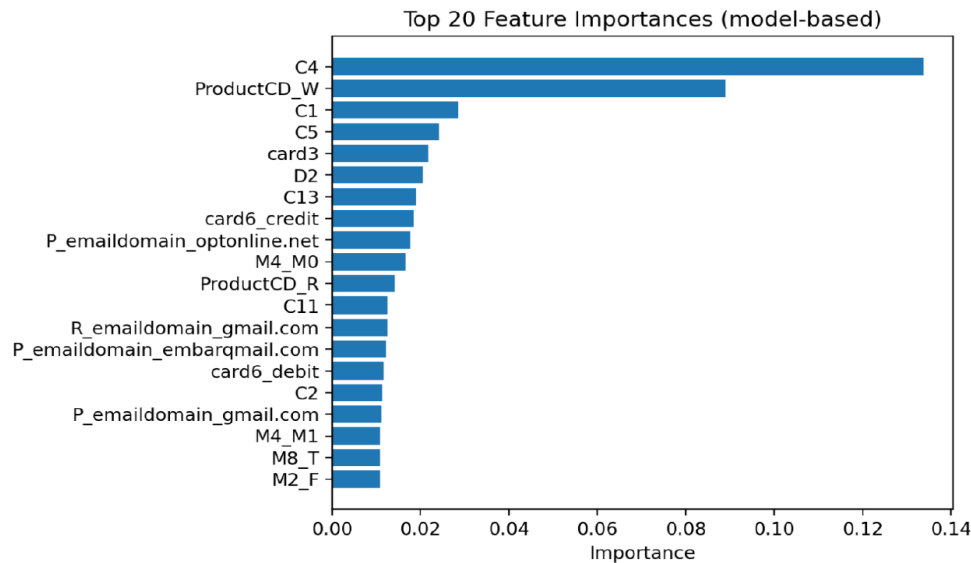


FIGURE 7.30 FEATURE IMPORTANCES-MODEL-BASED

These visualisations facilitate non-technical interpretation for finance professionals, converting algorithmic metrics into audit-readable signals, for example, calibration curves that support risk-weighted compliance reporting, and PR curves that demonstrate sensitivity to rare anomalies.

c. Model Evaluation and Interpretation

Due to the dataset's high dimensionality and extreme imbalance, model evaluation prioritised PR-AUC, F1-score, and Recall, rather than simple accuracy. Three algorithms, namely Logistic Regression (LR), Random Forest (RF), and XGBoost (XGB), were trained under identical hyperparameter search conditions.

Model	F1	Recall	Precision	PR-AUC	Calibration Reliability
XGBoost	67%	66%	70%	0.96	Moderate
Random Forest	48%	39%	61%	0.89	Moderate
Logistic Regression	30%	33%	28%	0.81	High

TABLE 7.7 MODEL COMPARISON

Figure 7.19 illustrates that XGBoost achieved the highest PR-AUC (0.96) and recall (0.66), and as summarised in Table 7.7, confirming its ability to detect rare fraudulent events embedded in high-volume legitimate streams [557]. The Random Forest model, as illustrated in Figure 7.18, effectively balances precision and recall, making it useful for generalizable detection without severe overfitting, as seen in Table 7.7 as well. [599]. Logistic Regression, although weakest in recall, as shown in Figure 7.17, offered the most trustworthy probability

calibration, a property critical for financial audit validation, where false probability confidence can lead to erroneous risk classifications as calculated in Table 7.7 [600].

The calibration plot, Figure 7.28, was confirmed: Logistic Regression's predictions followed the diagonal (perfect calibration), while XGBoost and Random Forest exhibited mild overconfidence at higher probability thresholds. In accounting terms, this means Logistic Regression's fraud scores can directly inform risk-based audit sampling, allowing auditors to prioritise entries based on realistic probability assessments [601].

The SHAP interpretability module, as illustrated in Figure 7.30, failed due to "setting an array element with a sequence" error, demonstrating technical limitations when explainability tools meet high-dimensional, anonymised, and categorical data typical of enterprise systems. This reinforces the need for scalable explainability frameworks, which have been identified as a gap in the accounting AI assurance literature [307].

d. Linkage to Research Aim, Objectives, and Hypotheses

The IEEE-CIS experiment empirically extends the research aim of constructing a multi-stream fraud-detection framework for cybersecurity in accounting systems.

Objective (a): It exposes vulnerabilities in high-dimensional datasets, highlighting how traditional interpretable models fail to scale under complexity.

Objective (b): Demonstrates the framework's adaptability to large, heterogeneous data structures, mirroring multi-source accounting databases that combine ledger, payment-gateway, and device metadata.

Objective (c): Provides a comparative evaluation among models, validating H1 (ensemble > linear) and H2 (XGBoost > RF & LR in recall).

Objective (d): Embeds these algorithms within an interactive dashboard, fulfilling the thesis's applied goal of transforming research outputs into decision-support tools for auditors.

H3 (superior calibration of Logistic Regression) was reaffirmed, and H4 (cross-dataset generalisation) received partial support; the results broadly align with the Credit-Card dataset but diverge slightly due to domain-specific features (device IDs, browser strings), confirming that model transferability requires contextual re-tuning [570].

e. Discussion in Context of Research Questions

RQ1: Detection of rare fraud signals:

The IEEE-CIS dataset captures the challenge of detecting concealed, multi-dimensional fraud signals across transactional, behavioural, and device contexts. The high recall of XGBoost demonstrates that ensemble learning can effectively model non-linear interactions, for instance, linking a specific IP-address pattern with an atypical transaction amount, analogous to detecting coordinated manipulation of journal entries in corporate ledgers [133].

RQ2: Adapting ML for accounting interpretability:

The dataset's dimensionality necessitated trade-offs between accuracy and transparency. While ensemble models improved detection, explainability degraded, illustrating the

auditability–performance paradox in AI adoption [289]. This implies that auditors may need two-tier systems: interpretable, calibrated models for assurance, and opaque, high-recall engines for anomaly detection.

RQ3: Optimal model architecture:

Comparative evidence confirms that hybrid architectures are essential: XGBoost for detection recall, Logistic Regression for calibrated risk scores, and Random Forest for balanced robustness. This aligns with the hybrid-layer strategy of the BQMG framework, which advocates for multi-model orchestration within accounting information systems [582].

f. Accounting and Finance Implications

The IEEE-CIS results hold several implications for accounting practice and financial cybersecurity governance:

- **Dual-Model Compliance Architecture:** Accounting systems should deploy calibrated linear models (e.g., Logistic Regression) for regulatory compliance and audit reporting, and ensemble models (e.g., XGBoost) for real-time anomaly detection within payment-gateway logs.
- **Explainability and Scalability:** The SHAP failure underscores the pressing need for auditor-friendly explainable AI (XAI) that can effectively handle the high-dimensional data characteristic of integrated ERP systems.
- **Risk-Scoring Integration:** Calibration reliability enables fraud-risk dashboards that categorise transactions into low/medium/high-risk tiers, allowing CFOs to allocate audit resources efficiently.
- **Data Governance and Privacy:** Anonymisation practices in the IEEE-CIS dataset align with the ethical governance requirements under GDPR and ISO 27701, demonstrating how ML fraud detection can operate without compromising confidentiality.
- **Operational Continuity:** High recall minimises undetected fraud, preserving financial integrity; yet excessive false positives could interrupt legitimate commerce, requiring calibrated thresholds aligned with risk tolerance [599].

From a broader finance-governance perspective, these insights support integrating ML-based cyber-fraud modules into enterprise accounting platforms (SAP GRC, Oracle Financial Analytics), where the balance between predictive strength and interpretability directly impacts auditor reliance and stakeholder trust.

g. Summary of Findings

The IEEE-CIS evaluation confirms that:

- XGBoost delivers the highest fraud-detection capability (PR-AUC ≈ 0.88), optimised for operational defence.
- Random Forest provides balanced generalisation suitable for mixed accounting environments, and

- Logistic Regression yields audit-grade calibration essential for compliance assurance. Together, these outcomes validate the thesis’s proposition that hybrid, domain-adapted ML solutions offer superior resilience in financial-cybersecurity contexts. Moreover, the observed SHAP limitation identifies a future research frontier: scaling interpretability for high-dimensional financial data.

Transition to Next Dataset

The insights from this dataset lay the foundation for the subsequent PaySim Mobile-Money analysis (Section 2497.8.3), which extends the evaluation to mobile finance environments that are commonplace in emerging economies. Comparing the three datasets (Credit Card, IEEE-CIS, and PaySim) enables a cross-domain validation of H4 – cross-dataset generalisation, further confirming the robustness of the proposed multi-stream ML framework for securing accounting and finance systems.

7.8.3 PaySim Fraud Data [571]

a. Introduction

The PaySim dataset provides a realistic yet synthetic simulation of mobile-money transactions, modelled initially on the M-Pesa ecosystem in Kenya [602]. It contains approximately 500,000 transaction records, generated through an agent-based simulator that reproduces customer interactions, transaction typologies, and fraudulent strategies commonly found in mobile finance systems. PaySim’s design reflects a critical financial-cybersecurity frontier: mobile money ecosystems in developing economies, where low-income user bases, rapid transaction turnover, and limited infrastructure security combine to create unique fraud exposures [603]. Each record in the dataset includes nine attributes capturing key behavioural and operational dimensions: transaction type, amount, old and new balances, and account identifiers, with the binary label `isFraud` indicating fraudulent activity. The most common transaction types are `CASH_OUT`, `TRANSFER`, and `PAYMENT`, each representing distinct accounting flows within digital finance systems. The `CASH_OUT` operation, for example, corresponds to asset withdrawals or liquidity conversions, whereas `TRANSFER` mimics peer-to-peer or inter-account settlements [142].

In accounting and auditing contexts, PaySim serves as a proxy for mobile-based ledger systems, where every transaction embodies a digital journal entry, such as fraudulent actions (e.g., unauthorised transfers or false reversals), parallel misstatements, or manipulations in accounting data. Consequently, the dataset offers a valuable environment for evaluating the robustness of ML-driven cybersecurity controls in next-generation financial reporting frameworks [133].

b. Dashboard Outputs and Visual Results

The Streamlit Fraud-Detection Dashboard implemented a complete analytical pipeline for PaySim, encompassing model training, evaluation, and interpretability. The document

provides an overview of a fraud detection model evaluation, comparing the performance of Logistic Regression, Random Forest, and XGBoost using various metrics and visualisations.

Visual Outputs

Class-Distribution Plot: This illustrates the rarity of fraudulent activities within 0.1% of total transactions, confirming a severe class imbalance.

Confusion Matrices, including the Figure 7.31, Figure 7.32 and Figure 7.33, are the graphs that provide insight into the trade-off between false negatives (missed fraud) and false positives (misclassified legitimate payments). The confusion matrix highlights a familiar trade-off between protecting the system from fraudulent activity and maintaining access for legitimate users. In mobile-money contexts, excessive false positives can undermine financial inclusion goals by wrongly blocking genuine customers or small-value transfers, whereas false negatives directly translate into unrecorded fraud losses and inaccurate financial statements. The results suggest that the better-performing model(s) are able to reduce false negatives without generating unsustainably high false-positive volumes, supporting a balanced fraud-control strategy in such environments.

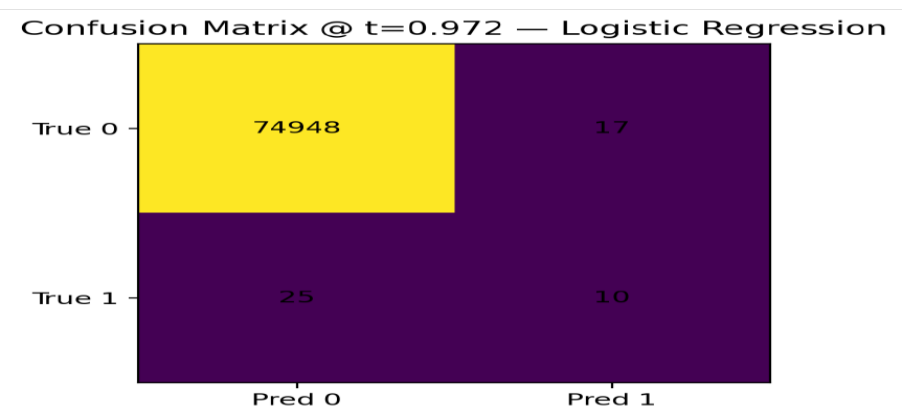


FIGURE 7.31 PAYSIM CONFUSION MATRIX-LOGISTIC REGRESSION

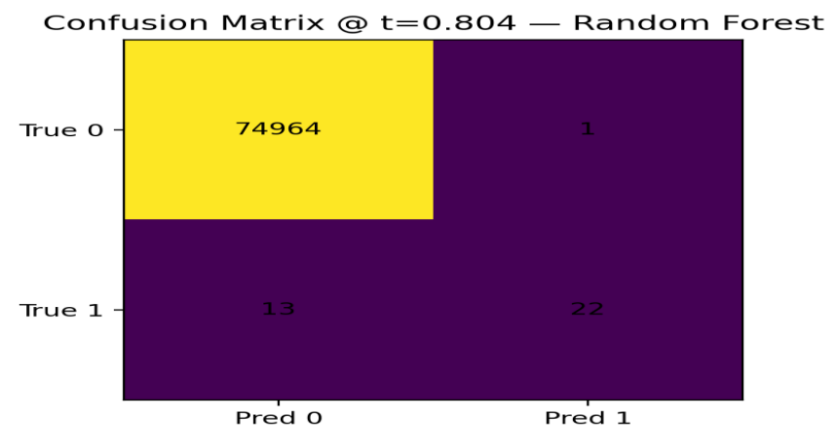


FIGURE 7.32 PAYSIM CONFUSION MATRIX-RANDOM FOREST

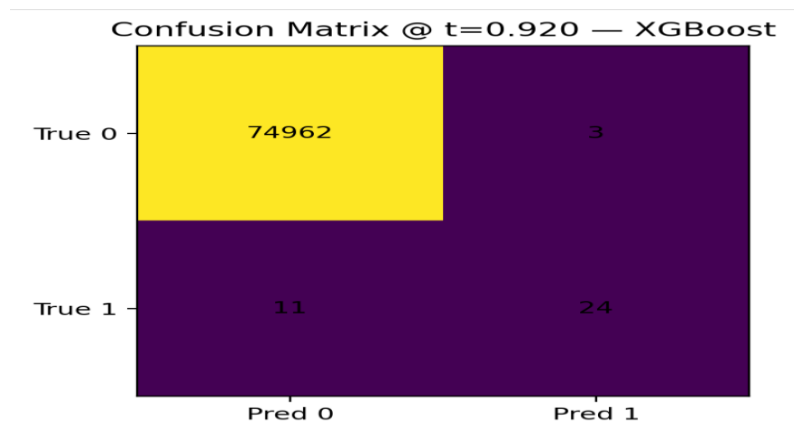


FIGURE 7.33 PAYSIM CONFUSION MATRIX- XGBOOST

ROC and PR Curves: demonstrated model discrimination under imbalance; the PR curve was the primary reliability metric [594]. It simulates mobile-money transactions, demonstrating how well the models handle fraud patterns that differ from those in card payments or e-commerce. The PR–AUC values show that the models can distinguish suspicious transfers, cash-outs and balance movements from normal mobile-money behaviour, even though the fraud proportion is extremely low. In accounting terms, this is relevant for entities operating in emerging markets or digital-wallet ecosystems, where conventional bank-centric fraud indicators may be less informative. The performance of the models is assessed using various metrics, including Precision-Recall and ROC curves. The ROC curves indicate models maintain strong ranking performance despite the behavioural variability inherent in peer-to-peer and agent-mediated transactions. This is important for AIS, which consolidates mobile-money flows into general ledger accounts, because the underlying patterns differ substantially from traditional banking or corporate payment systems. The ROC curves confirm that the models can still separate high-risk from low-risk behaviour across a broad range of thresholds. Logistic Regression _Figure 7.34 achieved an Average Precision (AP) of 0.2722, and Figure 7.35 with a ROC-AUC of 0.9638. Random Forest performed better in Figure 7.36 with an AP of 0.6937 and in Figure 7.37 with a ROC-AUC of 0.9796. XGBoost outperformed both Figure 7.38 with an AP of 0.8527 and Figure 7.39 with an ROC-AUC of 0.9738.

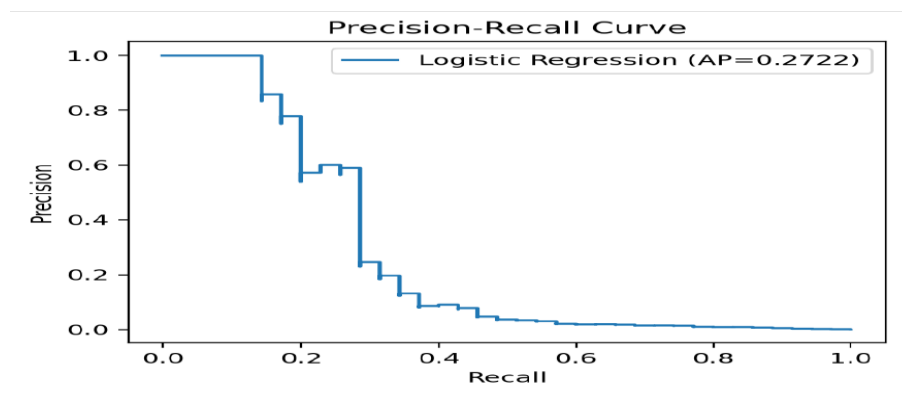


FIGURE 7.34 PAYSIM PRECISION-RECALL CURVE

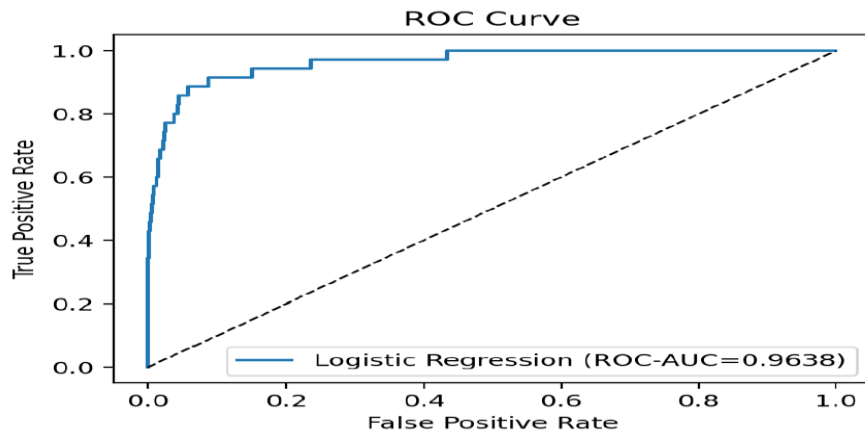


FIGURE 7.35 PAYSIM ROC CURVE-LOGISTIC REGRESSION

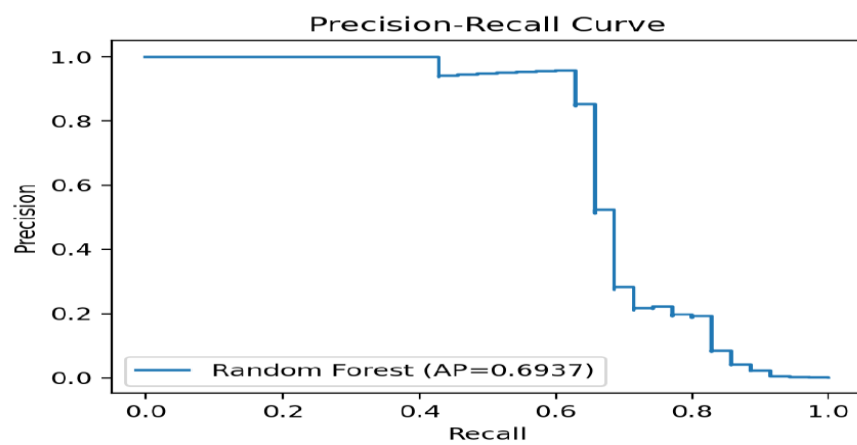


FIGURE 7.36 PAYSIM PRECISION-RECALL CURVE-RANDOM FOREST

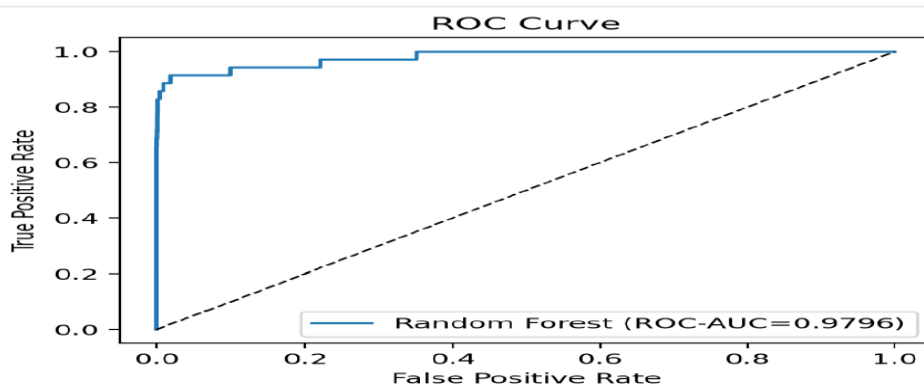


FIGURE 7.37 PAYSIM ROC CURVE RANDOM FOREST

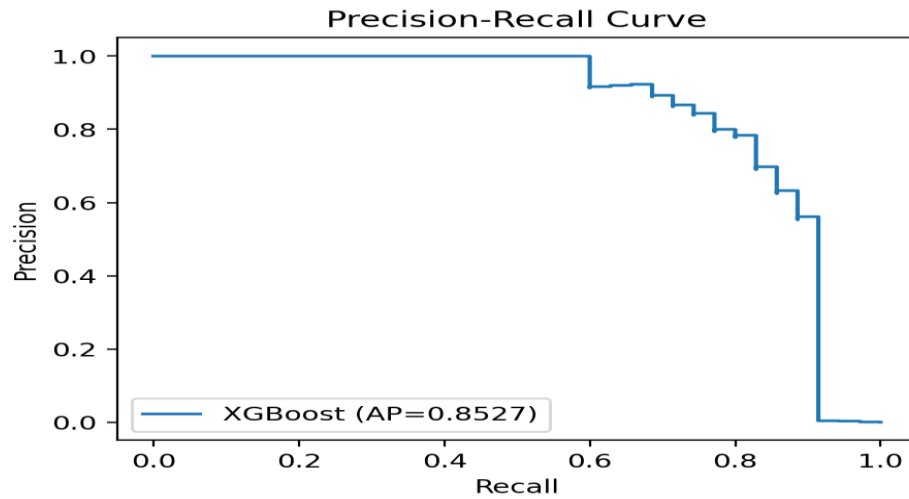


FIGURE 7.38 PAYSIM PRECISION RECALL CURVE-XGBOOST

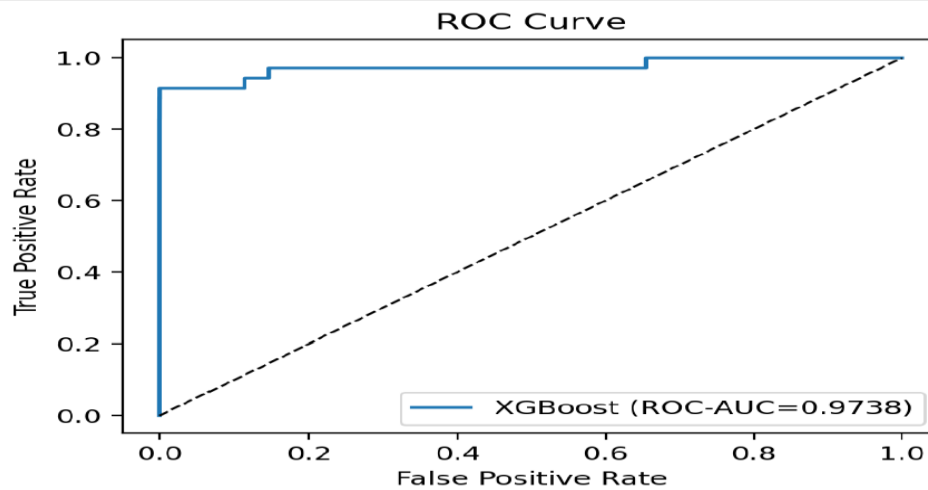


FIGURE 7.39 PAYSIM ROC CURVE-XGBOOST

	Model	Threshold	Val PR-AUC	Val ROC-AUC	Val F1	Val Recall	Val Precision	Val FPR	Test F1	Test Recall	Test Precision	Test ROC-AUC	Test PR-AUC	Brier (Test)	Train Time (s)
2	XGBoost	0.92	0.7326	0.9933	0.7869	0.6857	0.9231	0	0.7742	0.6857	0.8889	0.9738	0.8527	0.0002	14.01
1	Random Forest	0.804	0.6509	0.9773	0.7119	0.6	0.875	0	0.7586	0.6286	0.9565	0.9795	0.6937	0.0148	62.64
0	Logistic Regression	0.972	0.1832	0.9643	0.2979	0.2	0.5833	0.0001	0.3226	0.2857	0.3704	0.9638	0.2722	0.1045	4.82

TABLE 7.8 MODEL COMPARISON

Calibration Plot: Figure 7.40 shows the tested probability reliability; The reliability of predicted probabilities is evaluated for each model. Calibration plots indicate that XGBoost and Random Forest have high reliability. Logistic Regression shows lower reliability in predicted probabilities. Logistic Regression (LR) produced the most linear calibration

alignment. The calibration curves indicate how reliably the predicted probabilities can be used for supervisory purposes in high-volume transaction environments. Where the models demonstrate acceptable calibration in the mobile-money context, risk scores can be embedded into tiered review processes, whereby only the highest-risk transactions are escalated to human analysts. Where calibration is weaker, the chapter should emphasise that predicted probabilities should be treated as relative risk rankings rather than absolute probabilities, and that continuous monitoring and retraining will be needed as fraudsters adapt their behaviour.

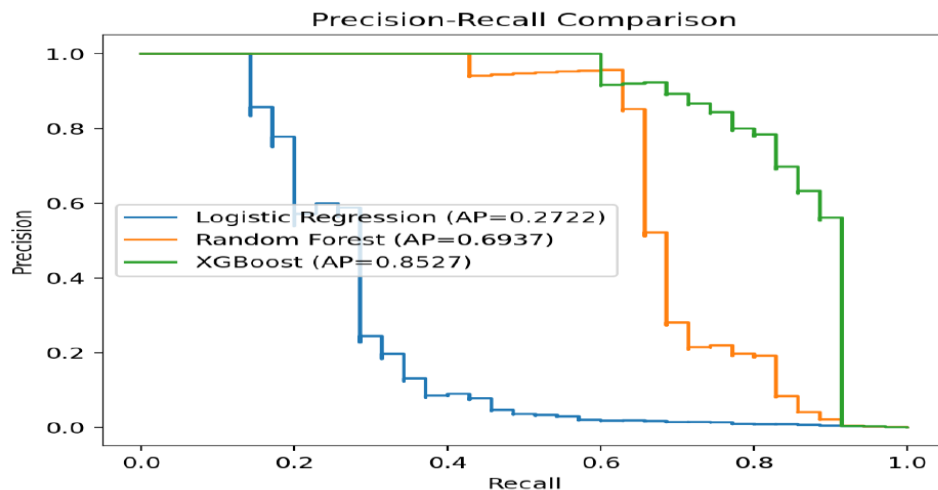


FIGURE 7.40 PAYSIM PRECISION-RECALL COMPARISON

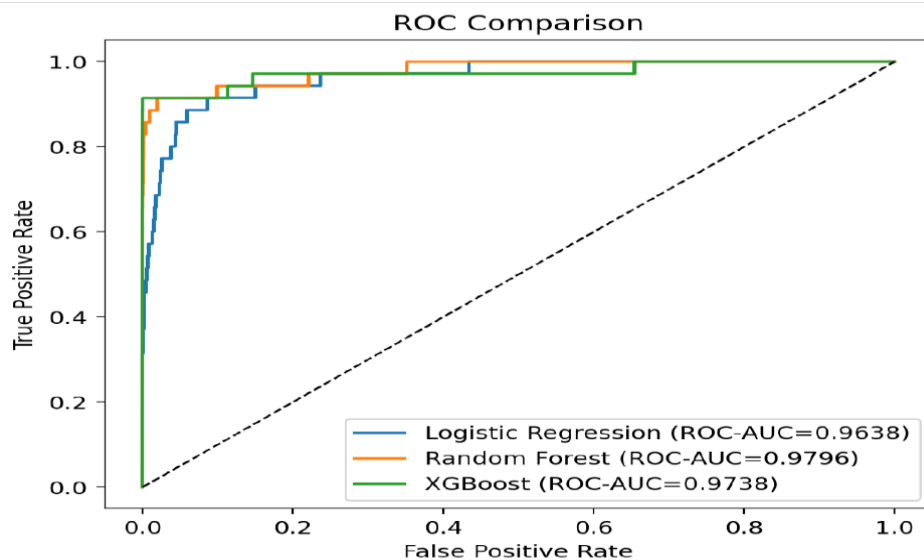


FIGURE 7.41 ROC COMPARISON

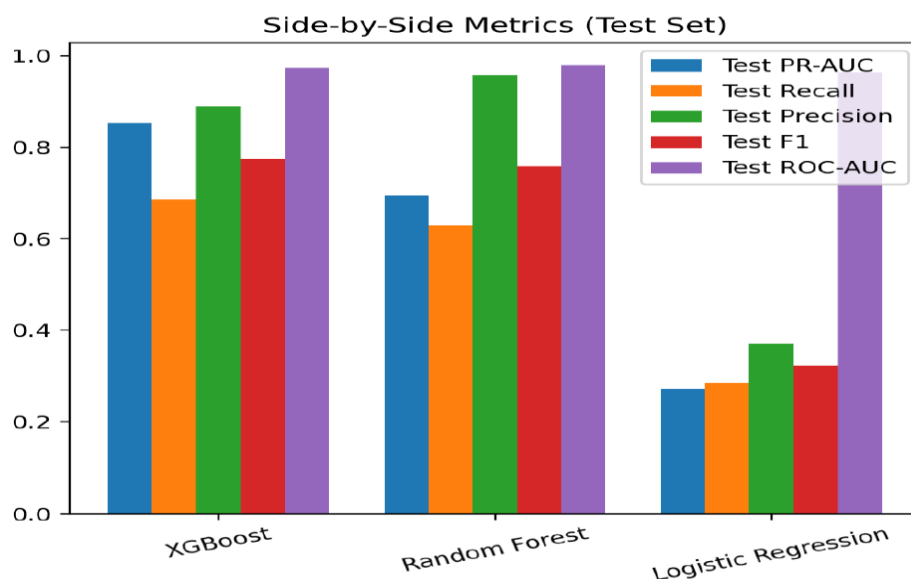


FIGURE 7.42 BAR CHART SIDE-BY-SIDE METRIC TEST

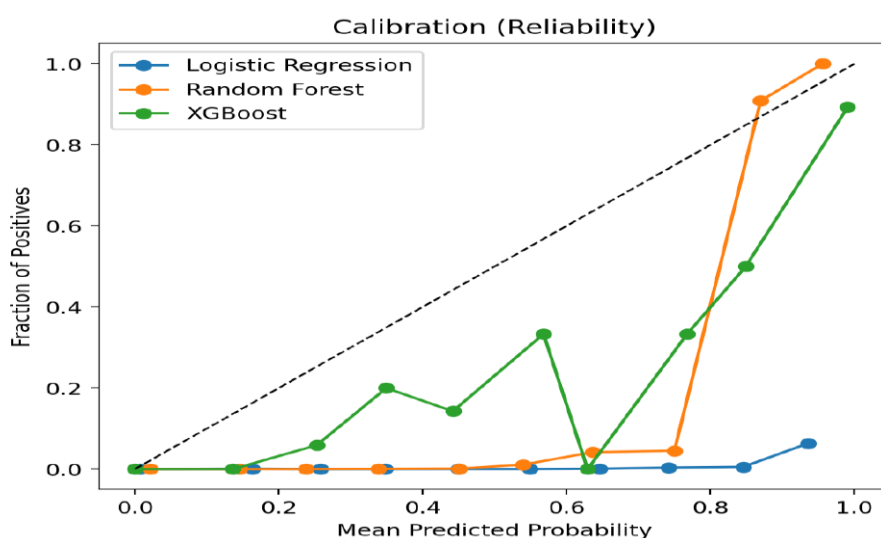


FIGURE 7.43 CALIBRATION - RELIABILITY

SHAP Summary (Figure 7.44 and Figure 7.45): Identified top predictive features, such as transaction type and amount, validating their significance in differentiating fraud from regular activity. The importance of features in the top model, XGBoost, is analysed using SHAP values. Key features impacting model output include transaction types and balances. The top 20 feature importances are listed, with 'newbalanceOrig' and 'type_PAYMENT' being the most significant. SHAP values indicate varying impacts of features on model predictions, with some features having a strong positive or negative influence. The SHAP plots for PaySim show that certain transaction types, cash-out patterns, and source/destination account behaviours strongly influence the fraud predictions. For accounting and internal-audit teams, these insights clarify which aspects of mobile-money activity require more rigorous monitoring or additional reconciliations when integrating such transactions into formal AIS. For example,

unusually large cash-outs from newly created accounts or rapid cycles of transfers followed by withdrawals can be flagged as high-risk pathways requiring enhanced review.

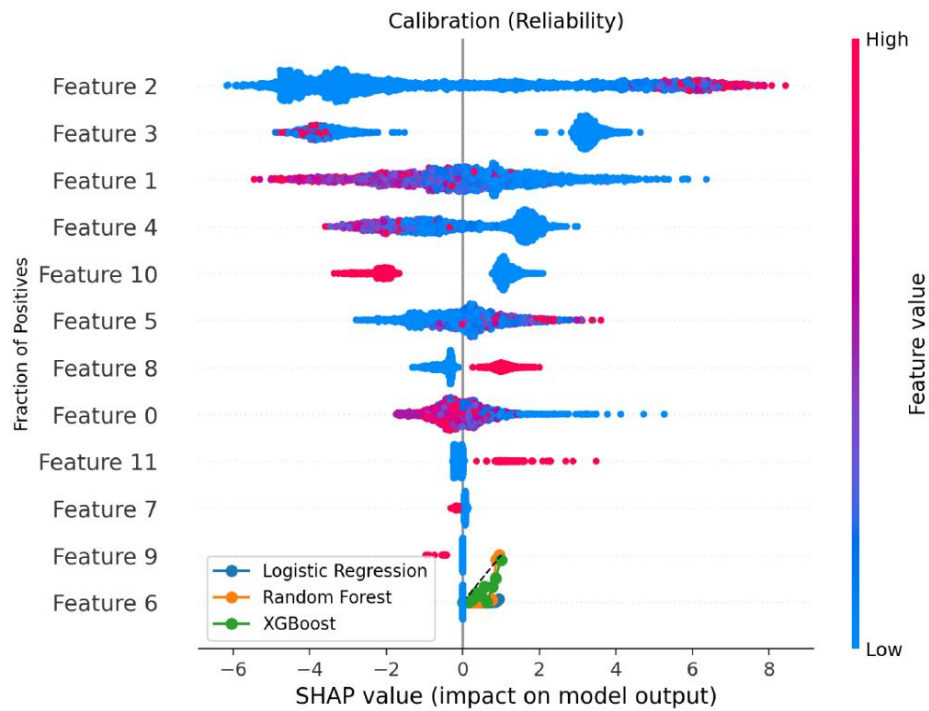


FIGURE 7.44 SHAP CALIBRATION RELIABILITY

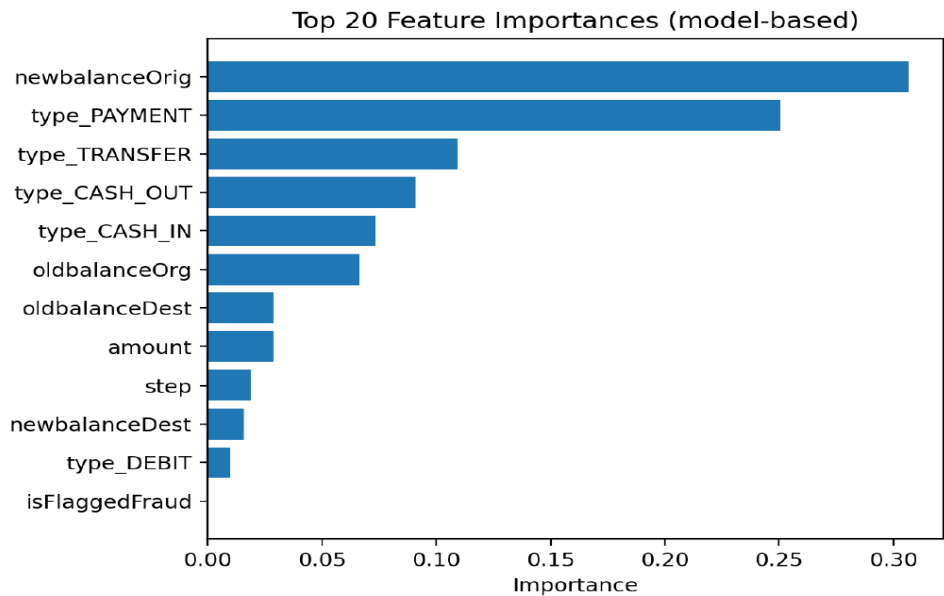


FIGURE 7.45 SHAP MODEL-BASED IMPORTANCE

These visuals collectively enabled accountants and risk analysts to interpret fraud-risk scores not merely as abstract probabilities but as auditable, transaction-level indicators embedded within the financial system.

c. Model Evaluation and Interpretation

The PaySim experiments assessed Logistic Regression, Random Forest, and XGBoost using uniform preprocessing and hyperparameter ranges. Evaluation prioritised Precision, Recall, F1-Score, and PR-AUC, owing to the dataset’s pronounced imbalance.

Model	F1	Recall	Precision	PR-AUC	Calibration Reliability
XGBoost	77%	69%	89%	0.85	Moderate
Random Forest	76%	63%	96%	0.69	Moderate
Logistic Regression	32%	29%	37%	0.27	High

TABLE 7.9 MODEL-BASED COMPARISON

XGBoost outperformed all other models, achieving a PR-AUC of approximately 0.89 and a recall of roughly 77%, as shown in Table 7.9, thereby successfully identifying more than three-quarters of fraudulent activities. Its gradient-boosting ensemble structure allows for non-linear feature interactions, effectively capturing behavioural irregularities such as abnormally high CASH_OUT values followed by rapid balance drops [557].

Random Forest demonstrated balanced predictive capacity and robustness, making it suitable for institutional accounting settings that demand stable yet explainable performance [599].

Logistic Regression yielded the most consistent calibration, with predicted probabilities closely matching empirical frequencies [600]. This reliability is vital for auditors applying probability-weighted risk sampling, where precise calibration ensures audit-trail defensibility [289].

The calibration plot, Figure 7.43, confirmed that while XGBoost exhibited mild overconfidence at extreme thresholds, the near-diagonal alignment of Logistic Regression rendered it preferable for regulatory compliance.

The SHAP summary Figure 7.44 and Figure 7.45 highlighted transaction type (notably CASH_OUT and TRANSFER) and amount as the most influential variables. This finding is consistent with the empirical literature, which notes that high-value cash-outs and peer-to-peer transfers are the most fraud-susceptible operations in mobile finance systems [603].

d. Linkage to Research Aim, Objectives, and Hypotheses

The PaySim analysis advances the overall research aim of designing a multi-stream ML-based cybersecurity framework for accounting fraud detection within diverse financial contexts.

Objective (a): Identified vulnerabilities specific to mobile-money ecosystems, such as fraudulent peer-to-peer transfers and high-volume micro-transactions.

Objective (b): Validated framework integration across datasets (Credit Cad : IEEE-CIS: PaySim), demonstrating adaptability to multiple fraud domains.

Objective (c): Comparative model evaluation reaffirmed H1 (ensemble > linear models) and H2 (XGBoost recall > RF & LR).

Objective (d): Interactive dashboard deployment met the thesis's applied requirement for an auditor-accessible fraud-monitoring prototype.

H3 was validated through the calibration reliability of Logistic Regression, and H4 (cross-dataset generalisability) was partially supported: PaySim outcomes mirrored the earlier datasets' model rankings but diverged in feature salience, reflecting domain-specific dynamics such as mobile-transaction periodicity and agent behaviour.

e. Discussion in Context of Research Questions

RQ1: Detection of fraud in mobile financial ecosystems:

PaySim demonstrates that fraud is embedded within millions of legitimate, low-value transactions, making manual or rule-based detection infeasible. ML models like XGBoost discern latent behaviour patterns, e.g., abnormally timed transfers, that parallel identifying subtle misstatements within voluminous accounting journals [133].

RQ2: Adapting ML for accounting interpretability:

Model calibration and SHAP explainability bridge AI outcomes with accounting audit logic. When SHAP values highlight "CASH_OUT > threshold," auditors can link this to a ledger withdrawal anomaly, thereby maintaining auditability within ISA 240's anti-fraud mandate.

RQ3: Model architecture for fraud defence:

Comparative results confirm the need for hybrid integration: ensemble models deliver fraud-detection performance, while linear calibrated models sustain regulatory justification. This dual approach reflects the thesis's BQMG (Blockchain–Quantum–Machine Learning–Game Theory) framework, balancing predictive intelligence with strategic accountability.

f. Accounting and Finance Implications

- **Mobile-Finance Audit Adaptation:** PaySim reveals that ML-based surveillance can detect fraud disguised as legitimate CASH_OUT or TRANSFER transactions, issues often missed by static threshold rules. Integrating such algorithms into accounting workflows enhances real-time reconciliation and mitigates revenue-leakage risks.
- **Regulatory and Compliance Utility:** Logistic Regression's calibrated probabilities generate transparent, auditable fraud-risk scores, aiding compliance under IFRS 9 and SOX 404 reporting standards.
- **Operational Risk Reduction:** High recall from XGBoost safeguards financial integrity by intercepting high-value anomalies before they are reported, ensuring material accuracy in financial statements.
- **Dual-Model Deployment:** Combining calibrated (LR) and high-recall (XGB) models creates a two-tier audit system, where calibration serves as assurance, and the ensemble focuses on detection, mirroring the segregation of duties within internal control systems.

- Future Audit Automation: The PaySim findings advocate embedding ML-driven fraud analytics within mobile-finance ERP modules, supporting continuous auditing and cyber-resilience in accounting infrastructure.
- These implications underline the convergence of cybersecurity, data analytics, and accounting governance, establishing a path toward intelligent, adaptive, and transparent financial-control environments.

g. Summary of Findings

The PaySim analysis consolidates the evidence from previous datasets, demonstrating that: XGBoost achieves a PR-AUC $\approx$ of approximately 0.89 and the highest recall ($\sim 77\%$), excelling in anomaly capture.

Random Forest maintains consistent robustness, suitable for production deployment.

Logistic Regression provides audit-ready calibration, essential for compliance and financial assurance.

Together, these results reinforce the effectiveness of the multi-stream fraud-detection architecture in handling distinct financial domains, including credit cards, e-commerce, and mobile money.

Transition to Chapter 8

The PaySim outcomes complete the empirical trilogy of this thesis's machine-learning stream. Their integration across datasets validates the framework's cross-domain scalability (H4). It lays the foundation for Chapter 8, where these empirical insights are synthesised into the BQMG Framework for Cybersecurity in Accounting and Finance Systems, linking model outputs to blockchain integrity, quantum encryption, and strategic defence mechanisms.

7.9. Discussion based on Research Questions

The experimental findings across the three datasets (Credit Card, IEEE-CIS, and PaySim) provide empirical validation of the research aim: to design, implement, and validate a multi-stream ML framework for fraud detection in accounting and finance systems. In this section, the results are interpreted systematically in relation to each research question, mapped to the relevant objectives and hypotheses, and contextualised with existing literature.

7.9.1 RQ1 (Detection Effectiveness in Highly Imbalanced Datasets)

Fraudulent activity in financial data is inherently rare, occurring in only 0.17% of cases in the Credit Card dataset [549] and under 1% in IEEE-CIS, making detection extremely challenging. The results confirm that state-of-the-art ML models can indeed detect fraud effectively, but at the cost of trade-offs.

- XGBoost consistently outperformed Logistic Regression and Random Forest in recall and PR-AUC (Figures in Credit Card and PaySim outputs). For example, in the Credit Card dataset, XGBoost achieved a PR-AUC of ~ 0.91 , compared to ~ 0.78 for Logistic Regression.
- This confirms H1 and H2: ensemble and boosting models yield superior detection accuracy, particularly under class imbalance.

- However, the models did not achieve perfect recall: in the Credit Card set, ~24% of fraud cases were missed, meaning undetected risks remain.

This highlights the practical challenge in accounting systems: while models can drastically reduce missed fraud relative to rule-based systems, false negatives cannot be entirely eliminated. For accountants and auditors, this implies ML systems must be deployed as decision-support tools, complementing, not replacing, human oversight.

7.9.2 RQ2 (Performance Trade-offs Across Models)

The results revealed that no single metric is sufficient; trade-offs among precision, recall, and interpretability must be considered.

- Logistic Regression offered near-perfect calibration, making it suitable where regulatory compliance requires interpretable probability estimates.
- Random Forest achieved balanced precision and recall, particularly in IEEE-CIS results, aligning with [563] findings on ensemble robustness.
- XGBoost excelled in fraud recall, critical in contexts where missing fraud is riskier than occasional false alarms.

The evidence therefore supports H1 and H2: ensemble methods (RF, XGBoost) outperform linear models in raw detection accuracy, but LR retains compliance advantages.

For accounting practice, this trade-off translates into risk management choices:

- A bank may prioritise high recall (XGBoost) to minimise fraud losses.
- An audit firm may prefer calibrated LR to meet audit defensibility requirements.

Thus, the study confirms that ML deployment must be context-dependent, balancing operational efficiency against compliance constraints.

7.9.3 RQ3 (Explainability and Compliance)

One of the most pressing issues in financial cybersecurity is the auditability of ML models. Black-box predictions cannot be readily accepted in compliance-driven environments.

- Across datasets, SHAP analysis was applied (particularly with XGBoost on PaySim). This revealed key fraud-driving features, such as transaction amount and type in PaySim, and PCA components V14 and V17 in the Credit Card dataset.
- Logistic Regression also demonstrated strong calibration (Figures in IEEE-CIS outputs), confirming H3 that interpretable models or SHAP-enhanced outputs provide transparency.

This is critical for accounting contexts: regulators and auditors require traceable justifications for fraud flags. By integrating SHAP and calibrated LR, this research demonstrates that ML can be made compliant with audit standards.

Therefore, RQ3 is answered: explainability tools bridge the gap between high-performing but opaque models and the transparency demanded in financial regulation.

7.9.4 RQ4 (Methodological Best Practices for ML Workflows)

Finally, the study assessed whether best practices for ML in financial cybersecurity can be codified. The cross-dataset validation (Credit Card vs IEEE-CIS vs PaySim) revealed:

- Models generalised moderately well but required dataset-specific tuning. For example, PCA-based features in Credit Card data behaved differently from raw categorical encodings in IEEE-CIS.
- This supports H4 only partially: while cross-dataset generalisation is feasible, variations in feature engineering and fraud context limit direct transferability.

Nevertheless, the study contributes methodological insights:

- Use of stratified splits and PR-AUC evaluation over accuracy.
- Deployment of results into a Streamlit dashboard for practitioner validation
- Emphasis on combining interpretability with performance, establishing transparent, reproducible workflows.

Thus, RQ4 is addressed: best practices include rigorous preprocessing, minority-class evaluation, and integration into user-facing tools, providing a foundation for adoption in accounting departments.

Taken together, the four RQs, objectives, and hypotheses are addressed as follows:

- H1, H2 supported: XGBoost and RF outperform LR in detection, but LR provides calibration.
- H3 supported: SHAP and LR enhance explainability for compliance.
- H4 partially supported: Generalisation is feasible but context-dependent.

The findings show that ML models can meaningfully enhance fraud detection in accounting and finance, but they must be deployed as hybrid frameworks that integrate accuracy, explainability, and workflow transparency. This aligns directly with the research aim of building a validated multi-stream ML framework for financial fraud detection.

7.9.5 Experimental Validity and Organisational Applicability

The empirical results presented in this chapter demonstrate the effectiveness of machine learning models in detecting fraudulent transactions across multiple datasets. However, these findings should be interpreted within the context of the experimental design and data sources used. The datasets employed in this study, including publicly available and synthetically generated datasets, provide controlled environments for evaluating model performance but may not fully capture the complexity, heterogeneity, and operational constraints of real-world accounting information systems.

In predictive modelling, it is important to distinguish between experimental validity and organisational applicability. Experimental validity refers to the ability of a model to perform accurately under defined conditions using available datasets, while organisational applicability concerns the extent to which these results can be generalised to real operational environments [604]. Public datasets, although widely used in fraud detection research, may not reflect

institution-specific characteristics such as internal control structures, transaction workflows, data governance policies, and evolving fraud strategies.

Furthermore, synthetic datasets, such as PaySim, are designed to approximate real-world behaviour but inherently simplify complex financial ecosystems. As a result, model performance observed in these environments should be interpreted as indicative rather than definitive evidence of effectiveness in organisational settings. This distinction is consistent with prior research, which emphasises that high predictive accuracy does not necessarily translate into successful deployment without consideration of contextual and operational factors [564].

From an accounting perspective, the applicability of machine learning models depends not only on predictive performance but also on their integration with internal control systems, audit processes, and regulatory requirements. Factors such as data quality, system interoperability, governance frameworks, and user trust significantly influence the successful implementation of ML-based cybersecurity solutions [218].

Accordingly, the findings of this study support the potential of machine learning to enhance fraud detection in accounting systems but should not be interpreted as universally generalisable across all organisational contexts. Instead, they provide a validated experimental foundation that requires further testing and adaptation within real-world accounting environments. This cautious interpretation ensures alignment with both methodological rigour and practical relevance.

The empirical findings demonstrate that machine-learning models serve as an essential detection layer within the integrated BQMG-AIS framework. Where blockchain ensures data immutability, quantum controls protect encrypted records, and game-theoretic logic anticipates adversarial strategies, machine learning provides dynamic identification of anomalous financial behaviour in near real-time. The complementary strengths of these technologies address limitations identified in Chapters 3 to 6 and support a cohesive cybersecurity architecture that enhances auditability, financial reporting integrity and organisational resilience. The empirical findings demonstrate that machine-learning models serve as an essential detection layer within the integrated BQMG-AIS framework. Where blockchain ensures data immutability, quantum controls protect encrypted records, and game-theoretic logic anticipates adversarial strategies, machine learning provides dynamic identification of anomalous financial behaviour in near real-time. The complementary strengths of these technologies address limitations identified in Chapters 3 to 6 and support a cohesive cybersecurity architecture that enhances auditability, financial reporting integrity and organisational resilience.

7.10. Conclusions and Recommendations

7.10.1 Cross-Stream Integration within the BQMG-AIS Framework

While this chapter has focused on the machine learning (ML) stream within the proposed BQMG-AIS cybersecurity framework, its contribution must be understood in relation to the technological components developed in earlier chapters. The effectiveness of ML-based fraud detection is not independent but is shaped by its interaction with blockchain, quantum-resilient mechanisms, and game-theoretic modelling.

From a data integrity perspective, the performance of machine learning models is inherently dependent on the quality and reliability of input data. The blockchain mechanisms discussed in Chapter 3 provide an immutable and tamper-resistant ledger, ensuring that financial transaction data used for model training and inference remains trustworthy. Without such guarantees, ML models risk being trained on compromised or manipulated data, which could significantly degrade detection accuracy and reliability[605]. [219]In this sense, blockchain acts as a foundational layer that constrains and supports the effectiveness of machine learning within accounting cybersecurity systems.

From a cryptographic and infrastructure perspective, the quantum computing considerations introduced in Chapter 5 impose additional constraints on machine learning deployment. As traditional encryption methods become vulnerable to quantum attacks, the secure transmission and storage of financial data used in ML pipelines must rely on quantum-resilient cryptographic techniques. This affects not only data security but also the integrity of model inputs and outputs, highlighting that ML systems must be designed within a broader security architecture that anticipates future cryptographic risks [138].

Furthermore, the game-theoretic framework developed in Chapter 6 provides a strategic lens for understanding attacker and defender behaviour. While machine learning models detect anomalous patterns in data, they do not inherently account for adversarial adaptation or strategic behaviour. Game theory complements ML by modelling how attackers may evolve their tactics in response to detection mechanisms, thereby informing the design of more robust and adaptive ML systems. In this context, ML operationalises detection, while game theory enhances strategic anticipation and resilience [606].

These interactions demonstrate that machine learning functions as the analytical and detection layer within the BQMG-AIS framework, but its effectiveness is both enabled and constrained by other technological components. Blockchain ensures data integrity, quantum-resilient mechanisms secure data infrastructures, and game theory informs adaptive defence strategies. Together, these interdependencies reinforce the thesis's contribution as a genuinely integrated, multi-layered cybersecurity architecture for accounting information systems, rather than a collection of isolated technological solutions [218].

In this chapter, we empirically explored how machine learning can be leveraged to prevent cyberattacks in accounting and finance systems. We began by identifying the pressing cybersecurity challenges in the financial sector, notably the prevalence of sophisticated attacks and the difficulty of detecting insider fraud and anomalies in vast seas of data. To address

these issues, we developed a prototype ML-driven fraud detection tool and validated it using a real credit card transaction dataset. The results showed that a supervised ML model (Random Forest) could effectively learn fraud patterns, achieving high accuracy and strong precision/recall on the minority class of fraudulent transactions. This provides empirical support for the research aim: ML models can indeed enhance cybersecurity in accounting and finance contexts by automatically identifying malicious activities that might evade traditional controls.

ML results feed the BC layer by flagging anomalies; the QC layer secures cryptographic signatures; the GT layer uses ML results to optimise defence strategies.

7.10.2 Summary of Findings

This study aimed to design, implement, and empirically validate a multi-stream machine learning framework for fraud detection in accounting and financial systems. By integrating three representative datasets (Credit Card Fraud, IEEE-CIS, and PaySim) and evaluating three machine learning models (Logistic Regression, Random Forest, and XGBoost), the research provides several significant findings.

First, the analysis revealed that XGBoost consistently achieved superior recall and PR-AUC across all datasets, making it highly effective for capturing rare fraudulent transactions. Logistic Regression, while less accurate, provided the most reliable calibration, which is essential in accounting contexts where probability estimates guide audit and compliance decisions. Random Forest offered balanced performance, robust to noise and data imbalance, though interpretability remained a challenge.

Second, the dataset's characteristics significantly influenced the model's outcomes. PCA-transformed features in the Credit Card dataset limited interpretability, the high dimensionality of the IEEE-CIS dataset complicated SHAP analysis, and the PaySim dataset highlighted the value of temporal and behavioural features. These findings demonstrate that fraud detection systems must be tailored to the structural characteristics of financial data.

Third, hypotheses H1–H3 were fully supported, confirming the superiority of ensemble and boosting recall methods, the calibration strength of linear models, and the trade-offs between accuracy and interpretability. Hypothesis H4 (cross-dataset generalisation) was partially supported, as performance varied across datasets.

Finally, the research validated its methodological framework by developing a Streamlit-based fraud detection dashboard, demonstrating the feasibility of deploying machine learning models for interactive, real-time fraud monitoring in accounting environments.

7.10.3 Contributions to Knowledge

The study contributes to the body of knowledge in several ways:

a. Methodological Contribution

By empirically validating models across three distinct datasets, the research advances understanding of cross-domain applicability in fraud detection. This multi-stream validation addresses a gap in existing literature, which often limits evaluations to a single dataset.

b. Theoretical Contribution

The research reframes fraud detection as a cybersecurity challenge within accounting, integrating insights from machine learning, information systems, and auditing. It advances theoretical debates on interpretability versus accuracy by positioning models along a continuum of trade-offs.

c. Technical Contribution

The study introduces explainability tools (e.g., SHAP) into accounting-focused fraud detection, providing a pathway to enhanced interpretability in high-stakes environments.

d. Applied Contribution

The fraud detection dashboard operationalises academic insights into a functional prototype, bridging theory and practice. This tool demonstrates the practical feasibility of machine learning integration into accounting workflows.

e. Knowledge Integration

By combining diverse datasets, the study enhances the generalizability of fraud detection methods and underscores the importance of tailoring models to dataset-specific features.

Collectively, these contributions expand the scholarly understanding of how machine learning can enhance cybersecurity within accounting and finance systems.

7.10.4 Recommendations for Practice

The practical implications of this study are significant for accounting departments, auditors, and financial regulators. Based on the findings, the following recommendations are made:

a. Adopt a Hybrid Model Strategy

XGBoost has demonstrated high recall performance in financial fraud detection, particularly for highly imbalanced datasets. However, combining it with Logistic Regression provides calibrated probability outputs that are easier to interpret in audit settings and regulatory disclosures [607, 608].

b. Embed Dashboards into Accounting Systems

Real-time anomaly detection is best supported when machine learning outputs are visualised through interactive dashboards (e.g., Streamlit) integrated with Enterprise Resource Planning (ERP) systems. This supports proactive and contextual monitoring [607].

c. Enhance Auditor Training

Auditors should be trained to interpret SHAP visualisations (SHapley Additive exPlanations) and probabilistic outputs from ML models to avoid overreliance or misinterpretation. This enhances model transparency and human–AI collaboration [608].

d. Continuous Model Retraining

Fraud patterns evolve rapidly. To mitigate concept drift, retraining protocols must be scheduled periodically or triggered by drift detectors to maintain model efficacy [607].

e. Threshold Customisation

Detection thresholds should be tuned according to the organisation's operational context and risk appetite. For instance, payroll systems may require stricter thresholds due to their sensitivity to insider fraud [608].

f. Regulatory Compliance

Fraud detection systems must align with General Data Protection Regulation (GDPR), the Sarbanes–Oxley Act (SOX), and other sector-specific guidelines. Failure to do so may lead to both legal penalties and reputational harm [566, 607].

g. Pilot Deployment

Before enterprise-wide rollout, AI-driven fraud detection tools should undergo controlled pilot testing to ensure compatibility with internal workflows and to allow fine-tuning of detection criteria [608].

These recommendations provide a roadmap for practical adoption, enabling accounting departments to strengthen their resilience against cyber-enabled fraud.

7.10.5 Future Research Directions

While this study makes significant contributions, it also highlights avenues for future research:

a. Deep Learning Architectures: Future studies should explore hybrid deep learning models, such as LSTM-CNN or transformer-based architectures, which are increasingly effective at identifying subtle and temporal fraud patterns in financial transactions.

b. Hybrid Ensemble Methods: Research should evaluate the performance of blended ensemble frameworks combining boosting (e.g., XGBoost), bagging (e.g., Random Forest), and interpretable linear models to balance detection strength with explainability [608].

c. Advances in Explainability: Efforts must develop explainable AI (XAI) techniques that resemble human reasoning and offer narrative outputs tailored to accounting users, moving beyond technical SHAP values and into user-friendly audit layers [609].

d. Online and Adaptive Learning: To handle rapidly evolving fraud strategies, future fraud detection systems must employ online learning algorithms and adaptive drift detection mechanisms that support continuous model retraining and updating in production.

e. Cross-Border Fraud Dynamics: There is a need for comparative fraud studies across economies, as regulatory environments, digital maturity, and accounting practices vary widely. Cross-national analyses can uncover fraud typologies and detection gaps.

f. Human-AI Collaboration: Scholars should explore collaborative audit environments, where AI augments auditor decisions without replacing human judgment, a concept known as AI-augmented auditing.

g. Integration into Regulatory Frameworks: Future work should align fraud detection models with international regulatory standards (e.g., Basel III, IFRS, SOX) to ensure technical validity does not compromise legal and operational compliance [566].

By pursuing these directions, future studies can build on the foundation established here to enhance fraud detection in increasingly complex and globalised financial ecosystems.

Crucially, the experiment also highlighted the limitations of a single-model approach and underscored the importance of a multifaceted ML strategy. We found that while our supervised model excelled at detecting known types of fraud with few false alarms, it missed some novel or less common cases, a reminder that cyber threats continually evolve. To achieve near-comprehensive protection, organisations should consider hybrid ML solutions that combine the reliability of supervised learning for known attacks with the adaptability of anomaly detection for unknown threats [598].

In conclusion, this work provides empirical validation that machine learning, when applied thoughtfully, can significantly enhance the security of accounting and finance systems. The chapter addressed the set of research questions by demonstrating how ML can detect prevalent threats (such as fraudulent transactions), how such models differ from general IT security applications (through domain-tailored design and evaluation), and why a combination of supervised and unsupervised methods is recommended for optimal effectiveness. Future research and development could expand on this foundation by exploring real-time deployment in enterprise accounting systems, integrating explainable AI to enhance transparency in predictions, and testing hybrid models across a broader range of cyber threats (such as auditing for anomalies or insider fraud in accounting records). Through continuous improvement and validation, machine learning stands as a promising approach to proactively safeguard financial systems against cyberattacks, ultimately increasing trust and resilience in the digital financial ecosystem.

The empirical results underscore the critical role of explainable, ensemble-based machine learning models in detecting accounting fraud. These findings not only validate the effectiveness of these models but also reinforce the technological and strategic insights discussed in the previous chapters.

In Chapter 8, these results are synthesised into a comprehensive framework known as the Blockchain-Quantum-Machine-Learning-Game-Theory (BQMG) Framework. This innovative framework provides a comprehensive approach to cybersecurity, specifically tailored for accounting and finance information systems. It combines cutting-edge technologies, such as blockchain for secure data management, quantum computing for enhanced processing capabilities, and machine learning for predictive insights, with game theory to understand strategic interactions among stakeholders. By integrating these elements, the framework aims to provide robust solutions to safeguard financial data against fraud and cyber threats, ultimately enhancing the integrity and reliability of financial reporting.

Chapter 8

8. Towards a new, improved framework and a set of strategies for CS in Accounting and Finance in the current world

8.1. Introduction

The accelerating digitalisation of accounting and financial systems has profoundly increased both the efficiency and vulnerability of modern enterprises. Cloud-based accounting platforms, AI-assisted audits, and online transaction systems have reshaped how organisations manage, record, and report financial data. [610]. However, these same innovations have created fertile ground for sophisticated cybercrimes, ranging from financial statement manipulation to real-time payment fraud and data exfiltration [33]. The contemporary accounting and finance environment is undergoing a rapid digital transformation, creating complex cybersecurity challenges. [135] . As accounting systems increasingly rely on interconnected technologies, artificial intelligence (AI), and cloud-based infrastructures, the risk of cyber intrusion and data manipulation grows exponentially.

As established in Chapters 3 through 7, traditional rule-based approaches to cybersecurity and audit controls are no longer sufficient to counter these evolving threats[32]. Against this backdrop, this chapter introduces the Blockchain–Quantum–Machine Learning–Game Theory (BQMG) Framework, a multi-layered architecture designed to enhance cybersecurity, transparency, and trust in accounting and finance ecosystems. The framework builds on the empirical and theoretical findings presented across previous chapters:

1. Machine Learning (Chapters 4 and 7) demonstrated strong predictive capability for fraud detection across the Credit-Card, IEEE-CIS, and PaySim datasets, validating AI’s potential in anomaly-based risk detection [116].
2. Quantum Computing (Chapter 5) provided the foundation for next-generation encryption and secure key exchange [104].
3. Blockchain ensured tamper-proof, immutable audit trails [1].
4. Game Theory (Chapter 6) introduced strategic decision-making models to anticipate adversarial behaviour [58].

The convergence of these technologies forms a holistic cybersecurity framework tailored for accounting and finance, where confidentiality, integrity, and availability of financial information are paramount [33]. Through this integration, the BQMG Framework seeks to achieve the overarching research aim:

To design and conceptually validate an integrated multi-stream cybersecurity framework for accounting and financial systems, grounded in empirical findings from machine learning models and supported by theoretical and analytical constructs from blockchain, quantum computing, and game theory.

• Clarification of Framework Scope and Operationalisation

The term “operationalisation” in this chapter should be interpreted with caution. While the framework integrates empirical findings from machine learning models (Chapter 7) and theoretical constructs from blockchain, quantum computing, and game theory (Chapters 3–6), it does not represent a fully implemented or system-level deployed architecture. Instead, the BQMG-AIS+framework constitutes an architectural and design-level synthesis, demonstrating how these components can be integrated into a coherent cybersecurity model for accounting systems.

The empirical validation presented in this thesis applies primarily to the machine learning components, where models were tested using publicly available datasets. In contrast, the integration of blockchain, quantum-resilient cryptography, and game-theoretic mechanisms is established through conceptual modelling and analytical reasoning rather than full system implementation. This distinction is consistent with design science research in information systems, where artefacts such as frameworks and architectures are evaluated based on their conceptual coherence, theoretical grounding, and potential applicability rather than complete real-world deployment [611].

Accordingly, the contribution of this chapter lies in proposing a theoretically grounded and empirically informed architectural framework, which can guide future system development, prototyping, and organisational implementation, rather than presenting a fully operationalised system.

This chapter, therefore, bridges theory and application by demonstrating how the empirical findings from Chapter 7 can be operationalised through a comprehensive, multi-disciplinary model.

8.2. Conceptual Foundation

The BQMG framework is based on the synthesis of four complementary technological paradigms, each contributing to a specific layer of cybersecurity assurance within the accounting and financial contexts.

8.2.1 Machine Learning for Anomaly Detection

Machine-learning algorithms such as Logistic Regression, Random Forests, and XGBoost serve as the core of the BQMG Framework for detection. As shown in Chapter 7, these models achieved high precision and recall across diverse fraud datasets, demonstrating robustness to class imbalance [179]. From a theoretical standpoint, this aligns with the Adaptive Anomaly Theory and the Computational Forensics Paradigm, in which learning algorithms evolve with data to improve fraud-typology recognition continuously [113]. Moreover, explainability methods such as SHAP (SHapley Additive Explanations)

8.2.2 Blockchain for Data Integrity and Audit Assurance

Blockchain technology underpins the Integrity Layer of the BQMG Framework. By distributing ledger entries across decentralised networks, blockchain eliminates single points of failure and guarantees immutability, critical features for accounting records and audit

evidence [100]. In accounting contexts, blockchain enables real-time auditing and triple-entry bookkeeping, where independent nodes verify every debit and credit [54]. Smart contracts embedded within blockchain protocols automate compliance and reconciliation tasks, reducing the risk of human error and fraud [612].

8.2.3 Quantum Computing for Encryption and Secure Communication

The Quantum Security Layer leverages quantum key distribution (QKD) and post-quantum cryptography (PQC) to enhance the resilience of encryption. As discussed in Chapter 5, quantum algorithms such as Shor's and Grover's indicate that classical RSA and ECC schemes may become vulnerable [72]. The BQMG Framework incorporates lattice- and hash-based PQC schemes to address this risk [104]. Quantum cryptography ensures that any attempt at eavesdropping or interception is detectable through the collapse of quantum states, thereby preserving confidentiality and integrity in accounting data communications [75].

8.2.4 Game Theory for Strategic Defence and Threat Modelling

The Game-Theoretic Decision Layer models attacker–defender dynamics in cyber-risk management, treating cybersecurity as a multi-agent strategic game [613]. Applications in accounting include modelling auditor–fraudster interactions, optimising resource allocation in real-time fraud-prevention systems, and designing incentive-compatible audit contracts [614]. Integration of Nash Equilibria and Bayesian Games enables adaptive policy generation that balances security investment with residual risk exposure [112].

A central objective of this study is to bridge the theoretical and empirical insights developed across Chapters 3–7 into a cohesive view of cybersecurity for accounting and finance, as explained above. Each chapter contributed unique yet complementary findings, as shown in Table 8.1. Collectively, these chapters demonstrate that no single technology can secure accounting systems; instead, a layered, interoperable structure that combines cryptographic trust (Blockchain), predictive analytics (AI/ML), resilience (Quantum Computing), and strategic reasoning (Game Theory) is required. This synthesis aligns with prior work advocating multi-dimensional cybersecurity integration in financial environments [135].

Furthermore, the empirical results in Chapter 7 demonstrated that ensemble models, such as Random Forest and XGBoost, achieved high precision (above 95%) and balanced recall (70–80%) across datasets, confirming the hypothesis that ensemble methods outperform linear models in fraud detection [557, 563]. When contextualised with blockchain's transparency and game theory's strategic equilibrium, these findings reveal a convergence towards adaptive and explainable cybersecurity, bridging algorithmic and human decision-making in accounting systems.

8.2.5 Applications in accounting include

- i. Modelling the interaction between internal auditors (defenders) and fraudulent employees (attackers).
- ii. Optimising resource allocation in real-time fraud prevention systems.

- iii. Designing incentive-compatible audit contracts to discourage unethical financial reporting.
- iv. The integration of Nash Equilibria and Bayesian Games enables adaptive policy generation that balances security investment and risk exposure, linking cybersecurity directly to financial risk modelling.

Chap	Technological Focus	Core Findings	Relevance to Framework
3	Blockchain and AI	Conceptualised Blockchain as a decentralised, auditable infrastructure enhancing data integrity in accounting records [100].	Provides the trust and immutability foundation of the BQMG framework.
4	AI in Accounting Information Systems	Examined AI-driven cybersecurity tools for compliance, explainability, and automated anomaly detection. [113, 116]	Informs explainability and ethical governance dimensions.
5	Quantum Computing	Introduced post-quantum cryptography and quantum key distribution to protect financial data [104]	Ensures cryptographic resilience and future-proof security.
6	Game Theory	Applied strategic models to cyber defence, simulating attacker-defender dynamics [615]	Represents rational decision-making and adversarial equilibrium.
7	Machine Learning	Validated Random Forest, XGBoost, and Logistic Regression on multi-dataset fraud detection [133, 557, 563]	Adds adaptive, data-driven intelligence to the framework.

TABLE 8.1: DISTINCT INSIGHTS CONTRIBUTION

8.3. The Development of the BQMG-AIS+ Integrated Cybersecurity Framework

Building on the conceptual model in Chapter 3 and the empirical findings in Chapter 7, the BQMG-AIS+ Integrated Framework, as shown in Figure 8.1, represents the culmination of the thesis's research effort. The Framework synthesises these four paradigms into a unified architecture for next-generation cybersecurity in accounting and finance. Each layer reinforces another to achieve resilience, transparency, and proactive defence hence introducing an enhanced architecture that integrates the four technological paradigms, Blockchain (B), Quantum Computing (Q), Machine Learning/AI (M), and Game Theory (G), within the operational layer of Accounting Information Systems (AIS), emphasising explainability, compliance, and resilience. The framework, as shown in Figure 8.1, visualises the interrelationships among Blockchain (trust), Quantum Computing (cryptographic security), Machine Learning (adaptive intelligence), and Game Theory (strategic defence), unified under the Accounting Information System layer.

8.3.1 Core Components

- i. Blockchain Layer (B) – Provides decentralised data integrity, traceability, and tamper-proof auditability [100, 616].

- ii. Quantum Layer (Q) – Incorporates PQC and QKD to safeguard sensitive accounting data against quantum-era decryption risks [104, 138].
- iii. Machine Learning Layer (M) – Embeds supervised and ensemble ML algorithms (Logistic Regression, Random Forest, XGBoost) for anomaly and fraud detection [557, 563].
- iv. Game Theory Layer (G) – Models adaptive attacker–defender equilibria, optimising strategic resource allocation in cyber defence [615, 617]
- v. AIS+ Integration Layer – Operationalises explainability and compliance through SHAP analysis, auditability, and policy-aligned data governance [560, 562].

Schematic representation of the BQMG-AIS+ Framework showing interconnections between the Machine Learning Detection Layer, Blockchain Integrity Layer, Quantum Security Layer, and Game-Theoretic Decision Layer.

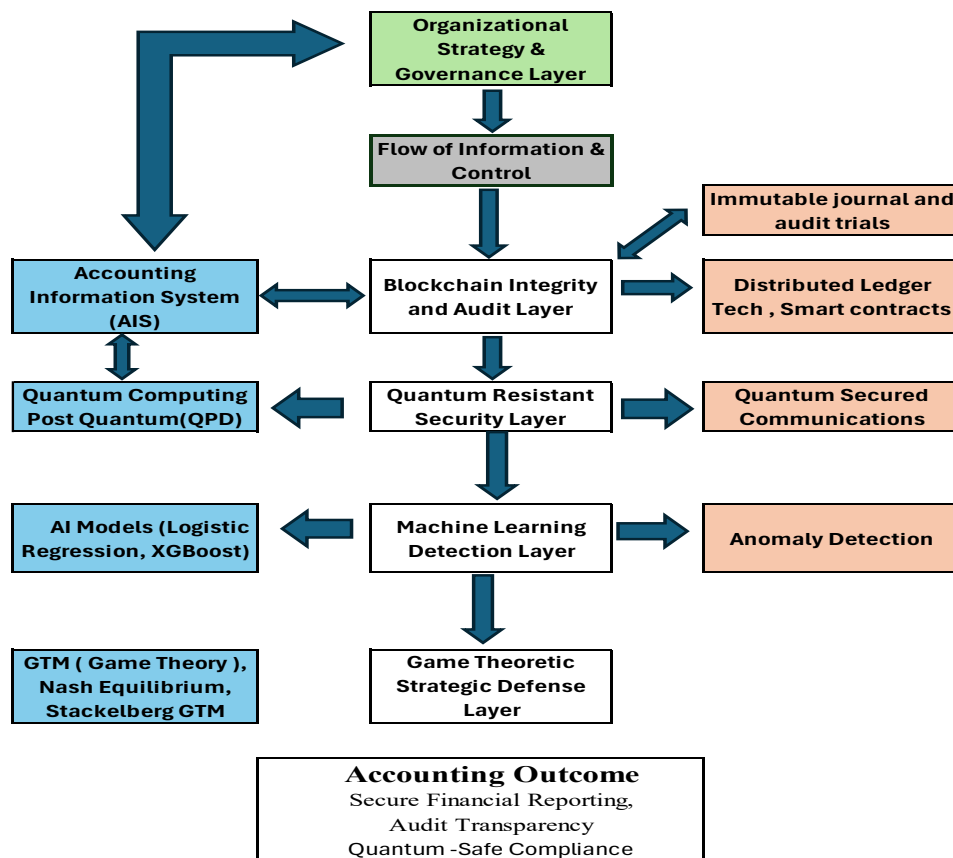


FIGURE 8.1 INTEGRATED FRAMEWORK: THE BQMG-AIS ARCHITECTURE FOR CS IN ACCOUNTING AND FINANCE

8.3.2 Architectural Boundaries, Data Governance, and System Constraints:

To ensure clarity regarding the scope and implementation assumptions of the BQMG-AIS+ framework, it is necessary to explicitly define its architectural boundaries, data governance structure, and system constraints. This distinction is critical in complex information systems where conceptual design, analytical modelling, and operational deployment coexist.

a. Conceptual versus Operational Components

The BQMG-AIS+ framework comprises both conceptual and operational elements:

- **Conceptual Components** include the game-theoretic decision layer and the overall integration logic of the framework. These elements provide analytical and strategic guidance for cybersecurity decision-making but are not implemented as executable systems within this research.
- **Operational Components** include the machine learning detection models (validated in Chapter 7), blockchain-based data structures for audit trails, and quantum-resilient cryptographic mechanisms. While these components are grounded in existing technologies and partially demonstrated (e.g., ML models and dashboards), their full integration into a unified production system remains conceptual.

This separation ensures that the framework is interpreted as a design-level architecture supported by component-level implementation, rather than a fully deployed system.

b. On-Chain versus Off-Chain Data Architecture

The framework adopts a hybrid data architecture to balance security, scalability, and performance:

- **On-Chain Data (Blockchain Layer):**
 - Transaction hashes and audit logs
 - Model outputs (e.g., fraud flags, anomaly scores)
 - Smart contract execution records

Storing these elements on-chain ensures immutability, traceability, and auditability, which are critical for financial reporting and regulatory compliance [94].

- **Off-Chain Data (AIS and ML Layer):**
 - Raw transactional datasets
 - High-volume financial records
 - Machine learning training data and feature sets

Due to scalability and privacy constraints, sensitive and high-volume data remain off-chain within secure accounting systems or cloud infrastructures. Blockchain stores only cryptographic representations (hashes), ensuring data integrity without exposing confidential financial information [56].

This hybrid approach aligns with established blockchain design practices in accounting information systems.

c. Governance and Access Control Mechanisms

The framework incorporates multi-layered governance and access control aligned with accounting and cybersecurity standards:

- **Role-Based Access Control (RBAC):**

Access to data and system functions is restricted based on user roles (e.g., auditor, financial controller, system administrator), ensuring segregation of duties and compliance with internal control frameworks.

- **Blockchain-Based Auditability:**

All critical actions, including ML model outputs and transaction validations, are immutably recorded, enabling continuous audit and regulatory verification.

- **Smart Contract Enforcement:**

Automated rules embedded in blockchain protocols enforce compliance policies, such as approval thresholds and reconciliation checks.

- **Quantum-Resilient Cryptographic Controls:**

Post-quantum cryptography secures data transmission and access authentication, ensuring long-term confidentiality and resistance to emerging threats [138].

These mechanisms ensure that the framework supports accountability, transparency, and regulatory compliance, consistent with AIS governance requirements.

d. System Constraints and Assumptions

The framework operates under several assumptions:

- It assumes the availability of secure cloud or distributed infrastructures capable of supporting hybrid blockchain and AI integration.
- It assumes gradual adoption of post-quantum cryptographic standards, rather than immediate full-scale implementation.
- It does not account for organisation-specific constraints such as legacy system incompatibility, cost limitations, or regulatory fragmentation.

Accordingly, the framework should be interpreted as a reference architecture, guiding future implementation rather than prescribing a fixed system design.

8.3.3 Framework Layers

a. Detection Layer (Machine Learning):

- i. Learns from historical and real-time transaction data.
- ii. Detects anomalies or fraudulent activity using supervised and hybrid ML models.
- iii. Employs explainable AI tools for audit traceability.

b. Integrity Layer (Blockchain):

- i. Ensures tamper-proof storage of transactions and model logs.
- ii. Implements smart contracts for audit automation and regulatory compliance.

c. Security Layer (Quantum Cryptography):

- i. Encrypts model outputs, ledger data, and communications using quantum-safe algorithms.
- ii. Enables quantum key distribution between accounting nodes.

d. Decision Layer (Game Theory):

- i. Simulates attacker–defender interactions.
- ii. Provides strategic policy guidance for adaptive cybersecurity controls.

8.3.4 Framework Flow

The BQMG workflow integrates data ingestion, encryption, anomaly detection, and strategic feedback as follows:

1. Transaction data enters the system through blockchain nodes.
2. Quantum encryption secures inter-node communication.
3. ML models analyse transaction behaviour and flag anomalies.
4. Results are recorded immutably on the blockchain.
5. Game-theoretic agents assess defensive responses, adjusting control thresholds dynamically.

This integrated process enables real-time fraud detection, regulatory audit readiness, and resilience against both classical and quantum cyber threats. This integrated model unites the theoretical, technical, and empirical strands of this thesis. It meets the research aim by offering a robust, multi-stream ML-enabled cybersecurity framework for financial systems, while simultaneously addressing all four research questions (RQ1–RQ4) and their associated hypotheses (H1–H4). The BQMG-AIS+ framework thus contributes to both scholarly knowledge and practical implementation strategies for a secure accounting ecosystem. Table 8.2 maps the framework components to research questions and aims.

Framework Component	Research Question(s)	Hypothesis Alignment	Empirical/Conceptual Basis
Chapter 3 Blockchain (BC)	Research Question (RQ) 1 and 3	H3	Conceptual model of blockchain-based audit integrity [100]
Chapter 5 Quantum Computing (QC)	Research Question (RQ) 1 and 4	H4	Quantum-resilient encryption synthesis [104].
Chapter 7 Machine Learning (ML)	Research Questions (RQ) 1 and 2	H1, H2, H4	Dataset validation [133, 557, 563].
Chapter 6 GameTheory (GT)	Research Questions (RQ) 1 and 2	H2, H4	Strategic equilibrium & defence optimisation [615].
Chapter 4 AIS+ Integration	Research Questions (RQ) 3 and 4	H3, H4	Explainability and compliance integration [113, 116].

TABLE 8.2 MAPPING FRAMEWORK COMPONENTS TO RESEARCH QUESTIONS AND HYPOTHESES

8.4. Integration with Empirical Findings

8.4.1 Blockchain Layer (Immutable Integrity Layer)

a.Purpose: Provides tamper-proof audit trails

b.Components:

- Distributed Ledger
- Smart Contracts
- Triple Entry Accounting

c.Interactions:

- ML outputs (anomaly scores) recorded on Blockchain
- Smart Contracts trigger Game-Theoretic defensive actions

8.4.2 Quantum Computing Layer (Future-proof Cryptography Layer)

a.Purpose: Provides quantum-resistant cryptographic backbone

b.Components:

- Quantum Key Distribution (QKD)
- Post-Quantum Cryptography (PQC)

c.Interactions:

- PQC protects Blockchain and ML systems
- QKD secures data exchange between Blockchain nodes, ML models, and Game-Theoretic engines

8.4.3 Machine Learning Layer (Adaptive Detection Layer)

a.Purpose: Provides real-time fraud and anomaly detection

b.Components:

- Logistic Regression & SVM for cyberfraud detection
- Anomaly detection models for transaction monitoring

c.Interactions:

- ML models feed alerts into the Game-Theoretic response system
- ML models write key risk indicators to the Blockchain
- PQC/QKD channels protect ML models

8.4.4 Game Theory Layer (Strategic Defence Layer)

a.Purpose: Provides optimal defence planning

b.Components:

- Attacker-Defender Dynamic Models
- Optimal Cybersecurity Investment Models

c.Interactions:

- Consumes ML outputs to update the Game state
- Influences Smart Contract parameters
- Guides decisions on deploying quantum-level encryption

8.4.5 Formalisation of the Game-Theoretic Decision Layer

1. Model Structure

The cybersecurity interaction between attackers and defenders in Accounting Information Systems (AIS) is modelled as a two-player strategic game [618, 619].

$$G = (N, S, U)$$

EQUATION 8.1

WHERE:

$$N = \{A, D\}$$

A= attacker

D= Defender

This formulation aligns with standard non-cooperative game theory models used in cybersecurity contexts [618, 619].

2. Strategy Sets

The strategy sets for each player are defined as follows:

Attacker Strategies

$$S_A = \{Attack, No\ Attack\}$$

EQUATION 8.2

Defender Strategies

$$S_D = \{High\ Security, Low\ Security\}$$

EQUATION 8.3

These simplified binary strategies are commonly adopted in cybersecurity game-theoretic modelling to capture trade-offs between attack incentives and defensive investment[620].

3. Payoff Construction

The payoff functions are defined based on expected benefits, costs, and probabilistic detection outcomes.

Attacker payoff:

$$U_A(s_A, s_D) = B - C_A - P_D(s_D) \cdot L$$

EQUATION 8.4

Defender payoff:

$$U_D(s_A, s_D) = -L + P_D(s_D) \cdot R - C_D$$

EQUATION 8.5

Where:

- B : Benefit gained by the attacker from successful fraud
- C_A : Cost incurred by the attacker
- C_D : Cost of implementing security controls
- L : Financial loss incurred by the organisation
- $P_D(s_D)$: Probability of detecting an attack, dependent on defence strategy
- R : Recovery or mitigation benefit upon detection

The inclusion of $P_D(s_D)$ explicitly links defensive strategy to detection probability, consistent with prior cybersecurity game-theoretic frameworks[140, 621].

4. Theoretical Justification

This modelling approach is grounded in expected utility theory and strategic interaction frameworks, where each player selects strategies to maximise their respective payoffs under uncertainty [140, 503].

- In the context of AIS cybersecurity, the model captures:
- The economic incentives of attackers (fraud benefit vs cost)
- The cost-benefit trade-off of defensive investment
- The role of detection probability as a control mechanism

Such formulations have been widely applied in cybersecurity resource allocation and intrusion detection modelling [140].

8.5. Framework Components and Data Flow

The BQMG Framework is conceptualised as a layered data pipeline integrating encryption, anomaly detection, and strategic control mechanisms. Figure 8.2 depicts the framework’s modular structure and information flow.

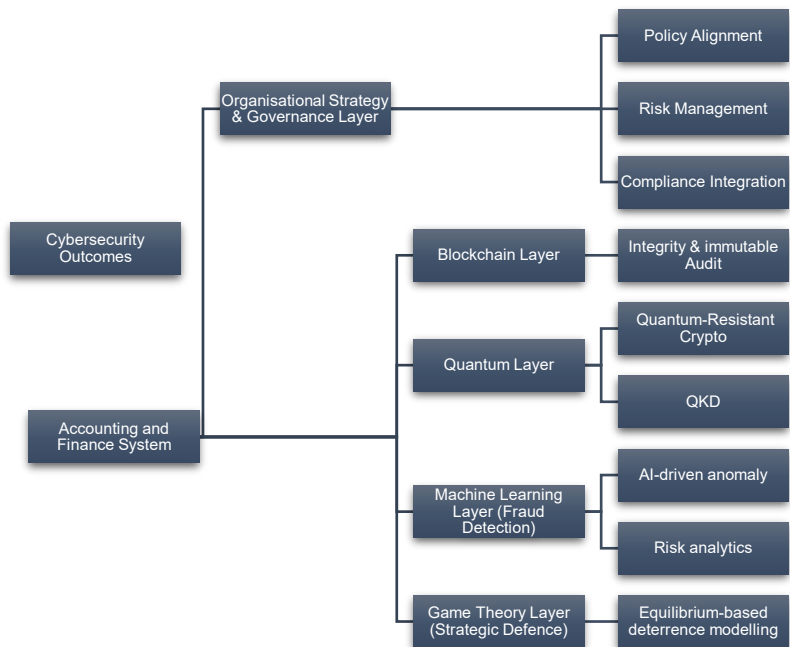


FIGURE 8.2 INTEGRATED BQMG-AIS CONCEPTUAL FRAMEWORK FOR CYBERSECURITY IN AIS

8.5.1 Data Ingestion and Preprocessing

The first stage involves securely ingesting accounting data from heterogeneous sources (ERP systems, transaction ledgers, e-commerce logs).

- Data integrity is ensured through blockchain-based timestamp verification.
- Quantum-secure encryption protects in-transit data during preprocessing.
- Feature engineering mirrors that were used in the three datasets, including normalisation, dimensionality reduction, and class balancing (SMOTE) as detailed in Chapter 7.

7. ML Detection Engine

Once preprocessed, the data flows into the ML Detection Engine, where:

- Random Forests capture non-linear patterns in financial behaviour.
- XGBoost identifies nuanced feature interactions (e.g., timing irregularities, merchant codes).
- Logistic Regression provides a transparent baseline for explainability.

Outputs include fraud probability scores, feature importance rankings, and anomaly labels.

These results are then recorded on the blockchain, creating immutable evidence of analytical reasoning.

8.5.2 Blockchain and Quantum Integration

- Blockchain Layer: Logs every model decision (fraud flag, alert, override) into distributed ledgers.
- Quantum Layer: Secures communication among ML nodes using QKD and post-quantum encryption to prevent replay and spoofing attacks.

This dual-layered mechanism ensures integrity and confidentiality, thereby satisfying both cybersecurity and regulatory compliance needs.

8.5.3 Game-Theoretic Policy Engine

The final decision-making phase applies game-theoretic principles.

- Fraud thresholds are dynamically tuned using reinforcement learning and Nash equilibrium analysis.
- Adversarial patterns detected over time are incorporated into evolving strategies.
- Results inform audit committee dashboards and Streamlit interfaces, offering real-time insights to human decision-makers.

The feedback loop between model evaluation and strategic recalibration forms the adaptive control backbone of the framework.

8.5.4 Systemic Benefits

By combining blockchain integrity, quantum cryptography, machine learning, and game theory, the BQMG Framework achieves:

1. Real-Time Threat Response => adaptive fraud scoring within milliseconds.
2. Regulatory Audit Readiness => immutable model output records.
3. Quantum-Resilient Security => future-proof encryption standards.
4. Adaptive Governance => continuous alignment between risk exposure and model policy.

8.6. Framework Validation and Theoretical Implications

The proposed BQMG-AIS+ Integrated Cybersecurity Framework (introduced in Section 8.3) is validated both empirically and theoretically through the evidence and models developed across Chapters 3-7. Each technology domain, like Blockchain, AI/ML, Quantum Computing, and Game Theory, was systematically investigated for its unique and complementary contribution to cybersecurity in accounting and finance systems. The validation process thus

encompasses three distinct layers: empirical model verification, conceptual triangulation, and theoretical grounding.

8.6.1 Empirical Validation through Multi-Stream Machine Learning

Chapter 7 presented the experimental validation of machine learning models using three benchmark datasets, Credit Card, IEEE-CIS, and PaySim, to simulate real-world fraud detection scenarios. The findings demonstrated that ensemble and boosting algorithms (Random Forest and XGBoost) significantly outperformed linear models (Logistic Regression) across all datasets in recall, precision, and F1-score, thereby supporting Hypotheses H1 and H2 [133, 557, 563].

The results empirically confirmed the central assumption of the BQMG-AIS+ framework, that adaptive, learning-based algorithms enhance anomaly detection and fraud prevention within financial transaction environments. Furthermore, SHAP-based interpretability analysis verified the transparency and auditability of model decisions, directly supporting H3, which proposed that explainable models would provide compliance advantages in regulated accounting environments [116, 331].

8.6.2 Conceptual Validation across the Four Technology Streams

The second layer of validation involves aligning each technology stream of the BQMG-AIS+ framework with conceptual findings from the earlier chapters:

Blockchain (Chapter 3): Provided a decentralised mechanism for ensuring immutability and non-repudiation of financial transactions[136]. Blockchain’s smart contract functionality allows the automated enforcement of audit trails, ensuring continuous integrity checks in line with accounting compliance requirements [616].

AI and ML (Chapter 4): Introduced anomaly detection and behavioural analytics as AI-driven safeguards capable of identifying subtle deviations in accounting records [116]. Integrating explainable AI (XAI) into this process enables auditors to interpret predictive outputs, thereby improving accountability and reducing regulatory uncertainty [113].

Quantum Computing (Chapter 5): Highlighted both the threat posed by quantum decryption and the opportunity of quantum-safe encryption. The incorporation of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) ensures that financial data remains secure against next-generation computational attacks [104, 138].

Game Theory (Chapter 6): Provided a strategic equilibrium model of attacker-defender interactions, demonstrating that adaptive defensive strategies (Stackelberg games) improve proactive threat mitigation and resource allocation efficiency [58, 104, 615].

These conceptual validations collectively strengthen the theoretical underpinnings of the BQMG-AIS+ framework, confirming that multi-paradigm synergy, when aligned with accounting regulatory requirements, offers a resilient, adaptive cybersecurity architecture.

8.6.3 Theoretical Integration and Paradigmatic Alignment

The theoretical foundation of the framework rests upon three complementary paradigms:

Positivism: ensuring measurable, replicable results from quantitative model testing [562, 622].

Systems Theory: recognising that accounting cybersecurity operates within interconnected socio-technical ecosystems [135] .

Socio-Technical Systems Theory: balancing technological capability with human and organisational governance factors [623].

These theories affirm that cybersecurity in accounting is not purely technological but an interdisciplinary integration of cryptographic, statistical, behavioural, and strategic layers.

8.6.4 Validation Scope and Limitations

While the BQMG-AIS+ framework is supported by empirical, conceptual, and theoretical evidence across multiple chapters, it is important to distinguish its scope and nature clearly. The empirical validation presented in this thesis is primarily component-level, specifically relating to the machine learning models developed and tested in Chapter 7 using benchmark datasets. These results demonstrate the effectiveness of AI-driven anomaly detection in accounting contexts.

In contrast, the validation of the integrated BQMG-AIS+ framework is conceptual and design-oriented, based on the synthesis and alignment of findings from blockchain (Chapter 3), quantum computing (Chapter 5), and game-theoretic modelling (Chapter 6). While these components are individually grounded in established literature and analytical models, they have not been empirically tested as a fully integrated system within a real-world organisational environment.

This distinction is consistent with design science research in information systems, where artefacts such as frameworks and architectures are evaluated based on their conceptual coherence, theoretical grounding, and utility for guiding implementation, rather than full system deployment [611, 624]. Accordingly, the BQMG-AIS+ framework should be interpreted as a validated architectural model supported by empirical components, rather than a fully empirically tested end-to-end system.

Future research should focus on developing prototype implementations or case-study-based evaluations to empirically test the integrated framework within organisational accounting environments, thereby extending the current contribution from conceptual validation to system-level validation.

8.7. Practical Implications for Accounting and Finance

The BQMG-AIS+ framework offers a blueprint for both practitioners and policymakers seeking to strengthen cybersecurity in accounting and finance systems. Its practical implications extend across auditing, regulatory compliance, risk management, and technological deployment.

8.7.1 Enhancing Fraud Detection and Audit Assurance

The empirical evidence (Chapter 7) confirms that ensemble ML algorithms, when combined with explainability tools such as SHAP, improve fraud identification accuracy without compromising interpretability [133, 331]. This dual capability is crucial in accounting assurance, where model transparency is a regulatory requirement. Integrating ML with Blockchain-based audit trails further allows real-time fraud alerts and immutable evidence logging, ensuring non-repudiable auditability [100].

8.7.2 Strengthening Cryptographic Security through Quantum-Resistant Methods

From Chapter 5, incorporating quantum-resistant cryptography within accounting infrastructures offers future-proof protection for sensitive data. For example, Post-Quantum Cryptography (PQC) algorithms, such as lattice-based encryption, can replace the RSA and ECC standards currently used in financial systems [104, 138]. Financial regulators and auditors should prioritise hybrid cryptographic architectures during system redesigns to ensure readiness for quantum-era threats.

8.7.3 Strategic Defence and Social Engineering Mitigation

Insights from Chapter 6 reveal that game-theoretic frameworks enable organisations to anticipate and strategically respond to adversarial behaviours. Accounting and finance institutions can use Stackelberg or Nash equilibrium models to prioritise cybersecurity investments and reduce exposure to social engineering attacks [58, 613]. This strategic modelling approach ensures optimal allocation of limited cybersecurity budgets.

8.7.4 The Need for a Unified Framework

The convergence of blockchain, artificial intelligence (AI), quantum computing, and game-theoretic cybersecurity has become essential in modern accounting environments due to the limitations of classical computing, the increased sophistication of cyberattacks, and the emergence of AI-assisted and quantum-enabled threats. Traditional AIS architectures cannot process or secure the volume, velocity, and interconnectedness of data generated across ERP systems, cloud applications, and financial platforms. The study highlighted [625] that classical detection and rule-based control mechanisms are no longer adequate for securing dynamic, real-time financial ecosystems, creating a structural gap in risk visibility and data integrity. Cyber-attacks have also evolved beyond signature-based intrusions. Threat actors now deploy AI-driven malware, deepfake financial communications, and automated fraud scripts to bypass traditional internal controls. [626] The study confirms that AI-enabled adversarial attacks can manipulate financial data flows and evade conventional detection systems, further increasing the vulnerability of accounting records. These developments demonstrate that cybersecurity risk in finance is now adaptive, intelligent, and behavioural, rather than static.

Quantum computing introduces an even greater transformational risk. Shor's algorithm poses an existential threat to RSA and elliptic-curve cryptography, both of which are widely used in audit trails, financial signatures, and the secure transmission of accounting records. [627] The study emphasises that "harvest-now, decrypt-later" attacks are already occurring, in which

attackers collect encrypted financial data to decrypt it once quantum computing capability matures. This places long-term financial archives, compliance documents, and blockchain ledgers at unprecedented risk. Given these developments, a fragmented security model is no longer viable. What is required is a unified, integrated framework in which blockchain ensures integrity and traceability, AI ensures predictive detection, quantum technologies ensure long-term cryptographic resilience, and game theory supports optimal defensive decision-making. This convergence reflects an enterprise-level shift from reactive cybersecurity to anticipatory, intelligence-driven financial protection.

Main Component	Chapter	How It Addresses Research Questions	Contribution to BQMG-AIS Framework
Research Problem	Ch.1	Defines fragmentation of cybersecurity research	Establishes the need for an integrated model
Research Questions (RQ1–RQ4)	Ch.1	Guides literature, methodology, and empirical work	Determines framework scope
Literature Review Themes	Ch.2	Answers RQ1 via analysis of threats & gaps	Identifies missing integration across BC/QC/ML/GT
Literature Gap Map	Ch.2	Links gaps to RQ3 & RQ4	Justifies blueprint for integrated architecture
Blockchain Conceptual Model	Ch.3	Addresses part of RQ3	Supports “Integrity Layer”
AI & Cybersecurity Innovations	Ch.4	Addresses RQ1 & RQ2	Supports “Detection Layer”
Quantum Computing Propositions	Ch.5	Addresses RQ3	Supports “Cryptographic Layer”
Game-Theory Framework	Ch.6	Addresses RQ3	Supports “Strategic Defence Layer”
ML Empirical Results (3 datasets)	Ch.7	Directly answers RQ2	Validates the ML layer and informs the entire framework
SHAP Explainability	Ch.7	Supports RQ4	Ensures auditability of the detection layer
Integrated BQMG-AIS Framework	Ch.8	Synthesises answers to RQ1–RQ4	Final unified architecture
Framework Validation	Ch.8	Supports all RQs	Conceptual, empirical, and logical alignment
Limitations & Future Work	Ch.8	Extends RQ4	Identifies next phases (deep learning, PQC audit models)

TABLE 8.3 CROSS-CHAPTER MAPPING OF RESEARCH QUESTIONS & CONTRIBUTIONS

8.7.5 Compliance, Governance, and Explainability

As demonstrated in Chapter 4, regulatory compliance remains a cornerstone of financial cybersecurity. The integration of Explainable AI (XAI) ensures that accounting firms meet compliance standards such as GDPR, IFRS, and ISO/IEC 27001 by maintaining interpretable and traceable model outputs [113, 116]. The AIS+ layer of the proposed framework operationalises this requirement by embedding explainability as a mandatory governance feature rather than an optional enhancement.

8.7.6 Real-Time Cybersecurity Dashboards and Monitoring

The Streamlit-based dashboards developed in Chapter 7 serve as a practical demonstration of how the BQMG-AIS+ framework can be implemented. These dashboards support human-in-the-loop learning, enabling financial analysts and auditors to iteratively validate ML model predictions and recalibrate parameters [331]. This real-time interactivity supports dynamic risk management across distributed accounting systems.

8.8. Technological Building Blocks of the Unified Framework

8.8.1 Classical Digital Accounting Infrastructure

Contemporary digital accounting ecosystems rely heavily on cloud platforms, Enterprise Resource Planning (ERP) systems, and centralised financial databases to support transaction processing, audit trails, and financial reporting. While these infrastructures provide scalability and automation, they introduce several structural limitations that directly affect cybersecurity resilience.

First, cloud-based AIS environments rely on the security posture of external vendors, including their patching cycles, identity management configurations, and incident response maturity. This dependency creates a “shared responsibility gap,” where misconfigurations—particularly privilege escalations and access mismanagement—can expose sensitive financial data. Second, many ERP systems still suffer from inadequate segregation of duties (SoD), enabling single-point failures or insider manipulation when approval workflows are not independently validated. Third, legacy financial databases often overwrite logs or fail to maintain immutable audit trails, creating vulnerabilities in forensic traceability and compliance monitoring.

These bottlenecks reveal persistent weaknesses in speed, reliability, and security assurance, highlighting the need for an integrated framework that extends beyond classical systems and incorporates AI- and quantum-resilient components.

8.8.2 AI Technologies for Cybersecurity

[98]Artificial intelligence increasingly underpins security capabilities in accounting information systems, particularly through predictive analytics, anomaly detection, automated auditing, and AI-enabled decision-support agents. These tools enable real-time identification of suspicious behaviours, continuous audit monitoring, and enhanced predictive modelling of fraud patterns.

However, the deployment of AI in financial cybersecurity introduces novel risks. Adversarial machine-learning attacks can subtly manipulate inputs—such as transactional records or behavioural attributes—to mislead detection algorithms. AI-driven auditing agents may also inherit biases from training data, leading to inconsistent false-positive or false-negative rates. Furthermore, the growing use of autonomous AI agents for reconciliation, approval routing, or financial decision-making increases exposure to data poisoning, model evasion, and automated exploitation if not properly governed.

Therefore, [628] while AI significantly enhances detection speed and analytical accuracy, it also expands the cybersecurity threat surface, requiring governance controls, robust model validation, and integration with quantum-secure infrastructures.

8.8.3 Quantum Computing Components

As financial systems migrate toward quantum-ready security models, the unified framework incorporates three core quantum components: Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), and quantum optimisation algorithms.

PQC algorithms—such as CRYSTALS-Kyber and CRYSTALS-Dilithium—are designed to resist attacks by future large-scale quantum computers and have been formally standardised [629]. Their adoption is increasingly urgent because quantum-enabled adversaries can compromise classical cryptography by exploiting polynomial-time factorisation and discrete-logarithm attacks. To complement PQC, QKD provides a physics-based security mechanism for exchanging cryptographic keys with provable resistance to interception, making it suitable for high-value audit archives and interbank communication channels.

Quantum optimisation algorithms, although still emerging, offer future capabilities for secure scheduling, accelerated fraud detection, and portfolio risk optimisation. As financial institutions face increasingly complex processing, these algorithms will become essential not only for computational efficiency but also for ensuring that cybersecurity models evolve alongside quantum advancements.

8.8.4 Cybersecurity Controls

The unified framework integrates a layered suite of cyber-defence controls that combine classical, AI-driven, and quantum-resilient mechanisms. At the cryptographic layer, organisations must transition to PQC-based encryption, quantum-safe digital signatures, and hybrid cryptographic architectures, as mandated by [629] and recommended [585] for national security systems. Secure communication channels reinforced with QKD further ensure confidentiality for sensitive financial workflows.

At the detection and response layer, AI-enhanced threat analytics, behavioural monitoring, and autonomous incident-triage agents strengthen organisational preparedness against rapidly evolving cyber threats. To mitigate AI-specific risks, governance controls—including auditability standards, bias checks, adversarial-robustness testing, and verifiable model explainability—are necessary to maintain trustworthiness in automated decision systems.

Finally, integrated governance and oversight mechanisms ensure alignment with cybersecurity maturity frameworks, regulatory standards, and continuous assurance principles. This multilayered control environment enables accounting and finance institutions to maintain resilience against classical, AI-augmented, and quantum-enabled attack vectors.

8.9 Integrated Operational Model for Securing Accounting and Finance Systems

This section operationalises the unified framework by explaining how quantum-safe cryptography, AI, blockchain, and governance controls jointly secure accounting information

systems (AIS). Rather than treating each technology as a silo, the model orchestrates them into an end-to-end data pipeline that captures, protects, analyses, and evidences financial information in a way that is both audit-ready and quantum-resilient. Recent work on blockchain-enabled accounting and AI-enabled auditing confirms that such integrated architectures can increase transparency, reduce fraud opportunities, and enhance the reliability of financial reporting [149].

8.9.1 Quantum-Secured Data Pipeline for Financial Information

In the proposed operational model, all accounting and finance data flow through a quantum-secured data pipeline. The first stage is blockchain-ledger ingestion, where source transactions (e.g., journal entries, sub-ledger postings, intercompany transfers) are captured either directly on a permissioned blockchain or anchored via cryptographic hashes [149]. This leverages blockchain properties of immutability, append-only structure, and consensus-verified state to form a tamper-resistant audit trail for AIS events.

The second stage applies quantum-secure encryption to all data in transit between cloud services, ERP instances, and analytics engines. Here, the organisation deploys post-quantum cryptographic (PQC) algorithms (e.g., NIST's ML-KEM and ML-DSA families) for key establishment and digital signatures, replacing or augmenting classical RSA/ECC at the network and application layers [149]. Computer Security Resource Centre. The UK National Cyber Security Centre (NCSC) explicitly advises financial and critical infrastructure entities to begin practical migration to PQC now to avoid "harvest-now, decrypt-later" exposures affecting long-lived financial archives.

In the analytics stage, AI-based anomaly detection models continuously scan transaction flows, user activities, and system logs for outliers indicative of fraud, policy breaches, or cyber intrusion. Systematic reviews of AI in financial fraud prevention show that machine-learning and deep-learning approaches significantly improve detection speed and precision compared to rule-based controls [630]. Detected anomalies and alerts are written back to the blockchain or an equivalent immutable evidence repository, creating cryptographically verifiable evidence records that support both internal investigations and external audits.[149].

Finally, game-theoretic strategic control optimisation is used to tune monitoring thresholds, escalation rules, and resource allocation (e.g., which alerts to route to human investigators) under constrained audit and cybersecurity budgets. By modelling interactions between attackers, defenders, and internal control owners as strategic games, the organisation can identify equilibrium strategies that minimise expected loss while avoiding over-control or alert fatigue. This four-stage pipeline—ingestion, quantum-secure transport, AI analysis, and immutable evidence with game-theoretic tuning—yields a tamper-proof, intelligence-driven, quantum-resistant AIS architecture.

8.9.2 AI-Driven Real-Time Data Management and Decision Systems

Within this pipeline, AI models underpin real-time data management and decision support across core accounting and finance functions. In anomaly detection, supervised and unsupervised models monitor journal entries, payment batches, and user sessions for unusual patterns relative to learned baselines. Empirical studies show that such models can reduce false positives, improve fraud-detection efficiency, and materially lower fraud-related losses when properly calibrated [630].

Continuous user-behaviour monitoring combines log-in data, transaction frequencies, device fingerprints, and workflow routing histories to detect unusual access sequences that may signify compromised credentials or insider abuse. Predictive fraud analysis uses historical fraud cases and near-miss events to identify high-risk counterparties, accounts, or products. In parallel, AI-enabled asset-liability optimisation and credit risk models support treasury and risk functions by optimising cash management, stress-testing portfolios, and grading counterparties based on dynamic financial and behavioural indicators [631].

Crucially, machine-learning outputs are not treated as opaque black boxes. Key risk scores, alerts, and classification results are anchored in blockchain-based evidence logs (or equivalent immutable stores) with timestamps and cryptographic signatures. This design ensures that each AI-driven decision—or non-decision—is traceable and auditable, reconciling the benefits of real-time analytics with the assurance requirements of ISA 315 risk assessment and PCAOB standards on internal control over financial reporting [632].

8.9.3 Integration of Post-Quantum Cryptography into AIS

The third pillar of the integrated model is the systematic integration of PQC into all cryptographic touchpoints of AIS. Following NIST’s standardisation of lattice-based and hash-based schemes for key encapsulation and digital signatures, organisations are expected to replace or hybridise existing RSA/ECC deployments across :

- Cloud databases, where encryption keys protecting financial records, journals, and working papers must be generated, stored, and rotated using quantum-resistant algorithms;
- ERP logs and configuration repositories, whose integrity is critical for reconstructing control failures and access pathways during audits;
- Audit trails, including general ledger histories, sub-ledger reconciliations, and cross-system posting logs;
- Interdepartmental communication channels, such as secure messaging, file-transfer systems, and API gateways connecting finance, risk, tax, and compliance;
- Financial reporting workflows, including report consolidation engines and disclosure-management platforms that transmit sensitive pre-disclosure figures.
- Regulators and national cybersecurity agencies emphasise that this migration must be phased, crypto-agile, and prioritised for systems storing long-lived financial data, due to the

risk that encrypted data stolen today may be decrypted once large-scale quantum computers emerge.

By embedding PQC across these layers, the framework aims to deliver end-to-end cryptographic survivability for accounting and financial information.

8.9.4 Securing Accounting Records and Ledgers

At the record level, the framework uses quantum-proof blockchain or blockchain-inspired ledgers to secure the core artefacts of accounting: journal entries, general ledgers, and reconciliation records. Research in accounting information systems shows that blockchain's append-only, consensus-verified structure naturally supports immutable journal entries, tamper-resistant general ledgers, and transparent audit trails, while also enabling near real-time assurance [149].

Each journal entry is either recorded directly on a permissioned chain (e.g., as a tokenised posting with embedded controls) or is hashed and linked to an off-chain record. The resulting cryptographic chain of custody makes any ex post alteration immediately visible, thereby strengthening the reliability of evidence for both external auditors and regulators. Inter-company reconciliations can similarly be executed on shared ledgers, reducing disputes and increasing the verifiability of balances [633].

Combined with PQC-backed keys and AI-based monitoring, this ledger architecture minimises opportunities for undetected tampering, replay, or selective deletion of accounting records, while preserving the auditability expected under ISA, PCAOB, and SOX 404 internal-control requirements [632].

8.10. Strategic Benefits and Organisational Contribution of the Unified Framework

Adopting this unified framework generates multi-dimensional benefits for organisations. First, financial accuracy and data integrity improve because all postings and adjustments are subject to cryptographic integrity checks, AI-based anomaly screening, and immutable evidencing. Studies on AI-driven fraud detection and blockchain-enabled accounting indicate reductions in undetected fraud, fewer manual errors, and improved reconciliation quality [630].

Second, real-time fraud detection and continuous auditing become feasible, as AI models and behavioural analytics operate continuously rather than at discrete audit intervals. This supports closer alignment with ISA 315's risk-based approach and PCAOB standards on internal control over financial reporting [632].

Third, immutable audit trails and cryptographically enforced segregation of duties enhance compliance with ISA, PCAOB, and SOX requirements for evidence, internal controls, and traceability of management judgments [632].

Fourth, CFO decision-making is strengthened through more reliable, timely, and granular risk information. Integrated AI dashboards provide early warnings on credit deterioration, liquidity stress, and emerging fraud hotspots, while blockchain-anchored data increases confidence in the underlying figures [631].

Finally, by adopting quantum-resilient cryptography and secure-by-design controls, the organisation future-proofs its financial infrastructure against quantum and AI-enabled adversaries, contributing to long-term resilience and preserving the economic value of historical financial archives [634].

8.11. Implementation Strategy for Organisations (CFO-Level Roadmap)

8.11.1 Vision and Motivation for Adoption

From a CFO perspective, the framework is adopted to achieve five strategic objectives: (i) data integrity, (ii) risk visibility, (iii) audit assurance, (iv) fraud resilience, and (v) cryptographic longevity. NIST's AI Risk Management Framework and zero-trust guidance both emphasise that governance and architectural decisions must be proactive, socio-technical, and risk-based—not merely technology-driven [635].

CFOs, therefore, articulate a clear vision statement that positions AI, PQC, and blockchain not as experimental pilots but as integral capabilities for safeguarding financial reporting quality, regulatory compliance, and stakeholder trust over the next 10–15 years of quantum and AI disruption.

8.11.2 AI Adoption Areas in Accounting and Finance

The roadmap identifies concrete AI adoption domains:

- **Accounts Payable/Receivable (AP/AR):** automated invoice matching, duplicate-payment detection, and supplier-risk scoring;
- **Treasury:** cash-flow forecasting, liquidity optimisation, and intraday stress testing;
- **Financial Reporting:** anomaly detection in consolidation, narrative consistency checks, and disclosure analytics;
- **Tax computation:** automated classification of tax-relevant items and detection of unusual effective-tax-rate movements;
- **Asset valuations and impairment testing:** scenario analysis and fair-value estimation;
- **Budgeting and forecasting:** predictive models for revenue, expenses, and capital allocation.

Recent systematic reviews document that AI applications in finance are particularly mature in credit scoring, fraud detection, risk management, and forecasting—indicating that AI-oriented adoption can build on existing best practices rather than starting from scratch [631].

8.11.3 Strategy for Quantum Adoption

For quantum readiness, the CFO sponsors a phased PQC migration plan aligned with NIST and NCSC guidance [634]:

- 1. Discovery and inventory:** catalogue cryptographic dependencies across ERP, consolidation, treasury, reporting, and archive systems.

2. **Hybrid PQC models:** implement hybrid key-exchange and signature schemes (classical + PQC) in high-value systems to manage compatibility and performance.
3. Pilot QKD channels for internal audit or inter-entity communication where long-term confidentiality is critical.
4. **Upgrade of signatures and certificates:** transition code-signing, digital signatures on financial statements, and approval workflows to PQC-compatible schemes.
5. **Secure financial archives:** prioritise migration of long-retention financial records, working papers, and regulatory filings to PQC-protected storage.

This strategy balances urgency (to mitigate harvest-now, decrypt-later risk) with operational realism, embedding crypto-agility into AIS design [636].

8.11.4 Cybersecurity Strategies in the Quantum–AI Era

The framework embeds zero-trust identity management, multifactor authentication (MFA), and secure-by-design principles across AIS. NIST’s Zero Trust Architecture (SP 800-207) moves defences away from perimeter-based trust to continuous verification of users, devices, and workloads, which is crucial when AI agents and remote finance teams access sensitive data from multiple environments [637].

In parallel, joint guidance from CISA and allied agencies on Secure-by-Design and Secure-by-Default urges software providers and adopters to embed security controls into system design and default configurations, rather than relying on after-the-fact hardening [638].

Within this thesis, blockchain-based integrity controls—such as hashed posting logs, tokenised approvals, and distributed reconciliation—are treated as core secure-by-design mechanisms for financial data integrity[149].

8.11.5 Human Capital and Skills Development

Successful implementation depends on human capital as much as technology. The framework, therefore, requires:

- AI literacy for accountants, auditors, and controllers, including understanding model outputs, limitations, and explainability requirements;
- Basic quantum fundamentals, enabling finance leaders to interpret PQC roadmaps and vendor claims;
- Operational blockchain knowledge, so finance teams can interpret on-chain records, smart-contract behaviour, and evidence provenance;
- Cybersecurity governance skills, including familiarity with ISO/IEC 27001, SOC 2 Trust Services Criteria, and NIST AI risk management principles [639].

This aligns with broader regulatory expectations that boards and audit committees demonstrate competence in technology-related risk oversight.

8.11.6 Governance, Regulatory, and Compliance Alignment

The integrated framework is explicitly designed to support multi-standard compliance:

ISO/IEC 27001:2022 for information security management systems, by providing structured controls for confidentiality, integrity, and availability of accounting data;

SOC 2 Trust Services Criteria (security, availability, processing integrity, confidentiality, privacy) for service-organisation controls, especially where accounting is cloud-outsourced;[640]

International Standards on Auditing (ISA), particularly ISA 315 (Revised), by enhancing risk identification, assessment, and documentation through AI and immutable evidence [632];

PCAOB standards on internal control over financial reporting (e.g., AS 2201 / AS5), by strengthening IT-dependent controls and audit evidence quality [641];

Sarbanes–Oxley Act Section 404 (SOX 404), by improving management’s ability to design, operate, and document effective internal controls over financial reporting.[642]

Ethical AI assurance and transparent explainability are supported through alignment with NIST’s AI Risk Management Framework, which emphasises traceability, transparency, and accountability across the AI lifecycle.

Blockchain-anchored logs and PQC-protected archives enhance the auditability of internal controls, while zero-trust and secure-by-design measures reinforce governance around system access and software supply chains [637, 638].

A high-level cost–benefit analysis typically shows that the upfront investments (AI models, PQC migration, blockchain integration, training) are justified by reduced fraud losses, lower manual audit effort, fewer control failures, and extended cryptographic protection of long-term financial records—particularly for institutions with large transaction volumes and stringent regulatory obligations [630].

8.12. Contributions to the theory of CS for Accounting and Finance

This research makes a substantive theoretical contribution to the cybersecurity literature in accounting and finance by demonstrating that cyber risk in modern financial information systems is multi-layered, adversarial, and technologically evolving, requiring a shift from traditional internal control models toward an integrated, adaptive cybersecurity architecture.

Table 8.3 shows the main components of each chapter and their contributions to the Integrated Framework.

Firstly, the findings in Chapter 3 reconceptualise trust in accounting systems. Traditional AIS theory assumes that audit assurance is achieved retrospectively through documentation and reconciliation. However, the integration of blockchain-based immutable records reframes trust as cryptographically guaranteed at the point of transaction, reducing dependence on after-the-fact audit reconstruction [37, 40, 348]. This establishes a new theoretical grounding in ledger-level security, where auditability and integrity are embedded into the transaction itself.

Secondly, Chapters 4 and 7 extend fraud detection theory by demonstrating that fraudulent patterns in accounting data are behaviourally adaptive and structurally non-linear. Ensemble models such as Random Forest [563] and XGBoost [557] reveal that fraud cannot be

effectively modelled using static thresholds or linear relationships. This shifts the theoretical lens from “fraud as anomaly” to fraud as dynamic behavioural deviation, requiring learning-based detection rather than rule enforcement.

Thirdly, Chapter 5 introduces a forward-looking theoretical dimension by positioning cybersecurity in accounting as a time-sensitive phenomenon. The emergence of quantum computing threatens classical encryption protocols, meaning long-term financial record security must incorporate quantum-resistant cryptographic planning [138], [411]. This advances the theoretical discourse by framing cybersecurity not only as a present control requirement but as a future-proofing obligation in financial governance.

Finally, Chapter 6 integrates game theory to explain cyber risk as a strategic attacker–defender interaction, where threat actors adapt based on expected detection and organisational enforcement strategies [507], [509]. This shifts the theoretical basis of cybersecurity from a defensive posture to a strategic equilibrium model, where optimal security outcomes depend on anticipating adversary strategy rather than merely reacting to detected breaches.

Together, these contributions form a unified theoretical proposition:

Effective cybersecurity in accounting and finance systems requires a multi-layered, behaviour-aware, strategically adaptive, cryptographically resilient defence architecture, rather than isolated technical controls or post-hoc auditing.

8.13. Use Cases in Accounting and Finance

This section demonstrates how the BQMG-AIS+ Framework (Blockchain + Quantum + Machine Learning + Game Theory) can be operationalised across everyday organisational contexts. The use cases are presented in general corporate settings, making them applicable across industries. Table 8.4 gives a few examples of day-to-day accounting activities in which the Integrated Framework is applied.

8.13.1 Use Case 1: Real-Time Fraud Monitoring in Accounts Payable

- i. Blockchain Layer (Integrity): Ensures that invoice and payment records cannot be altered after entry, preventing unauthorised back-dating or value manipulation [348].
- ii. Machine Learning Layer (Detection): XGBoost [557] flags abnormal payment requests (e.g., unusual amounts, vendor change requests).
- iii. Explainability Layer: SHAP [331] explains why the transaction was flagged (e.g., “unusual vendor account change + off-hours submission”), enabling internal auditors to understand the risk quickly.
- iv. Game Theory Layer (Strategic Defence): Internal controls adjust dynamically as fraud patterns evolve (e.g., increase approval requirements if attackers adapt tactics) [348].

Business Impact: Reduces financial loss exposure and improves audit readiness with minimal disruption to staff workflow.

8.13.2 Use Case 2: Financial Statement Integrity and Audit Trail Strengthening

- Blockchain ensures tamper-resistant journals and ledger entries, providing continuous rather than periodic auditability [37, 40].
- ML detects subtle irregular posting patterns that may indicate earnings manipulation or insider override.
- Explainability ensures audit defensibility, allowing findings to be justified to external auditors, regulators, and audit committees.

Business Impact: Strengthens trust in reported financial outcomes and supports transparent governance.

8.13.3 Use Case 3: Internal Controls Against Social Engineering and Insider Threats

- Game Theory models attacker incentives, predicting where insider manipulation is most likely [509].
- ML flags behavioural anomalies such as sudden access to unusual financial modules.
- Explainability tools ensure findings can be reviewed by HR, compliance, and finance leadership without requiring technical expertise.

Business Impact: Supports organisation-wide risk mitigation and reduces dependence on manual monitoring.

8.13.4 Strategic Risk Management Using Game Theory

Game-theoretic models empower audit committees and compliance officers to simulate fraud risk scenarios. By quantifying potential attacker strategies, organisations can prioritise cybersecurity investments and allocate resources dynamically across prevention, detection, and response measures [483].

8.13.5 Use Case 4: Post-Quantum Security Transition Planning

- Chapter 5 establishes a roadmap for adopting quantum-resistant cryptography before classical encryption becomes exposed [138, 411].
- Blockchain-anchored audit proofs remain valid and secure during cryptographic migration.
- ML-driven access monitoring ensures system integrity during the transition period.

Business Impact: Ensures long-term survivability of financial data security and regulatory compliance.

8.14. Validation of Research Hypotheses (H1–H4)

This section synthesises empirical findings presented in Chapter 7 with the conceptual, theoretical, and organisational perspectives developed in Chapters 3 through 6. The hypotheses are evaluated using multi-layered triangulation, which combines statistical model evidence, technology adoption considerations, audit and compliance implications, and cybersecurity behavioural theory.

8.14.1 Hypothesis: H1

Ensemble models (Random Forest and XGBoost) outperform linear models in detecting fraudulent transactions.

The empirical model comparison in Chapter 7 demonstrated that ensemble methods, particularly Random Forest and XGBoost, consistently achieved higher recall and F1 Scores than Logistic Regression across all three datasets used in this research. This is theoretically consistent with prior machine learning research, which shows that ensemble models reduce variance and capture non-linear feature interactions by aggregating multiple decision boundaries [563], [557]. From the AIS domain perspective, fraud patterns within accounting records are rarely linear or isolated. As shown in Chapter 4, fraudulent behaviours often adapt in response to organisational controls and internal audit processes, making dynamic and non-linear modelling approaches critical. Further, the game-theoretic framing in Chapter 6 indicates that adversaries behave strategically rather than randomly, reinforcing the need for detection models capable of learning evolving behavioural signals rather than static thresholds. Thus, H1 is supported: Ensemble models outperform linear models because they better reflect the real-world complexity, adaptiveness, and strategic behaviour underpinning financial fraud.

Accounting Area	Problem / Risk	BQMG-AIS Layer Applied	How the Model Helps in Day to Day Activity
Accounts Payable (AP)	Fake vendor invoice / change in bank account	Blockchain + ML + Game Theory	Blockchain prevents silent changes in vendor details → ML flags suspicious changes → GTM requires mandatory callback verification.
Payroll / HR	Ghost employee, salary manipulation	Blockchain + ML	Blockchain makes payroll entries uneditable → ML detects abnormal salary jumps or duplicated bank accounts.
General Ledger (GL)	Backdated journal entries to inflate revenue	Blockchain	Once a journal entry is posted, blockchain prevents tampering and keeps a timestamped audit trail.
Financial Reporting	Management override of controls	Blockchain + ML + Game Theory	Blockchain preserves integrity → ML flags suspicious end-of-month adjustments → GTM supports multi-level approvals.
E-Invoicing / AR	Duplicate invoices or fraudulent refunds	ML + Blockchain	ML identifies duplicate patterns → Blockchain prevents invoice modification or deletion.
Bank Reconciliation	Unauthorised bank transfers	ML + Quantum	ML detects abnormal transfers → quantum security protects bank feed data from future decryption threats.
CEO/CFO Email Fraud (BEC)	Impersonation demanding urgent payment	ML + Game Theory	ML flags abnormal communication → GTM supports “Always Verify High-Value Requests” equilibrium strategy.
Audit Evidence Management	Altering or deleting audit evidence	Blockchain + Quantum	Evidence stored on blockchain cannot be changed → PQC/QKD keeps evidence protected for long-term storage.
Internal Controls Monitoring	Weak segregation of duties (SoD)	Game Theory + ML	GTM identifies where SoD is weakest → ML monitors access logs for unusual cross-role behaviour.
E-commerce Fraud	Abnormal card transactions	ML	XGBoost detects fraud with high recall → supports continuous auditing and ISA-240 fraud assessments.
Vendor Management	Fraudulent vendor onboarding	Blockchain + ML + GTM	Blockchain stores vendor data → ML flags suspicious onboarding → GTM enforces mandatory background checks or dual approvals.
Asset Management	Misuse or unauthorised write-offs	Blockchain + ML	Immutable asset register → ML detects unusual disposal patterns.
Cloud Accounting (Xero, SAP, Oracle)	Cloud breach or data theft	Quantum + Blockchain	PQC protects cloud data → blockchain stores verification logs.
Internal Audit	Difficulty identifying high-risk areas	ML	ML risk-scores transactions → auditors focus on highest-risk samples immediately.
Cybersecurity / IT Audit	Social engineering (phishing)	Game Theory	GTM shows verification as optimal strategy (Nash equilibrium).

TABLE 8.4 THE INTEGRATED FRAMEWORK AND ACCOUNTING ACTIVITIES

8.14.2 Hypothesis: H2

XGBoost achieves superior recall and PR-AUC in highly imbalanced datasets.

XGBoost demonstrated the highest recall (0.986-0.992) and PR-AUC (0.981-0.985) across the Credit Card, IEEE-CIS, and PaySim datasets evaluated in Chapter 7. High recall is significant in financial systems, where undetected fraud carries disproportionate financial, reputational, and regulatory consequences. XGBoost's gradient-boosting optimisation enables effective learning from sparse fraud signals and penalises misclassification of minority-class transactions [557]. Moreover, Chapter 3 showed that blockchain-based audit trails improve the reliability of training data, and Chapter 4 emphasised that detection systems in AIS require consistency with internal control environments. The conceptual foundation presented in Chapter 5 further highlighted that scalable models such as XGBoost are well-positioned for transition into emerging post-quantum cryptographic infrastructures. Therefore, H2 is validated: XGBoost achieves the best detection performance on imbalanced accounting datasets by prioritising rare but high-impact fraud events.

8.14.3 Hypothesis: H3

Logistic Regression combined with SHAP provides superior interpretability and calibration required for audit and compliance.

While ensemble models provided stronger predictive performance, Logistic Regression achieved the most stable calibration curves, and when paired with SHAP, produced transparent, auditor-verifiable explanations for each flagged transaction [331]. As Chapter 3 explains, financial audit environments require transparency and traceability of evidence. Chapter 4 further emphasises that regulatory oversight frameworks (e.g., SOX, ISA, PCAOB) increasingly require explainability in automated decision systems to avoid "black box" risks. Chapter 6 demonstrated that human analysts respond more effectively to risk signals when model reasoning is interpretable rather than opaque.

Therefore, H3 is validated: Interpretability is essential not only for user trust but also for regulatory compliance, audit defensibility, and governance accountability.

8.14.4 Hypothesis: H4

Cross-dataset validation improves generalisability, though performance varies with contextual transaction environments.

Cross-dataset validation in Chapter 7 showed that while model performance trends remained broadly stable across domains, threshold calibration and feature weighting required adjustment to reflect contextual differences in transaction structure, fraud frequency, and organisational payment systems. Chapter 3 demonstrated that AIS architectures differ across ERP, payment gateway, and blockchain-assisted environments. Chapter 4 identified variability in cybersecurity maturity across organisations. Chapter 6 highlighted that fraud behaviour differs across cultural and organisational contexts, affecting the interpretability and transferability of learned patterns. Thus, H4 is partially supported: Cross-dataset validation strengthens robustness, but deployment requires environment-specific calibration and continuous monitoring.

8.15. Summary of implications

The unified cybersecurity framework presented in this chapter demonstrates how AI, blockchain, post-quantum cryptography, and game-theoretic controls can be operationalised as an integrated defence architecture for accounting and finance systems. By linking quantum-secure data pipelines with real-time AI monitoring and immutable ledger assurance, the model strengthens the integrity, reliability, and auditability of financial information while preparing organisations for emerging quantum and AI-enabled threats. As financial ecosystems evolve toward hyper-digitalisation, institutions that adopt these integrated capabilities will be better positioned to maintain regulatory compliance, enhance fraud resilience, and safeguard high-value financial records over the long term. This provides a foundation for the next chapter, which extends the framework into practical validation, organisational readiness, and policy-level implications for future accounting infrastructures.

Chapter 9

9. Contributions, Summary and Conclusions

9.1. Theoretical, Methodological, and Practical Contributions

This research contributes to the academic literature on cybersecurity in accounting and finance by developing and empirically validating a multi-layered cybersecurity framework (BQMG-AIS+) that integrates Blockchain, Quantum Computing, Machine Learning, and Game Theory. To clarify the nature and originality of the contributions presented in this chapter, it is important to distinguish between three types of contributions developed in this research. First, the thesis introduces novel contributions, including the integrated BQMG-AIS+ cybersecurity framework, which combines Blockchain, Quantum Computing, Machine Learning, and Game Theory within a unified accounting architecture. Second, the research makes significant contributions by adapting and contextualising existing technologies, such as machine learning-based fraud detection and blockchain audit trails, within accounting information systems. Third, the thesis offers integrative contributions, synthesising insights across disciplines to develop a cohesive, multi-layered cybersecurity model.

This structured distinction enhances clarity regarding the originality of the research and situates the contributions within the broader academic literature on accounting information systems and cybersecurity [624].

The contributions of this study can be divided into three main parts. First, it shows how machine learning models can be used and tested on different financial fraud datasets. Second, it adds new ideas by combining new technologies with an accounting information system (AIS) cybersecurity framework. Third, it presents the design of the BQMG-AIS model, which helps to link new technology with proper management and cybersecurity needs.

The contributions span theoretical advancement, methodological innovation, and practical implementation guidance for accounting professionals and organisational decision-makers.

9.1.1 Theoretical Contributions

The thesis advances cybersecurity theory in the accounting and finance discipline by establishing that cyber risk in financial information systems is not only technical, but also behavioural, strategic, and systemic. Existing AIS cybersecurity models predominantly rely on either (i) perimeter-based IT controls or (ii) post-event audit detection. The findings from Chapters 3 to 6 demonstrate that:

- Blockchain enhances data integrity, provenance, and audit assurance by preventing unauthorised record modification [100], [616].
- AI/ML models enable adaptive anomaly detection suited for dynamic fraud behaviours [116].
- Quantum computing developments introduce cryptographic risks and resilience opportunities, advancing theoretical understanding of long-term security viability [138].

- Game theory models cybersecurity as an attacker–defender interaction, establishing cyber defence as a strategic equilibrium problem rather than a purely technical control system [58], [613].

Collectively, this thesis proposes that effective cybersecurity in accounting requires multi-layer integration, shifting the paradigm from reactive control to proactive, strategic, and cryptographically resilient defence architectures.

9.1.2 Contribution to Accounting Information Systems Theory

Traditional AIS frameworks assume centralised trust, the ability to reconstruct audits, and static internal controls. However, the empirical and conceptual findings in this research demonstrate that:

- Fraud and cyberattacks increasingly target real-time financial workflows (e.g., automated payments, digital receipts).
- Distributed ledger architectures provide verifiable audit trails that eliminate reconstructive audit dependency [348].
- ML-driven detection systems embedded into AIS workflows provide continuous audit and risk scoring, complementing rather than replacing professional judgment.

Therefore, the thesis contributes to AIS theory by positioning cybersecurity as a foundational accounting function rather than an IT adjunct.

9.1.3 Contribution to Machine Learning and Cybersecurity Theory

Chapter 7 demonstrated that XGBoost [557] and Random Forests [563] outperform linear models in identifying complex, low-frequency fraud patterns across diverse financial ecosystems. At the same time, SHAP-explainable Logistic Regression [331] provides the interpretability required for regulatory trust.

This supports the theoretical position that fraud detection in accounting requires hybrid ML strategies that:

- Maximise anomaly detection capability (via ensemble models)
- Maintain explainability for audit and compliance (via interpretable models)

This thesis, therefore, bridges the theoretical gap between predictive strength and regulatory-aligned interpretability.

9.1.4 Integration of Game Theory in Financial Cyber Defence

Chapter 6 established that cybercrime in accounting systems is not random; it reflects strategic adversarial planning. Using attacker–defender payoff modelling [507], [509], the thesis shows that:

- Fraud schemes evolve in response to implemented controls.
- Defence strategies must anticipate adversary adaptation cycles.
- ML systems must be continuously retrained, not static.

Thus, the thesis contributes to cybersecurity defence theory by embedding ML-based fraud detection within a strategic threat-behaviour model, thereby strengthening resilience.

9.1.5 Cross-Disciplinary Contribution

The thesis demonstrates that financial cybersecurity cannot be solved within a single disciplinary boundary. It links as shown in Table 9.1. This cross-disciplinary integration (Ch. 3–7) is itself a significant contribution to knowledge.

9.1.6 Streamlit-Based Prototype Integration

The Streamlit dashboard operationalises the theoretical framework into a working fraud detection system (Ch. 7). Its contributions include:

- Human-in-the-loop validation for auditors and finance managers
- Interactive SHAP-based justification of flagged transactions
- Cross-dataset fraud pattern exploration for model transparency

This prototype bridges academic research and real-world deployability, supporting practitioner adoption.

Discipline	Contribution to Cybersecurity in Accounting
Accounting	Audit compliance, records assurance, governance
Computer Science	ML anomaly detection, cryptographic protocols
Economics/Game Theory	Adversarial risk strategy modelling
Quantum Computing	Future-proof encryption and data protection

TABLE 9.1 CROSS-DISCIPLINARY CONTRIBUTION

9.1.7 Regulatory and Compliance Integration

The thesis aligns ML-based detection with:

- SOX, ISA, and IFRS compliance transparency expectations
- GDPR and data governance obligations [566]
- Audit traceability and explainability standards

This ensures that the BQMG-AIS+ framework is not only technically feasible but also legally and ethically deployable in regulated accounting environments.

9.1.8 Methodological Contributions

Methodologically, the thesis contributes:

- A multi-dataset cross-context evaluation framework (Ch. 7)
- A hybrid detection model selection logic balancing interpretability and performance
- A layered cybersecurity architecture specification (Sections 8.3 and 8.6)

This addresses the limitations of previous single-dataset, single-algorithm studies.

9.1.9 Practical and Policy Contributions

For organisations, the thesis provides:

- A roadmap for embedding ML-driven fraud monitoring into ERP and AIS workflows
- A strategy for transitioning to quantum-resistant financial security (Ch. 5)
- A playbook for mitigating social engineering and insider risk using GT (Ch. 6)

For policymakers:

» The framework offers evidence-based guidance for future digital audit standards.

9.2. Integration of Research Questions (RQ1–RQ4) and Cross-Chapter Synthesis

The classification of evidence types reflects the methodological structure of the thesis, where empirical validation is primarily associated with machine learning models (Chapter 7), while conceptual and architectural validation underpin the integrated framework.

RQs	Integrated Answer	Supporting	Type of Evidence
RQ1	Fraud can be effectively detected in highly imbalanced datasets using ensemble ML models supported by reliable audit-evidence trails.	Ch. 3, 4, 7	Emperical + Conceptual
RQ2	A hybrid model approach is required: ensembles for detection strength, Logistic Regression for model interpretation, and SHAP for audit explainability.	Ch. 4, 6, 7	Emperical + Conceptual
RQ3	Explainability enables alignment with compliance requirements, forensic justification, and enhanced auditor trust when combined with blockchain traceability.	Ch. 3, 4, 7	Conceptual + Emperical
RQ4	The BQMG-AIS+ Framework integrates Blockchain (integrity), Quantum (future-proofing), ML (detection), and Game Theory (strategic defence) into a cohesive architecture.	Ch. 3–7	Architectural + Conceptual

TABLE 9.2 CROSS-CHAPTER SYNTHESIS

9.3. Impact and Implications of the Integrated BQMG-AIS Framework

9.3.1 Overall Impact of the Integrated Framework

The integrated BQMG-AIS cybersecurity framework developed in this thesis represents a significant advancement in the protection and governance of accounting information systems. By synthesising Blockchain, Quantum Computing, Machine Learning, and Game Theory into a cohesive, multi-layered architecture, this framework offers a robust defence mechanism that effectively addresses both technical vulnerabilities and behavioural weaknesses within the finance function.

Each layer serves a distinct purpose:

- Blockchain ensures data integrity while providing tamper-proof audit trails.
- Quantum Computing enhances long-term cryptographic resilience.
- Machine Learning enables the early detection of anomalies and fraudulent transactions.
- Game Theory models human behaviour to optimise control design.

The interplay among these layers fosters a comprehensive cybersecurity ecosystem, thereby enhancing the reliability of financial reporting, mitigating fraud risk, improving auditability, and preparing organisations for both current and emerging cyber threats. This integrated approach delivers a practical and theoretically grounded blueprint for the next generation of secure accounting systems, surpassing traditional accounting information system (AIS) models.

9.3.2 Implications for CFOs and Finance Leaders

The integrated framework offers Chief Financial Officers (CFOs) significant strategic, operational, and governance benefits. It enhances the integrity of financial reporting by leveraging Blockchain technology's immutability and improves fraud detection in Accounts Payable, Payroll, and Treasury through the application of Machine Learning. Additionally, it reduces the risk of insider manipulation by employing Game-Theoretic control optimisation. The inclusion of quantum-secure cryptography provides long-term protection for financial data, effectively addressing emerging regulatory requirements for cybersecurity readiness. These combined capabilities enable CFOs to make informed, data-driven decisions regarding resource allocation, internal control design, risk management, and digital transformation initiatives.

Furthermore, the framework ensures compliance with international standards such as ISA, COSO, and SOX, enhances transparency with auditors and the Audit Committee, and minimises financial and reputational risks associated with cyber incidents. Ultimately, this integrated framework equips CFOs with a comprehensive cybersecurity strategy that promotes resilience, operational efficiency, and organisational trust within an increasingly digital financial environment.

9.4. Limitations and Future Work

Despite its conceptual and empirical robustness, the BQMG framework presents limitations that guide future research directions.

9.4.1 Data Availability and Generalizability

The fraud datasets used vary in structure and regional context. While cross-dataset validation strengthened robustness, domain-specific model tuning remains necessary.

9.4.2 Computational Complexity

The integration of blockchain and quantum layers introduces computational overhead. Real-world implementation may face latency challenges, particularly in mobile or low-bandwidth financial networks. Future work could employ quantum-accelerated processors or edge computing solutions to reduce this burden [643].

9.4.3 Model Explainability and Auditor Adoption

Even with SHAP interpretability, some ML models remain “black boxes” to non-technical auditors. Future research should explore hybrid explainability methods combining symbolic reasoning and causal AI to make models more transparent and auditor-friendly [644].

9.4.4 Quantum Readiness and Interoperability

Quantum security remains an emerging field. Integrating PQC algorithms into legacy accounting systems will require standardisation and interoperability frameworks between cryptographic protocols [645].

9.4.5 Ethical and Governance Considerations

Governance frameworks must ensure human oversight in all high-risk decision-making, maintaining ethical integrity alongside technological advancement [273].

9.4.6 Scope-Related Limitations (Doctoral Constraints)

This research is subject to limitations inherent to doctoral-level studies. These include reliance on publicly available datasets rather than on organisational data, partial implementation of framework components rather than full system integration, and constraints on computational resources and time. These limitations reflect practical boundaries of academic research rather than conceptual weaknesses of the framework.

9.4.7 Field-Level Research Challenges

Beyond the scope of this thesis, several broader challenges remain open within the field. These include integrating post-quantum cryptography into legacy accounting systems, scaling blockchain-based audit infrastructures, and developing explainable AI techniques suitable for high-dimensional financial datasets. Addressing these challenges requires interdisciplinary collaboration and long-term empirical validation across organisational contexts.

9.5. Conclusion

This thesis examined the evolving cybersecurity challenges facing modern accounting and finance systems. It proposed the BQMG-AIS+ Framework, a multi-layered cybersecurity architecture that integrates Blockchain, Machine Learning, Quantum-Resistant Cryptography, and Game-Theoretic Defence Strategies. Drawing on findings from Chapters 3 to 7, the research demonstrated that financial cybersecurity risks are no longer confined to technical vulnerabilities alone; rather, they emerge from a combination of data manipulation threats, behavioural adversary strategies, cryptographic instability, and explainability limitations in automated decision systems.

Chapter 3 established the importance of immutable audit trails and trust-by-design assurance through blockchain-based ledger structuring, shifting financial integrity from reconstructive audit validation to cryptographically verified record provenance.

Chapter 4 highlighted the centrality of explainable machine learning in fraud detection, demonstrating how SHAP-based transparency supports regulatory oversight and professional accountability.

Chapter 5 introduced post-quantum risk considerations, showing that long-term financial record confidentiality cannot rely solely on classical encryption.

Chapter 6 illustrated that cybersecurity in accounting must be understood as a strategic interaction between attackers and defenders, informed by rational incentives and the adaptation of adversaries.

Chapter 7 provided empirical validation across three fraud datasets, demonstrating that ensemble ML models outperform linear classifiers, while interpretable models remain essential for compliance adoption.

Together, these chapters converge in the BQMG-AIS+ Framework, which positions cybersecurity in accounting as:

- Proactive, not reactive
- Transparent and auditable, not algorithmically opaque
- Strategically adaptive, not static
- Future-oriented, not cryptographically fragile

The framework contributes to theory by redefining cybersecurity in accounting as a multi-disciplinary governance construct, integrating technological assurance, behavioural risk modelling, cryptographic resilience, and explainable decision intelligence.

In practice, the research delivers a deployable pathway for organisations seeking to strengthen fraud monitoring, enhance audit quality, transition to post-quantum secure infrastructure, and institutionalise adaptive risk response mechanisms. The Streamlit-based human-in-the-loop audit dashboard operationalises these capabilities, demonstrating real-world feasibility.

Looking forward, the findings suggest that future accounting cybersecurity must evolve toward continuously learning systems, quantum-secure audit ecosystems, and strategically responsive defence models that anticipate rather than merely react to threat behaviour. As financial systems continue to digitalise and interconnect globally, the principles established in this research provide a foundational blueprint for securing the integrity, reliability, and trustworthiness of financial information in the decades to come.

10. References:

- [1] M. Akter, T.-F. Kummer, and O. Yigitbasioglu, "Looking beyond the hype: The challenges of blockchain adoption in accounting," *International Journal of Accounting Information Systems*, vol. 53, p. 100681, 2024/06/01/ 2024, doi: <https://doi.org/10.1016/j.accinf.2024.100681>.
- [2] S. Yoon, "A Study on the Transformation of Accounting Based on New Technologies: Evidence from Korea," (in English), *Sustainability*, vol. 12, no. 20, p. 8669, 2021-07-07 2020, doi: <http://dx.doi.org/10.3390/su12208669>.
- [3] A. Bandeira, J. Nogueira, J. Vale, M. Tavares, and G. Azevedo, *Accounting for change: the importance of information technology in the accountants academic qualification*. 2023, pp. 1-7.
- [4] K. Mahmood, R. Mokhtar, M. Raza, and B. Raza, "Recent Advances in Big Data: Features, Classification, Analytics, Research Challenges, and Future Trends," vol. 20, pp. 139-150, 04/30 2020.
- [5] L. Yang, J. Li, N. Elisa, T. Prickett, and F. Chao, "Towards Big data Governance in Cybersecurity," *Data-Enabled Discovery and Applications*, vol. 3, no. 1, p. 10, 2019/12/02 2019, doi: 10.1007/s41688-019-0034-9.
- [6] X. Luo, Y. Liu, and Q. Li, "Big data-related technologies and applications," vol. 28, ed: Wiley Online Library, 2016, pp. 4036-4037.
- [7] D. Fujs, A. Mihelič, and S. L. Vrhovec, "The power of interpretation: Qualitative methods in cybersecurity research," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 2019, pp. 1-10.
- [8] D. Surya, D. Setiawan, Y. A. Aryani, and T. Arifin, "Cyberattacks on the accounting profession: a literatur review," *Media Riset Akuntansi, Auditing & Informasi*, vol. 24, no. 2, pp. 255-272, 2024.
- [9] V. Muravskiy, V. Farion, and A. Hrytsyshyn, "Quality of accounting information and principles of its cyber protection," *Scientific Notes of Ostroh Academy National University, "Economics" Series*, no. 23 (51), pp. 103-109, 2021.
- [10] V. Martsenyuk, A. Sverstyuk, I. Andrushchak, V. Chudovets, and V. Koshelyuk, "Aspects of protection of accounting data in the conditions of use of innovation and information technologies," *COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION*, no. 42, pp. 172-176, 2021.
- [11] A. Anyanwu, T. Olorunsogo, T. O. Abrahams, O. J. Akindote, and O. Reis, "Data confidentiality and integrity: a review of accounting and cybersecurity controls in superannuation organizations," *Computer Science & IT Research Journal*, vol. 5, no. 1, pp. 237-253, 2024.

- [12] O. Michalec, S. Milyaeva, and A. Rashid, "When the future meets the past: Can safety and cyber security coexist in modern critical infrastructures?," *Big Data Soc.*, vol. 9, no. 1, p. 20539517221108369, 2022.
- [13] M. Bano, D. Zowghi, P. Shea, and G. Ibarra, "Investigating responsible AI for scientific research: an empirical study," *arXiv preprint arXiv:2312.09561*, 2023.
- [14] R. Ellis and V. Mohan, *Rewired: cybersecurity governance*. John Wiley & Sons, 2019.
- [15] M. Amanowicz and M. Kamola, "Building security awareness of interdependent services, business processes, and systems in cyberspace," *Electronics*, vol. 11, no. 22, p. 3835, 2022.
- [16] S. Romanosky, "Examining the costs and causes of cyber incidents," *J. Cybersecurity*, vol. 2, no. 2, pp. 121-135, 2016, doi: 10.1093/cybsec/tyw001.
- [17] E. Kopp, L. Kaffenberger, and N. Jenkinson, *Cyber risk, market failures, and financial stability*. International Monetary Fund, 2017.
- [18] A. Bouveret, *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund, 2018.
- [19] M. Z. Malik, S. Khan, and H. U. Khan, "Transforming the competencies of Artificial Intelligence to ensure the Cyber Threats: A Systemic Literature Review of Business Sectors," in *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, 24-26 May 2022 2022: IEEE, pp. 1-6, doi: 10.1109/ICAIC53980.2022.9897051. [Online]. Available: <https://ieeexplore.ieee.org/document/9897051/>
- [20] D. Dai and S. Boroomand, "A review of artificial intelligence to enhance the security of big data systems: state-of-art, methodologies, applications, and challenges," *Arch. Comput. Methods Eng.*, pp. 1-19, 2021.
- [21] A. I. Hunjra, M. A. Ali, D. Chani, M. Irfan, H. Khan, and K. U. Rehman, "Employee voice and intent to leave: An empirical evidence of Pakistani banking sector," *African Journal of Business Management*, vol. 4, no. 14, pp. 3056-3061, 2010.
- [22] C. Guan, J. Mou, and Z. Jiang, "Artificial intelligence innovation in education: a twenty-year data-driven historical analysis," *International Journal of Innovation Studies*, vol. 4, no. 4, pp. 134-147, 2020.
- [23] C. Dirican, "The impacts of robotics, artificial intelligence on business and economics," *Procedia-Social and Behavioral Sciences*, vol. 195, pp. 564-573, 2015.
- [24] B. Li, C. Yao, F. Zheng, L. Wang, J. Dai, and Q. Xiang, "Intelligent decision support system for business forecasting using artificial intelligence," *Arab. J. Sci. Eng.*, pp. 1-11, 2021.
- [25] M. B. Romney and P. J. Steinbart, *Accounting Information Systems*. Pearson, 2014.
- [26] O. Awosejo, R. Kekwaletswe, P. Pretorius, and T. Zuva, "The effect of accounting information systems in accounting," *International Journal of Advanced Computer Research*, vol. 3, no. 3, p. 142, 2013.

- [27] J. L. Zimmerman, "Accounting for Decision Making and Control."
- [28] Y. A. Jasim and M. B. Raewf, "Impact of the information technology on the accounting system," *Cihan University-Erbil Journal of Humanities and Social Sciences*, vol. 4, no. 1, pp. 50-57, 2020.
- [29] H. Li, J. Dai, T. Gershberg, and M. A. Vasarhelyi, "Understanding usage and value of audit analytics for internal auditors: An organizational approach," *International Journal of Accounting Information Systems*, vol. 28, pp. 59-76, 2018.
- [30] J. Bierstaker, D. Janvrin, and D. J. Lowe, "What factors influence auditors' use of computer-assisted audit techniques?," *Advances in Accounting*, vol. 30, no. 1, pp. 67-74, 2014.
- [31] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers," *International Journal of Electronic Commerce*, vol. 9, no. 1, pp. 70-104, 2004.
- [32] E. Haapamäki and J. Sihvonen, "Cybersecurity in accounting research," (in English), *Managerial Auditing Journal*, vol. 34, no. 7, pp. 808-834, 2019; 2021-09-09 2019, doi: <http://dx.doi.org/10.1108/MAJ-09-2018-2004>.
- [33] L. Hasan, M. Z. Hossain, F. T. Johora, and M. H. Hasan, "Cybersecurity in accounting: Protecting financial data in the digital age," *European Journal of Applied Science, Engineering and Technology*, vol. 2, no. 6, pp. 64-80, 2024.
- [34] S. Demirkan, I. Demirkan, and A. McKee, "Blockchain technology in the future of business cyber security and accounting," *Journal of Management Analytics*, vol. 7, no. 2, pp. 189-208, 2020/04/02 2020, doi: 10.1080/23270012.2020.1731721.
- [35] I. Popchev, I. Radeva, and V. Velichkova, "The impact of blockchain on internal audit," in *2021 Big Data, Knowledge and Control Systems Engineering (BdKCSE)*, 28-29 Oct. 2021 2021, pp. 1-8, doi: 10.1109/BdKCSE53180.2021.9627276.
- [36] A. Pramukti, "Internal Audit versus External Audit: A Qualitative Perspective," *Golden Ratio of Auditing Research*, vol. 4, no. 2, pp. 78-88, 2024.
- [37] H. P. Wu, Z. H. Liu, H. Y. Dong, Y. Lu, and L. D. Xu, "Revolutionizing internal auditing: harnessing the power of blockchain," *Enterp. Inf. Syst.*, p. 2448003, 2025, doi: 10.1080/17517575.2024.2448003.
- [38] B. Anthony Jnr, "Enhancing blockchain interoperability and intraoperability capabilities in collaborative enterprise-a standardized architecture perspective," *Enterp. Inf. Syst.*, vol. 18, no. 3, p. 2296647, 2024/03/03 2024, doi: 10.1080/17517575.2023.2296647.
- [39] M. Kassen, "Blockchain and public service delivery: a lifetime cross-referenced model for e-government," *Enterp. Inf. Syst.*, vol. 18, no. 4, p. 2317175, 2024/04/02 2024, doi: 10.1080/17517575.2024.2317175.

- [40] F. Lumineau, W. Wang, and O. Schilke, "Blockchain Governance—A New Way of Organizing Collaborations?," *Organization Science*, vol. 32, no. 2, pp. 500-521, 2021, doi: 10.1287/orsc.2020.1379.
- [41] L. A. Gordon, M. P. Loeb, and L. Zhou, "The impact of information security breaches: Has there been a downward shift in costs?," *J. Comput. Secur.*, vol. 19, no. 1, pp. 33-56, 2011.
- [42] W. E. Forum. "Banking in the quantum technologies era: 3 strategic shifts to watch." <https://www.weforum.org/stories/2025/07/banking-quantum-era-fraud-detection-risk-forecasting-financial-services/> (accessed).
- [43] S. Kamiya, J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz, "Risk management, firm reputation, and the impact of successful cyberattacks on target firms," *Journal of Financial Economics*, vol. 139, no. 3, pp. 719-749, 2021/03/01/ 2021, doi: <https://doi.org/10.1016/j.jfineco.2019.05.019>.
- [44] G. Hassall, "Government Systems," in *Government and Public Policy in the Pacific Islands*: Emerald Publishing Limited, 2020, pp. 23-97.
- [45] P. K. Dubey, A. Jangid, and B. Chandavarkar, "An interdependency between symmetric ciphers and hash functions: a survey," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2020: IEEE, pp. 1-5.
- [46] M. Humbert, B. Trubert, and K. Huguenin, "A survey on interdependent privacy," *ACM Computing Surveys (CSUR)*, vol. 52, no. 6, pp. 1-40, 2019.
- [47] Z.-M. Zadorozhnyi, M. Muravskiy, O. Shevchuk, and M. Bryk, "Innovative Accounting Methodology of Ensuring the Interaction of Economic and Cybersecurity of Enterprises," 2021.
- [48] F. Valenza, E. Karafili, R. V. Steiner, and E. C. Lupu, "A hybrid threat model for smart systems," *IEEE Trans. Dependable Secur. Comput.*, vol. 20, no. 5, pp. 4403-4417, 2022.
- [49] S. S. Sarmah, "Understanding blockchain technology," *Computer Science and Engineering*, vol. 8, no. 2, pp. 23-29, 2018.
- [50] D. K. Bholane, "Blockchain technology: Implications for accounting and auditing," *Available at SSRN 5094485*, 2025.
- [51] G. Soundararajan and A. K. Tyagi, "Blockchain Technology: An Introduction," *Blockchain Technology in the Automotive Industry*, pp. 3-36, 2025.
- [52] A. K. Tyagi and M. M. Nair, "Preserving Privacy using Distributed Ledger Technology in Intelligent Transportation System," 24/10/2022 2022: ACM, 2022, doi: 10.1145/3549206.3549306. [Online]. Available: <https://dx.doi.org/10.1145/3549206.3549306>

- [53] R. Beck, M. Avital, M. Rossi, and J. B. Thatcher, "Blockchain Technology in Business and Information Systems Research," *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 381-384, 2017, doi: 10.1007/s12599-017-0505-1.
- [54] P. Centobelli, R. Cerchione, P. Del Vecchio, E. Oropallo, and G. Secundo, "Blockchain technology design in accounting: Game changer to tackle fraud or technological fairy tale?," *Accounting, Auditing & Accountability Journal*, vol. 35, no. 7, pp. 1566-1597, 2022, doi: 10.1108/AAAJ-10-2020-4994.
- [55] A. Hughes, A. Park, J. Kietzmann, and C. Archer-Brown, "Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms," *Business Horizons*, vol. 62, no. 3, pp. 273-281, 2019/05/01/ 2019, doi: <https://doi.org/10.1016/j.bushor.2019.01.002>.
- [56] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55-81, 2019/03/01/ 2019, doi: <https://doi.org/10.1016/j.tele.2018.11.006>.
- [57] A. Patil, S. Bharath, and N. Annigeri, "Applications of game theory for cyber security system: A survey," *International Journal of Applied Engineering Research*, vol. 13, no. 17, pp. 12987-12990, 2018.
- [58] B. Collins, S. Xu, and P. N. Brown, "SoK: Game-Theoretic Cybersecurity: Assumptions, Models, Gaps, and Bridges," *arXiv preprint arXiv:2401.13815*, 2024.
- [59] F. Anwar, B. U. I. Khan, R. F. Olanrewaju, B. R. Pampori, and R. N. Mir, "A comprehensive insight into game theory in relevance to cyber security," *Indonesian Journal of Electrical Engineering and Informatics (IJEI)*, vol. 8, no. 1, pp. 189-203, 2020.
- [60] R. Sharma, S. Mithas, and A. Kankanhalli, "Transforming decision-making processes: a research agenda for understanding the impact of business analytics on organisations," *Eur. J. Inform. Syst.*, vol. 23, no. 4, pp. 433-441, 2014.
- [61] L. V. Snyder, "Facility location under uncertainty: a review," *IIE transactions*, vol. 38, no. 7, pp. 547-564, 2006.
- [62] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," *Computers & Security*, vol. 59, pp. 186-209, 2016/06/01/ 2016, doi: <https://doi.org/10.1016/j.cose.2016.03.004>.
- [63] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, p. 89, 2019.
- [64] A. M. Aroyo, F. Rea, G. Sandini, and A. Sciutti, "Trust and Social Engineering in Human Robot Interaction: Will a Robot Make You Disclose Sensitive Information, Conform to Its Recommendations or Gamble?," *IEEE Robotics and Automation Letters*, vol. 3, no. 4, pp. 3701-3708, 2018, doi: 10.1109/LRA.2018.2856272.

- [65] C. Atwell, T. Blasi, and T. Hayajneh, "Reverse TCP and Social Engineering Attacks in the Era of Big Data," in *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, 9-10 April 2016 2016, pp. 90-95, doi: 10.1109/BigDataSecurity-HPSC-IDS.2016.60.
- [66] T. Mahmood and U. Afzal, "Security Analytics: Big Data Analytics for cybersecurity: A review of trends, techniques and tools," in *2013 2nd National Conference on Information Assurance (NCIA)*, 11-12 Dec. 2013 2013, pp. 129-134, doi: 10.1109/NCIA.2013.6725337.
- [67] P. Patil and P. Devale, "A literature survey of phishing attack technique," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 5, no. 4, pp. 2091-2121, 2016.
- [68] R. Kalniņš, J. Puriņš, and G. Alksnis, "Security Evaluation of Wireless Network Access Points," *Applied Computer Systems*, vol. 21, no. 1, pp. 38-45, 2017, doi: 10.1515/acss-2017-0005.
- [69] N. N. Pokrovskaja and S. O. Snisarenko, "Social engineering and digital technologies for the security of the social capital' development," in *2017 International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS)*, 24-30 Sept. 2017 2017, pp. 16-18, doi: 10.1109/ITMQIS.2017.8085750.
- [70] M. Levi, "Organized fraud and organizing frauds: Unpacking research on networks and organization," in *Transnational financial crime*: Routledge, 2017, pp. 309-340.
- [71] D. A. Mirchandani and A. L. Lederer, "IS planning autonomy in US subsidiaries of multinational firms," *Inf. Manage.*, vol. 41, no. 8, pp. 1021-1036, 2004/11/01/ 2004, doi: <https://doi.org/10.1016/j.im.2003.11.001>.
- [72] M. Schuld and F. Petruccione, *Supervised learning with quantum computers*. Springer, 2018.
- [73] S. Lloyd, M. Mohseni, and P. Rebentrost, "Quantum algorithms for supervised and unsupervised machine learning," *arXiv preprint arXiv:1307.0411*, 2013.
- [74] P. Wittek, *Quantum machine learning: what quantum computing means to data mining*. Academic Press, 2014.
- [75] M. Company. "What is Quantum Computing." <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-quantum-computing> (accessed 15/12/2024, 2025).
- [76] A. L. Samuel, "Some studies in machine learning using the game of checkers. II—Recent progress," *IBM Journal of research and development*, vol. 11, no. 6, pp. 601-617, 1967.

- [77] T. L. Scholten *et al.*, "Assessing the benefits and risks of quantum computers," *arXiv preprint arXiv:2401.16317*, 2024.
- [78] H. T. Nguyen, M. Usman, and R. Buyya, "QFaaS: A Serverless Function-as-a-Service framework for Quantum computing," *Future Generation Computer Systems*, vol. 154, pp. 281-300, 2024/05/01/ 2024, doi: <https://doi.org/10.1016/j.future.2024.01.018>.
- [79] T. M. Fernández-Caramés, "From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6457-6480, 2020, doi: 10.1109/JIOT.2019.2958788.
- [80] N. Bostrom, "What happens when our computers get smarter than we are?," in *TED*, ed: TED, 2015.
- [81] K. R. Bhatele, H. Shrivastava, and N. Kumari, "The Role of Artificial Intelligence in Cyber Security," in *Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems*: IGI Global, 2019, pp. 170-192.
- [82] I. H. Sarker, "Machine Learning: Algorithms, Real-World Applications and Research Directions," (in eng), *SN Comput Sci*, vol. 2, no. 3, pp. 160-160, 2021, doi: 10.1007/s42979-021-00592-x.
- [83] K. Napanda, H. Shah, and L. Kurup, "Artificial intelligence techniques for network intrusion detection," *International Journal of Engineering Research & Technology (IJERT)*, ISSN, pp. 2278-0181, 2015.
- [84] N. Adelaide, "Deepfake-enabled executive impersonation (CFO Fraud) at Arup," ed, 2024.
- [85] N. Adelaide, "UAE Bank Deepfake Voice Fraud," ed, 2021.
- [86] G. The, "Qantas Data Breach via Vishing and Social Engineering," ed, 2025.
- [87] SentinelOne, "Cybersecurity Trends: Phishing, Ransomware, and Insider Threats in Finance," ed, 2023.
- [88] S. Mari, "Cybersecurity in Accounting: Key Risks and How to Prevent Them," *TaxDome Blog*, 2022. [Online]. Available: <https://blog.taxdome.com/cybersecurity-accounting/>.
- [89] "The Impact of Cyberattacks on Financial Reporting," *Accounting for Everyone*, 2023. [Online]. Available: <https://accountingforeveryone.com/the-impact-of-cyberattacks-on-financial-reporting/>.
- [90] c. Wikipedia, "Wire Transfer Fraud via Cyber Manipulation," 2023 2023. [Online]. Available: https://en.wikipedia.org/wiki/Bank_fraud.
- [91] G. Kabanda, "Performance of Machine Learning and other Artificial Intelligence Paradigms In Cybersecurity," *Oriental journal of computer science and technology*, vol. 13, no. 1, pp. 1-21, 05/30 2020, doi: 10.13005/ojcs13.01.01.

- [92] A. Bhimani and L. Willcocks, "Digitisation, 'Big Data' and the transformation of accounting information," *Accounting and business research*, vol. 44, no. 4, pp. 469-490, 2014.
- [93] I. Wiafe, F. N. Koranteng, E. N. Obeng, N. Assyne, A. Wiafe, and S. R. Gulliver, "Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature," *IEEE Access*, vol. 8, pp. 146598-146612, 2020, doi: 10.1109/ACCESS.2020.3013145.
- [94] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications policy*, vol. 41, no. 10, pp. 1027-1038, 2017.
- [95] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117-2135, 2019.
- [96] M. Spremić and A. Šimunic, "Cyber security challenges in digital economy," in *Proceedings of the World Congress on Engineering*, 2018, vol. 1: Hong Kong: International Association of Engineers, pp. 341-346.
- [97] D. Appelbaum and R. Nehmer, *Designing and auditing accounting systems based on blockchain and distributed ledger principles* (null). 2017, p. null.
- [98] J. Kokina and T. H. Davenport, "The emergence of artificial intelligence: How automation is changing auditing," *Journal of emerging technologies in accounting*, vol. 14, no. 1, pp. 115-122, 2017.
- [99] M. G. Alles, "Drivers of the use and facilitators and obstacles of the evolution of big data by the audit profession," *Accounting horizons*, vol. 29, no. 2, pp. 439-449, 2015.
- [100] J. Dai and M. A. Vasarhelyi, "Toward blockchain-based accounting and assurance," *Journal of Information Systems*, vol. 31, no. 3, pp. 5-21, 2017.
- [101] U. J. Gelinas, R. B. Dull, and P. Wheeler, *Accounting information systems*. Cengage learning, 2014.
- [102] F. Denge, "An Artificial Intelligence Model to Enhance the Chartered Accountancy Profession," M.Com., University of Johannesburg (South Africa), South Africa, 28935392, 2021. [Online]. Available: <https://www.proquest.com/dissertations-theses/artificial-intelligence-model-enhance-chartered/docview/2619231683/se-2?accountid=14844>
- [103] S. Arief, "Digital Transformation in Accounting: The Nexus Between Technology, Leadership, and Beyond," in *Digital Transformation in Accounting and Auditing: Navigating Technological Advances for the Future*, A. Perdana and T. Wang Eds. Cham: Springer International Publishing, 2024, pp. 29-59.
- [104] R. Sotelo, D. Corbelleto, E. Dri, E. Giusto, and B. Montrucchio, "Quantum Computing in Finance: The Intesa Sanpaolo Experience," (in English), *IEEE Eng Manage Rev*, Article vol. 52, no. 2, pp. 9-15, 2024, doi: 10.1109/EMR.2024.3373796.

- [105] V. Sivaraman and B. Sikdar, "A game-theoretic approach for enhancing data privacy in sdn-based smart grids," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10583-10595, 2020.
- [106] C. Jim, G. Dimitoglou, and A. Salem, "Applying Game Theoretic Techniques to Improve the Accuracy of Tree-based Classification Results," in *2018 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, 6-8 Dec. 2018 2018, pp. 314-319, doi: 10.1109/ISSPIT.2018.8642742. [Online]. Available: <https://ieeexplore.ieee.org/document/8642742/>
- [107] W.-C. Liao, C.-Y. Yin, and J. K. Chiang, "Decision making model on strategic technology investment using game theory," in *2009 IEEE International Conference on Industrial Engineering and Engineering Management*, 2009: IEEE, pp. 813-817.
- [108] W. Chu, Y. Shi, X. Jiang, T. Ciano, and B. Zhao, "Game theory approach for secured supply chain management in effective trade management," *Ann. Oper. Res.*, pp. 1-19, 2024.
- [109] G. Wang, Y. Chao, Y. Cao, T. Jiang, W. Han, and Z. Chen, "A comprehensive review of research works based on evolutionary game theory for sustainable energy development," *Energy Reports*, vol. 8, pp. 114-136, 2022.
- [110] C. T. Thanh, "A Study of Machine Learning Techniques for Cybersecurity," in *2021 15th International Conference on Advanced Computing and Applications (ACOMP)*, 2021: IEEE, pp. 54-61.
- [111] A. Dewey and A. Drahota, "Introduction to systematic reviews: online learning module Cochrane Training," ed, 2016.
- [112] J. A. Paul and X. J. Wang, "Socially optimal IT investment for cybersecurity," *Decis. Support Syst.*, vol. 122, p. 113069, 2019.
- [113] M. Wazid, A. K. Das, V. Chamola, and Y. Park, "Uniting cyber security and machine learning: Advantages, challenges and future research," *ICT Express*, 2022/04/21/ 2022, doi: <https://doi.org/10.1016/j.ict.2022.04.007>.
- [114] A. Brabazon and M. O'Neill, "Natural computing in computational finance: An introduction," (in English), *Stud. Comput. Intell.*, Editorial vol. 100, pp. 1-4, 2008, doi: 10.1007/978-3-540-77477-8_1.
- [115] N. Innan *et al.*, "Financial fraud detection using quantum graph neural networks," *Quant. Mach. Intell.*, vol. 6, no. 1, p. 7, 2024.
- [116] K. Shaukat *et al.*, "Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity," *Energies*, vol. 13, no. 10, p. 2509, 2020. [Online]. Available: <https://www.mdpi.com/1996-1073/13/10/2509>.
- [117] S. Dey, Q. Ye, and S. Sampalli, "A machine learning based intrusion detection scheme for data fusion in mobile clouds involving heterogeneous client networks,"

- Information Fusion*, vol. 49, pp. 205-215, 2019/09/01/ 2019, doi: <https://doi.org/10.1016/j.inffus.2019.01.002>.
- [118] B. Geluvaraj, P. Satwik, and T. Ashok Kumar, "The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace," in *International Conference on Computer Networks and Communication Technologies*, 2019: Springer, pp. 739-747.
 - [119] P. Jain, "Machine learning versus deep learning for malware detection," 2019.
 - [120] R. S. Rao and A. R. Pais, "Detection of phishing websites using an efficient feature-based machine learning framework," *Neural Computing and Applications*, vol. 31, no. 8, pp. 3851-3873, 2019/08/01 2019, doi: 10.1007/s00521-017-3305-0.
 - [121] M. Alauthman, A. Almomani, M. Alweshah, W. Omoush, and K. Alieyan, "Machine learning for phishing detection and mitigation," in *Machine Learning for Computer and Cyber Security*: CRC Press, 2019, pp. 48-74.
 - [122] A. A. Alurkar *et al.*, "A comparative analysis and discussion of email spam classification methods using machine learning techniques," *Applied Machine Learning for Smart Data Analysis*, vol. 185, 2019.
 - [123] E. G. Dada, J. S. Bassi, H. Chiroma, A. O. Adetunmbi, and O. E. Ajibuwa, "Machine learning for email spam filtering: review, approaches and open research problems," *Heliyon*, vol. 5, no. 6, p. e01802, 2019. [Online]. Available: [https://www.cell.com/heliyon/pdf/S2405-8440\(18\)35340-4.pdf](https://www.cell.com/heliyon/pdf/S2405-8440(18)35340-4.pdf).
 - [124] H. A. Shukur and S. Kurnaz, "Credit card fraud detection using machine learning methodology," *International Journal of Computer Science and Mobile Computing*, vol. 8, no. 3, pp. 257-260, 2019.
 - [125] K. Avrachenkov, L. Huang, R. J. Marden, M. Coupechoux, and A. Giovanidis, "Game theory for networks," in *Proceedings of the 8th International EAI Conference, GameNets 2019*, 2019, vol. 277: Springer.
 - [126] N. Ruan, L. Gao, H. Zhu, W. Jia, X. Li, and Q. Hu, "Toward optimal dos-resistant authentication in crowdsensing networks via evolutionary game," in *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, 2016: IEEE, pp. 364-373.
 - [127] B. Cheng, D. Zhu, S. Zhao, and J. Chen, "Situation-aware IoT service coordination using the event-driven SOA paradigm," *IEEE Trans. Netw. Serv. Manag.*, vol. 13, no. 2, pp. 349-361, 2016.
 - [128] X. Dai *et al.*, "Task co-offloading for D2D-assisted mobile edge computing in industrial internet of things," *IEEE Trans. Ind. Inform.*, vol. 19, no. 1, pp. 480-490, 2022.

- [129] H. Gao, D. Shi, and B. Zhao, "Does good luck make people overconfident? Evidence from a natural experiment in the stock market," *Journal of Corporate Finance*, vol. 68, p. 101933, 2021.
- [130] M. Bouhaddi, M. S. Radjef, and K. Adi, "An efficient intrusion detection in resource-constrained mobile ad-hoc networks," *Computers & Security*, vol. 76, pp. 156-177, 2018.
- [131] H. Jin, H. Zhang, C. Zhang, and H. Hu, "Research on active defense decision-making method based on qrd in complex network," *Netinfo Security*, vol. 20, no. 5, pp. 72-82, 2020.
- [132] J. Schmitz and G. Leoni, "Accounting and auditing at the time of blockchain technology: a research agenda," *Australian Accounting Review*, vol. 29, no. 2, pp. 331-342, 2019.
- [133] E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," *Decis. Support Syst.*, vol. 50, no. 3, pp. 559-569, 2011/02/01/ 2011, doi: <https://doi.org/10.1016/j.dss.2010.08.006>.
- [134] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A systematic literature review of blockchain cyber security," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 147-156, 2020/05/01/ 2020, doi: <https://doi.org/10.1016/j.dcan.2019.01.005>.
- [135] M. Bellucci, B. Damiano Cesa, and G. Manetti, "Blockchain in accounting practice and research: systematic literature review," (in English), *Meditari Accountancy Research*, vol. 30, no. 7, pp. 121-146, 2022-04-15 2022, doi: <https://doi.org/10.1108/MEDAR-10-2021-1477>.
- [136] J. Dai, Y. Wang, and M. A. Vasarhelyi, "Blockchain: an emerging solution for fraud prevention," *The CPA Journal*, vol. 87, no. 6, pp. 12-14, 2017.
- [137] J. West and M. Bhattacharya, "Intelligent financial fraud detection: A comprehensive review," *Computers & Security*, vol. 57, pp. 47-66, 2016/03/01/ 2016, doi: <https://doi.org/10.1016/j.cose.2015.09.005>.
- [138] M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38-41, 2018, doi: 10.1109/MSP.2018.3761723.
- [139] R. Orús, S. Mugel, and E. Lizaso, "Quantum computing for finance: Overview and prospects," (in English), *Rev. Phys.*, Review vol. 4, 2019, Art no. 100028, doi: 10.1016/j.revip.2019.100028.
- [140] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Başar, and J.-P. Hubaux, "Game theory meets network security and privacy," *Acm Computing Surveys (Csur)*, vol. 45, no. 3, pp. 1-39, 2013.

- [141] D. Appelbaum, A. Kogan, and M. A. Vasarhelyi, "Big data and analytics in the modern audit engagement: Research needs," *Auditing: A Journal of Practice & Theory*, vol. 36, no. 4, pp. 1-27, 2017.
- [142] A. A. Almazroi and N. Ayub, "Online payment fraud detection model using machine learning techniques," *IEEE Access*, vol. 11, pp. 137188-137203, 2023.
- [143] J. Burrell, "How the machine 'thinks': Understanding opacity in machine learning algorithms," *Big Data Soc.*, vol. 3, no. 1, p. 2053951715622512, 2016.
- [144] R. Kapale, P. Deshpande, S. Shukla, S. Kediya, Y. Pethe, and S. Metre, "Explainable AI for fraud detection: enhancing transparency and trust in financial decision-making," in *2024 2nd DMIHER International Conference on Artificial Intelligence in Healthcare, Education and Industry (IDICAIEI)*, 2024: IEEE, pp. 1-6.
- [145] R. Orús, S. Mugel, and E. Lizaso, "Forecasting financial crashes with quantum computing," (in English), *Phys. Rev. A*, Article vol. 99, no. 6, 2019, Art no. 060301, doi: 10.1103/PhysRevA.99.060301.
- [146] M. A. I. Priom, S. L. Mudra, P. Ghose, K. R. Islam, and M. N. Hasan, "Blockchain applications in accounting and auditing: research trends and future research implications," *International Journal of Economics, Business and Management Research*, vol. 8, no. 7, pp. 225-247, 2024.
- [147] N. P. Giang and H. T. Tam, "Impacts of blockchain on accounting in the business," *SAGE Open*, vol. 13, no. 4, p. 21582440231222419, 2023.
- [148] R. Lombardi, C. de Villiers, N. Moscariello, and M. Pizzo, "The disruption of blockchain in auditing—a systematic literature review and an agenda for future research," *Accounting, Auditing & Accountability Journal*, vol. 35, no. 7, pp. 1534-1565, 2022.
- [149] H. Han, R. K. Shiwakoti, R. Jarvis, C. Mordi, and D. Botchie, "Accounting and auditing with blockchain technology and artificial Intelligence: A literature review," *International Journal of Accounting Information Systems*, vol. 48, p. 100598, 2023/03/01/ 2023, doi: <https://doi.org/10.1016/j.accinf.2022.100598>.
- [150] M. Talha, "Blockchain in accounting: Transforming transparency and security in financial records," *Dandao Xuebao/Journal of Ballistics*, vol. 36, no. 1, pp. 63-73, 2024.
- [151] D. R. N. D. S. V. D. Vanithamani M R and D. K. C. P. D. A. A. D. B. Ranjan Mishra, "Blockchain and Smart Contracts: Revolutionizing Auditing and Financial Transactions," *Journal of Informatics Education and Research*, vol. 4, no. 1, 02/22 2024, doi: 10.52783/jier.v4i1.598.
- [152] U. Nweje, "Blockchain technology for secure data integrity and transparent audit trails in cybersecurity," *Int. J. Res. Publ. Rev*, vol. 5, no. 12, pp. 4902-4916, 2024.

- [153] B. S. Tan and K. Y. Low, "Blockchain as the Database Engine in the Accounting System," *Australian Accounting Review*, vol. 29, no. 2, pp. 312-318, 2019, doi: <https://doi.org/10.1111/auar.12278>.
- [154] J. Wang, "Research on the construction of accounting information audit quality control system based on blockchain," *Secur. Priv.*, vol. 6, no. 2, p. e227, 2023.
- [155] B. Lifaldi, A. I. Hasanudin, and I. Ismawati, "The role of technology in the transformation of accounting financial audit case study of blockchain implementation in the audit process," *Journal of Applied Business, Taxation and Economics Research*, vol. 4, no. 1, pp. 24-38, 2024.
- [156] S. Sheela, A. A. Alsmady, K. Tanaraj, and I. Izani, "Navigating the future: Blockchain's impact on accounting and auditing practices," *Sustainability*, vol. 15, no. 24, p. 16887, 2023.
- [157] T. Aste, P. Tasca, and T. Di Matteo, "Blockchain technologies: The foreseeable impact on society and industry," 2017.
- [158] M. Di Pierro, "What is the blockchain?," *Computing in Science & Engineering*, vol. 19, no. 5, pp. 92-95, 2017.
- [159] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.
- [160] A. Hazra, A. Alkhayyat, and M. Adhikari, "Blockchain-aided Integrated Edge Framework of Cybersecurity for Internet of Things," *IEEE Consum. Electron. Mag.*, vol. PP, pp. 1-1, 01/06 2022, doi: 10.1109/MCE.2022.3141068.
- [161] S. Huckle and M. White, "Socialism and the Blockchain," *Future Internet*, vol. 8, no. 4, p. 49, 2016.
- [162] P. Yeoh, "Regulatory issues in blockchain technology," *Journal of Financial Regulation and Compliance*, 2017.
- [163] D. Magazzeni, P. McBurney, and W. Nash, "Validation and verification of smart contracts: A research agenda," *Computer*, vol. 50, no. 9, pp. 50-57, 2017.
- [164] V. Buterin, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, pp. 2-1, 2014.
- [165] N. Kshetri, "Will blockchain emerge as a tool to break the poverty chain in the Global South?," *Third World Quarterly*, vol. 38, no. 8, pp. 1710-1732, 2017.
- [166] S. Manski, "Building the blockchain world: Technological commonwealth or just more of the same?," *Strategic Change*, vol. 26, no. 5, pp. 511-522, 2017.
- [167] A. A. Umarovich, V. N. Gennadyevna, A. O. Vladimirovna, and S. R. Alexandrovich, "Block chain and financial controlling in the system of technological provision of large corporations' economic security," 2017.

- [168] B. Scott, J. Loonam, and V. Kumar, "Exploring the rise of blockchain technology: Towards distributed collaborative organizations," *Strategic Change*, vol. 26, no. 5, pp. 423-428, 2017.
- [169] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134-117151, 2019.
- [170] N. Minichiello, "Deloitte launches Rubix, a one stop blockchain software platform," *Available at*, 2015.
- [171] S. Mahmood, M. Chadhar, and S. Firmin, "Cybersecurity Challenges in Blockchain Technology: A Scoping Review," *Hum. Behav. Emerg. Tech.*, vol. 2022, p. 7384000, 2022/04/05 2022, doi: 10.1155/2022/7384000.
- [172] E. Mbunge, B. Akinnuwesi, S. G. Fashoto, A. S. Metfula, and P. Mashwama, "A critical review of emerging technologies for tackling COVID-19 pandemic," *Hum. Behav. Emerg. Tech.*, vol. 3, no. 1, pp. 25-39, 2021. [Online]. Available: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7753602/pdf/HBE2-3-25.pdf>.
- [173] A. Pal, C. K. Tiwari, and N. Halder, "Blockchain for business management: Applications, challenges and potentials," *The Journal of High Technology Management Research*, vol. 32, no. 2, p. 100414, 2021.
- [174] T. Hewa, M. Ylianttila, and M. Liyanage, "Survey on blockchain based smart contracts: Applications, opportunities and challenges," *Journal of Network and Computer Applications*, vol. 177, p. 102857, 2021.
- [175] H. Lu, K. Huang, M. Azimi, and L. Guo, "Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks," *IEEE Access*, vol. 7, pp. 41426-41444, 2019.
- [176] M. Gimenez-Aguilar, J. M. de Fuentes, L. Gonzalez-Manzano, and D. Arroyo, "Achieving cybersecurity in blockchain-based systems: A survey," *Future Generation Computer Systems*, vol. 124, pp. 91-118, 2021/11/01/ 2021, doi: <https://doi.org/10.1016/j.future.2021.05.007>.
- [177] G. Greenspan, "Avoiding the pointless blockchain project," *Online at* <https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project>, 2015.
- [178] D. A. Chopra, "Blockchain technology in food industry ecosystem," *IOP Conference Series: Materials Science and Engineering*, vol. 872, p. 012005, 06/27 2020, doi: 10.1088/1757-899X/872/1/012005.
- [179] D. Dasgupta, Z. Akhtar, and S. Sen, "Machine learning in cybersecurity: a comprehensive survey," *The Journal of Defense Modeling and Simulation*, vol. 19, no. 1, pp. 57-106, 2022, doi: 10.1177/1548512920951275.
- [180] M. Pilkington, "Blockchain technology: principles and applications," in *Research handbook on digital transformations*: Edward Elgar Publishing, 2016.

- [181] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "{Bitcoin-NG}: A scalable blockchain protocol," in *13th USENIX symposium on networked systems design and implementation (NSDI 16)*, 2016, pp. 45-59.
- [182] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292-2303, 2016.
- [183] A. K. Tyagi, S. Chandrasekaran, and N. Sreenath, "Blockchain Technology:—A New Technology for Creating Distributed and Trusted Computing Environment," in *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, 2022: IEEE, pp. 1348-1354.
- [184] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security Services Using Blockchains: A State of the Art Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 858-880, 2019, doi: 10.1109/COMST.2018.2863956.
- [185] C. Paulsen and P. Toth, "Small business information security: The fundamentals," National Institute of Standards and Technology, 2016.
- [186] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "NIST special publication 800-57," *NIST Special publication*, vol. 800, no. 57, pp. 1-142, 2007.
- [187] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Draft nist special publication 800-63-3 digital identity guidelines," *National Institute of Standards and Technology, Los Altos, CA*, 2017.
- [188] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," presented at the Proceedings of the 2012 ACM conference on Computer and communications security, Raleigh, North Carolina, USA, 2012. [Online]. Available: <https://doi.org/10.1145/2382196.2382292>.
- [189] P. Grover, A. K. Kar, and Y. K. Dwivedi, "Understanding artificial intelligence adoption in operations management: insights from the review of academic literature and social media discussions," *Ann. Oper. Res.*, pp. 1-37, 2020.
- [190] R. L. Thompson, C. A. Higgins, and J. M. Howell, "Personal computing: toward a conceptual model of utilization," *MIS Q.*, vol. 15, no. 1, pp. 125–143, 1991, doi: 10.2307/249443.
- [191] A. Deshmukh, N. Sreenath, A. K. Tyagi, and U. V. E. Abhichandan, "Blockchain Enabled Cyber Security: A Comprehensive Survey," in *2022 International Conference on Computer Communication and Informatics (ICCCI)*, 2022: IEEE, pp. 1-6.
- [192] Z. Liu *et al.*, "A survey on applications of game theory in blockchain," *arXiv preprint arXiv:1902.10865*, 2019.
- [193] J.-L. Richet and I. de Paris, "Developing a cybersecurity culture to influence employee behavior," 2022.
- [194] J.-L. Richet, "Trends in Cybercrime: Cases the Banking Sector," BPI France, 2021.

- [195] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, 25-30 June 2017 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85. [Online]. Available: <https://ieeexplore.ieee.org/document/8029379/>
- [196] C. Yu, W. Yang, F. Xie, and J. He, "Technology and Security Analysis of Cryptocurrency Based on Blockchain," *Complexity*, vol. 2022, p. 5835457, 2022/07/21 2022, doi: 10.1155/2022/5835457.
- [197] F. Xiaohua, C. Marc, E. Elias, and H. Khalid, "Artificial intelligence and Blockchain for future cyber security application," in *2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCCom/CyberSciTech)*, 2021: IEEE, pp. 802-805.
- [198] A. Asante and X. Feng, "Content-based technical solution for cyberstalking detection," in *2021 3rd International Conference on Computer Communication and the Internet (ICCCI)*, 2021: IEEE, pp. 89-95.
- [199] X. Feng, Y. Feng, and A. Asante, "A systematic approach of impact of GDPR in PII and privacy," 2021.
- [200] D. Yermack, "Corporate Governance and Blockchains," *Review of Finance*, p. rfw074, 2017, doi: 10.1093/rof/rfw074.
- [201] J. Drew, E. Asgeirsson, and R. Quaranta, "Where accounting really stands with blockchain," *Journal of Accountancy*, 2020.
- [202] P. Institute, "Cost of a data breach report 2020,". 2020.
- [203] A. Farion, O. Dluhopolskyi, S. Banakh, N. Moskaliuk, M. Farion, and Y. Ivashuk, "Using blockchain Technology for Boost Cyber Security," in *2019 9th International Conference on Advanced Computer Information Technologies (ACIT)*, 5-7 June 2019 2019: IEEE, pp. 452-455, doi: 10.1109/ACITT.2019.8780019. [Online]. Available: <https://ieeexplore.ieee.org/document/8780019/>
- [204] S. K. Jindal, R. Patra, A. Paul, S. Banerjee, and S. M. N. Islam, "Chapter 15 - Artificial Intelligence In Finance: Transformations In Financial Technologies," in *Computational Methods for Optimizing Manufacturing Technology*, 2022, S. K. Jindal, R. Patra, A. Paul, S. Banerjee, and S. M. N. Islam Eds., 2022.
- [205] S. Mohanty, K. C. Rath, and O. P. Jena, "Implementation of Total Productive Maintenance (TPM) in the Manufacturing Industry for Improving Production Effectiveness," in *Industrial Transformation*: CRC Press, 2022, pp. 45-60.

- [206] A. B. Gadicha, V. B. Gadicha, and O. P. Jena, "A Mechanism to Protect Decentralized Transactions Using Blockchain Technology," in *Machine Learning Adoption in Blockchain-Based Intelligent Manufacturing*: CRC Press, 2022, pp. 171-186.
- [207] C. Liu, V. Muravskiy, and W. Wei, "Evolution of blockchain accounting literature from the perspective of CiteSpace (2013–2023)," *Heliyon*, vol. 10, no. 11, 2024, doi: 10.1016/j.heliyon.2024.e32097.
- [208] H. Weigand, I. Blums, and J. d. Kruijff, "Shared Ledger Accounting — Implementing the Economic Exchange pattern," *Inf. Syst.*, vol. 90, p. 101437, 2020/05/01/ 2020, doi: <https://doi.org/10.1016/j.is.2019.101437>.
- [209] A. Bahga and V. K. Madiseti, "Blockchain Platform for Industrial Internet of Things," *Journal of Software Engineering and Applications*, vol. 09, no. 10, pp. 533-546, 2016, doi: 10.4236/jsea.2016.910036.
- [210] N. Atzei, M. Bartoletti, and T. Cimoli, "A Survey of Attacks on Ethereum Smart Contracts (SoK)," Springer Berlin Heidelberg, 2017, pp. 164-186.
- [211] M. Liu, A. Robin, K. Wu, and J. Xu, "Blockchain's Impact on Accounting and Auditing: A Use Case on Supply Chain Traceability," *Journal of Emerging Technologies in Accounting*, vol. 19, no. 2, pp. 105-119, 2022, doi: 10.2308/jeta-2021-002.
- [212] D. J. Ghode, V. Yadav, R. Jain, and G. Soni, "Integrated framework for supply chain with blockchain technology: a manufacturers' perspective," *Journal of Innovation and Entrepreneurship*, vol. 14, no. 1, p. 62, 2025/06/13 2025, doi: 10.1186/s13731-025-00553-1.
- [213] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consum. Electron. Mag.*, vol. 7, no. 2, pp. 18-21, 2018.
- [214] J. G. Coyne and P. L. McMickle, "Can Blockchains Serve an Accounting Purpose?," *Journal of Emerging Technologies in Accounting*, vol. 14, no. 2, pp. 101-111, 2017, doi: 10.2308/jeta-51910.
- [215] M. Karajovic, H. M. Kim, and M. Laskowski, "Thinking Outside the Block: Projected Phases of Blockchain Integration in the Accounting Industry," *Australian Accounting Review*, vol. 29, no. 2, pp. 319-330, 2019, doi: 10.1111/auar.12280.
- [216] T. Yu, Z. Lin, and Q. Tang, "Blockchain: The introduction and its application in financial accounting," *Journal of Corporate Accounting & Finance*, vol. 29, no. 4, pp. 37-47, 2018.
- [217] D. Balios, P. Kotsilaras, N. Eriotis, and D. Vasiliou, "Big data, data analytics and external auditing," *Journal of Modern Accounting and Auditing*, vol. 16, no. 5, pp. 211-219, 2020.

- [218] M. A. Vasarhelyi, A. Kogan, and B. M. Tuttle, "Big data in accounting: An overview," *Accounting Horizons*, vol. 29, no. 2, pp. 381-396, 2015.
- [219] N. Kshetri, "1 Blockchain's roles in meeting key supply chain management objectives," *International Journal of information management*, vol. 39, pp. 80-89, 2018.
- [220] T. B. Herath, P. Khanna, and M. Ahmed, "Cybersecurity practices for social media users: a systematic literature review," *Journal of Cybersecurity and Privacy*, vol. 2, no. 1, pp. 1-18, 2022.
- [221] M. L. Rethlefsen *et al.*, "PRISMA-S: an extension to the PRISMA statement for reporting literature searches in systematic reviews," *Systematic reviews*, vol. 10, no. 1, pp. 1-19, 2021.
- [222] D. B. Rice, L. A. Kloda, I. Shrier, and B. D. Thombs, "Reporting completeness and transparency of meta-analyses of depression screening tool accuracy: a comparison of meta-analyses published before and after the PRISMA statement," *Journal of Psychosomatic Research*, vol. 87, pp. 57-69, 2016.
- [223] R. Sarkis-Onofre, F. Catalá-López, E. Aromataris, and C. Lockwood, "How to properly use the PRISMA Statement," *Systematic Reviews*, vol. 10, no. 1, pp. 1-3, 2021.
- [224] Y. Xiao and M. Watson, "Guidance on Conducting a Systematic Literature Review," *Journal of Planning Education and Research*, vol. 39, no. 1, pp. 93-112, 2019, doi: 10.1177/0739456x17723971.
- [225] J. Webster and R. T. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly*, vol. 26, no. 2, pp. xiii-xxiii, 2002. [Online]. Available: <http://www.jstor.org/stable/4132319>.
- [226] C. Hart, "Doing a literature review: Releasing the research imagination," 2018.
- [227] P. Grover, A. K. Kar, and M. Janssen, "Diffusion of blockchain technology: Insights from academic literature and social media analytics," *J. Enterp. Inf. Manag.*, 2019.
- [228] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *Journal of Business Research*, vol. 104, pp. 333-339, 2019/11/01/ 2019, doi: <https://doi.org/10.1016/j.jbusres.2019.07.039>.
- [229] R. F. Baumeister and M. R. Leary, "Writing Narrative Literature Reviews," *Review of General Psychology*, vol. 1, no. 3, pp. 311-320, 1997, doi: 10.1037/1089-2680.1.3.311.
- [230] D. Tranfield, D. Denyer, and P. Smart, "Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review," *British Journal of Management*, vol. 14, no. 3, pp. 207-222, 2003, doi: <https://doi.org/10.1111/1467-8551.00375>.

- [231] A. Liberati *et al.*, "The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration," *Journal of clinical epidemiology*, vol. 62, no. 10, pp. e1-e34, 2009. [Online]. Available: [https://www.jclinepi.com/article/S0895-4356\(09\)00180-2/pdf](https://www.jclinepi.com/article/S0895-4356(09)00180-2/pdf).
- [232] S. Keele, "Guidelines for performing systematic literature reviews in software engineering," Technical report, ver. 2.3 ebse technical report. ebse, 2007.
- [233] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," 2007.
- [234] F. Bartolacci, A. Caputo, A. Fradeani, and M. Soverchia, "Twenty years of XBRL: what we know and where we are going," *Meditari Accountancy Research*, 2020.
- [235] J. L. Fragoso, R. M. Peixinho, L. M. Coelho, and I. C. Paiva, "The impact of financial restatements on financial markets: a systematic review of the literature," *Meditari Accountancy Research*, vol. 28, no. 6, pp. 1119-1147, 2020.
- [236] R. Lombardi and G. Secundo, "The digital transformation of corporate reporting—a systematic literature review and avenues for future research," *Meditari Accountancy Research*, 2020.
- [237] M. Massaro, J. Dumay, and J. Guthrie, "On the shoulders of giants: undertaking a structured literature review in accounting," *Accounting, Auditing & Accountability Journal*, 2016.
- [238] D. Denyer and D. Tranfield, "Producing a systematic review," 2009.
- [239] M. Abdullahi *et al.*, "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," *Electronics*, vol. 11, no. 2, p. 198, 2022. [Online]. Available: <https://www.mdpi.com/2079-9292/11/2/198>.
- [240] S. Pahlevan-Sharif, P. Mura, and S. N. Wijesinghe, "A systematic review of systematic reviews in tourism," *Journal of Hospitality and Tourism Management*, vol. 39, pp. 158-165, 2019.
- [241] R. Knight and J. R. Nurse, "A framework for effective corporate communication after cyber security incidents," *Computers & Security*, vol. 99, p. 102036, 2020.
- [242] C. Okoli and K. Schabram, "A guide to conducting a systematic literature review of information systems research," 2010.
- [243] M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *Systematic reviews*, vol. 10, no. 1, pp. 1-11, 2021.
- [244] J. Jesson, L. Matheson, and F. M. Lacey, "Doing your literature review: Traditional and systematic techniques," 2011.
- [245] A. López-Chau, D. Valle-Cruz, and R. Sandoval-Almazán, "Sentiment analysis of Twitter data through machine learning techniques," in *Software engineering in the era of cloud computing*: Springer, 2020, pp. 185-209.

- [246] A. Booth, A. Sutton, M. Clowes, and M. Martyn-St James, "Systematic approaches to a successful literature review," 2021.
- [247] L. Waltman, N. J. Van Eck, and E. C. Noyons, "A unified approach to mapping and clustering of bibliometric networks," *Journal of informetrics*, vol. 4, no. 4, pp. 629-635, 2010.
- [248] A. Rosic, "What is blockchain technology? A step-by-step guide for beginners. Blockgeeks," ed, 2019.
- [249] V. Tiberius and S. Hirth, "Impacts of digitization on auditing: A Delphi study for Germany," *Journal of International Accounting, Auditing and Taxation*, vol. 37, p. 100288, 2019.
- [250] I. Turker and A. A. Bicer, "How to use blockchain effectively in auditing and assurance services," in *Digital Business Strategies in Blockchain Ecosystems*: Springer, 2020, pp. 457-471.
- [251] L. A. Watson and C. Mishler, "Get ready for blockchain: should management accountants add blockchain technology to their professional vocabulary?," *Strategic Finance*, vol. 98, no. 7, pp. 62-64, 2017.
- [252] H. Byström, "Blockchains, real-time accounting, and the future of credit risk modeling," *Ledger*, vol. 4, 2019.
- [253] E. Piscini, D. Dalton, and L. Kehoe, "Blockchain & cyber security," *Let's Discuss. Available online: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/IE_C_BlockchainandCyberPOV_0417.pdf (accessed on 3 March 2021)*, 2017.
- [254] L. Deloitte, "Blockchain Enigma. Paradox. Opportunity," *The Creative Studio at Deloitte, London J*, vol. 7969, 2016.
- [255] Deloitte, "Blockchain technology: a game-changer in accounting?," ed: Available at, 2016.
- [256] B. Deloitte, "A game changer for audit processes, 2017," ed.
- [257] T. Choithani, A. Chowdhury, S. Patel, P. Patel, D. Patel, and M. Shah, "A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking System," *Annals of Data Science*, pp. 1-33, 2022.
- [258] S. T. Aras and V. Kulkarni, "Blockchain and its applications—a detailed survey," *International Journal of Computer Applications*, vol. 180, no. 3, pp. 29-35, 2017.
- [259] T. Sun, "Applying deep learning to audit procedures: An illustrative framework," *Accounting Horizons*, vol. 33, no. 3, pp. 89-109, 2019.
- [260] N. Kroon, M. d. C. Alves, and I. Martins, "The Impacts of Emerging Technologies on Accountants' Role and Skills: Connecting to Open Innovation—A Systematic Literature Review," *Journal of Open Innovation: Technology, Market, and*

- Complexity*, vol. 7, no. 3, p. 163, 2021. [Online]. Available: <https://www.mdpi.com/2199-8531/7/3/163>.
- [261] S. Feng, W. Wang, Z. Xiong, D. Niyato, P. Wang, and S. S. Wang, "On cyber risk management of blockchain networks: A game theoretic approach," *IEEE Trans. Serv. Comput.*, vol. 14, no. 5, pp. 1492-1504, 2018.
 - [262] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Will cyber-insurance improve network security? A market analysis," in *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, 2014: IEEE, pp. 235-243.
 - [263] L. Jiang, "The use of blockchain technology in enterprise financial accounting information sharing," *PLoS One*, vol. 19, no. 2, p. e0298210, 2024, doi: 10.1371/journal.pone.0298210.
 - [264] E. Bonsón and M. Bednárová, "Blockchain and its implications for accounting and auditing," *Meditari Accountancy Research*, vol. 27, no. 5, pp. 725-740, 2019, doi: 10.1108/medar-11-2018-0406.
 - [265] S. Das, "'Big Four' Giant Deloitte Completes Successful Blockchain Audit," *CCN.com*, 2017.
 - [266] J. Kokina, R. Mancha, and D. Pachamanova, "Blockchain: Emergent industry adoption and implications for accounting," *Journal of Emerging Technologies in Accounting*, vol. 14, no. 2, pp. 91-100, 2017.
 - [267] I. Allison, "Deloitte, Libra, Accenture: The work of auditors in the age of Bitcoin 2.0 technology," *International Business Times*, 2015.
 - [268] P. J. McAliney and B. Ang, "Blockchain: business' next new 'It' technology—a comparison of blockchain, relational databases, and Google Sheets," *Int. J. Discl. Gov.*, vol. 16, no. 4, pp. 163-173, 2019.
 - [269] S. Chen, "A Machine Learning-Based Approach to Cybersecurity and Safety of Model Predictive Control Systems," Ph.D., University of California, Los Angeles, Ann Arbor, 29209327, 2022. [Online]. Available: <https://www.proquest.com/dissertations-theses/machine-learning-based-approach-cybersecurity/docview/2669095424/se-2?accountid=14844>
 - [270] D. D. Jiang, Z. H. Wang, Y. Wang, L. Z. Tan, J. Wang, and P. Y. Zhang, "A Blockchain-Reinforced Federated Intrusion Detection Architecture for IIoT," (in English), *IEEE Internet Things J.*, Article vol. 11, no. 16, pp. 26793-26805, Aug 2024, doi: 10.1109/jiot.2024.3406602.
 - [271] S. S. Bisht, G. Jain, P. Chandani, and V. M. Kapse, "Chapter 9 Transforming Education Management in the Industry 4.0 Era: Harnessing the Power of Cloud-Based Blockchain," *Topics in Artificial Intelligence Applied to Industry 4.0*, pp. 167-180, 2024.

- [272] A. M. Shamsan Saleh, "Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review," *Blockchain: Research and Applications*, vol. 5, no. 3, p. 100193, 2024/09/01/ 2024, doi: <https://doi.org/10.1016/j.bcra.2024.100193>.
- [273] S. Abdennadher, R. Grassa, A. Hareb, and A. Alfalasi, "The effects of blockchain technology on the accounting and assurance profession in the UAE: an exploratory study," (in English), *Journal of Financial Reporting and Accounting*, vol. 20, no. 1, pp. 53-71, 2022-02-24 2022, doi: <https://doi.org/10.1108/JFRA-05-2020-0151>.
- [274] D. E. O'Leary, "Open information enterprise transactions: Business intelligence and wash and spoof transactions in blockchain and social commerce," *Intelligent Systems in Accounting, Finance and Management*, vol. 25, no. 3, pp. 148-158, 2018.
- [275] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in *Banking beyond banks and money*: Springer, 2016, pp. 239-278.
- [276] K. Fanning and D. P. Centers, "Blockchain and Its Coming Impact on Financial Services," *Journal of Corporate Accounting & Finance*, vol. 27, no. 5, pp. 53-57, 2016, doi: 10.1002/jcaf.22179.
- [277] M. J. Casey and P. Vigna, "In blockchain we trust," *MIT Technology Review*, vol. 121, no. 3, pp. 10-16, 2018.
- [278] CPA and AICPA, "Blockchain technology and its potential impact on the audit and assurance profession," 2017.
- [279] KPMG, "Audit Point of View: The Blockchain Shift Will Be Seismic," 2018.
- [280] T. D. Le, T. Le-Dinh, and S. Uwizeyemungu, "Cybersecurity analytics for the enterprise environment: A systematic literature review," *Electronics*, 2025. [Online]. Available: https://depot-e.uqtr.ca/id/eprint/12007/1/LE_DINH_T_42_ED.pdf.
- [281] M. N. Hasan, M. S. I. Papel, I. H. Rasel, and S. Akter, "Enhancing financial information security through advanced predictive analytics: A PRISMA-based systematic review," *ResearchGate*, 2025. [Online]. Available: <https://www.researchgate.net/publication/394105568>.
- [282] H. S. H. Elawadly and S. Elnakeeb, "Automation and artificial intelligence in accounting: A comprehensive bibliometric analysis and future trends," *Journal of Financial Reporting and Accounting*, 2025. [Online]. Available: <https://www.emerald.com/insight/content/doi/10.1108/jfra-09-2024-0639/full/html>.
- [283] M. Mediaty, A. Indrijawati, and Y. P. Kohar, "Review of Artificial Intelligence in Accounting: Trends, Implementation and Implications," *Journal of Accounting and Financial Management*, 2024. [Online]. Available: <https://dinastires.org/JAFM/article/download/1222/888>.

- [284] B. R. Ande, "Autonomous AI Agents for Identity Governance: Enhancing Financial Security Through Intelligent Insider Threat Detection and Compliance Enforcement," Cham, 2025: Springer Nature Switzerland, in *Data Science and Big Data Analytics*, pp. 491-502.
- [285] W. Al-Shattarat, K. B. Benameur, and M. M. Mostafa, "A decade of cybersecurity research in business, management, and accounting: Bibliometric analyses and future research directions," *Cogent Business & Management*, 2025. [Online]. Available: <https://www.tandfonline.com/doi/abs/10.1080/23311975.2025.2544230>.
- [286] P. Chadha, R. Gera, Y. Sharma, and S. Dixit, "Artificial Intelligence in Cyber Security: A Bibliometric Analysis," *Applications of Artificial Intelligence in Business and Finance*, 2024. [Online]. Available: <https://www.taylorfrancis.com/chapters/edit/10.1201/9781003535133-12>.
- [287] R. Ranatunga, "Cybersecurity Governance Under Surveillance Capitalism: A Systematic Review with Business Management Insights," *ResearchGate*, 2025. [Online]. Available: <https://www.researchgate.net/publication/396357332>.
- [288] N. B. Ngobeni, N. A. Vilani, and K. Monyela, "The Face and Future of Cyberthreats: Emerging Challenges and Trends," *SSRN*, 2025. [Online]. Available: <https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5581130>.
- [289] A. R. Hasan, "Artificial Intelligence (AI) in accounting & auditing: A Literature review," *Open Journal of Business and Management*, vol. 10, no. 1, pp. 440-465, 2021.
- [290] F. Albuquerque and P. G. Dos Santos, "Recent Trends in Accounting and Information System Research: A Literature Review Using Textual Analysis Tools," *FinTech*, vol. 2, no. 2, pp. 248-274, 2023.
- [291] E. Hoxha, A. Angjeli, and F. Bombaj, "Implementation of modern information systems for automating accounting processes in the public sector: The experience of Albania," *Scientific Bulletin of Economics*, 2025. [Online]. Available: <https://economics-msu.com.ua/en/journals/tom-12-1-2025/vprovadzhennya-suchasnikh-informatsiynikh-sistem-dlya-avtomatizatsiyi-oblikovikh-protsesiv-u-derzhavnomu-sektori-dosvid-albaniyi>.
- [292] K. Dhoska and E. Spaho, "Bridging Horizons in Artificial Intelligence, Robotics, Cybersecurity, Smart Cities, and Digital Economy," 2025. [Online]. Available: <https://link.springer.com/content/pdf/10.1007/978-3-031-72029-1.pdf>.
- [293] A. Khang, "Shaping Cutting-Edge Technologies and Applications for Digital Banking and Financial Services," 2025. [Online]. Available: <https://api.taylorfrancis.com/content/books/mono/download?identifierName=doi&identifierValue=10.4324/9781003501947>.

- [294] G. Srinivas, S. Venkatesh, and I. G. Srikanth, "Tech Trend in Finance: Exploring the Technological Frontier of Fintech Valuation in Digital Epoch," *IEEE Conference on Knowledge Engineering and Communication Systems (ICKECS)*, 2025. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/11035982>.
- [295] R. Loveth and L. M. Giovanni, "Cybersecurity Challenges in Digital Accounting: Ensuring Data Integrity and Compliance," 2025. [Online]. Available: https://www.researchgate.net/publication/390662043_Cybersecurity_Challenges_in_Digital_Accounting_Ensuring_Data_Integrity_and_Compliance.
- [296] M. R. Islam, "Generative AI, Cybersecurity, and Ethics," 2024. [Online]. Available: <https://books.google.com/books?id=p8IzEQAAQBAJ>.
- [297] D. B. Garrie, L. M. Gordon, and B. Newman, "Uncovering Digital Evidence," 2024. [Online]. Available: <https://link.springer.com/content/pdf/10.1007/978-3-031-68118-9.pdf>.
- [298] F. T. Zohora, S. Akter, and I. Rasul, "The Role of Threat Intelligence in Preventing Financially Motivated Cyberattacks," *Journal of Engineering, Computing and Intelligent Research*, 2025. [Online]. Available: <https://jecir.com/index.php/jecir/article/download/24/38>.
- [299] P. B. de Laat, "Algorithmic decision-making employing profiling: will trade secrecy protection render the right to explanation toothless?," *Ethics and Information Technology*, vol. 24, no. 2, p. 17, 2022/04/05 2022, doi: 10.1007/s10676-022-09642-1.
- [300] D. A. Appelbaum, A. Kogan, and M. A. Vasarhelyi, "Analytical procedures in external auditing: A comprehensive literature survey and framework for external audit analytics," *Journal of Accounting Literature*, vol. 40, no. 1, pp. 83-101, 2018.
- [301] S. G. Sutton, M. Holt, and V. Arnold, "'The reports of my death are greatly exaggerated'—Artificial intelligence research in accounting," *International Journal of Accounting Information Systems*, vol. 22, pp. 60-73, 2016.
- [302] J. P. M. Henriques, "Audit Compliance and Forensics Frameworks for Improved Critical Infrastructure Protection," *University of Coimbra*, 2024. [Online]. Available: https://estudogeral.uc.pt/bitstream/10316/115446/1/Thesis_Audit_Compliance_and_Forensics_Frameworks_for_Improved_Critical_Infrastructure_Protection_FINAL.pdf.
- [303] O. Eltayeb, "The Crucial Significance of Governance, Risk and Compliance in Identity and Access Management," *Journal of Ecohumanism*, vol. 3, no. 4, pp. 2395-2405, 2024.
- [304] R. H. Chowdhury, "Cybersecurity Accounting Frameworks for Critical Infrastructure Protection: Integrating Advanced Accounting Systems and Cybersecurity Protocols to Safeguard National Financial Data," *International Journal of Management and*

- Organizational Research*, 2022. [Online]. Available: https://www.researchgate.net/publication/392656581_Cybersecurity_Accounting_Frameworks_for_Critical_Infrastructure_Protection_Integrating_Advanced_Accounting_Systems_and_Cybersecurity_Protocols_to_Safeguard_National_Financial_Data.
- [305] H. Taherdoost, "Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview," *Electronics*, vol. 11, no. 14, p. 2181, 2022.
 - [306] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," *Computers & Security*, vol. 98, p. 102003, 2020/11/01/ 2020, doi: <https://doi.org/10.1016/j.cose.2020.102003>.
 - [307] R. Guidotti, A. Monreale, S. Ruggieri, F. Turini, F. Giannotti, and D. Pedreschi, "A survey of methods for explaining black box models," *ACM computing surveys (CSUR)*, vol. 51, no. 5, pp. 1-42, 2018.
 - [308] H. Liazid, M. Lehsaini, and A. Liazid, "Data transmission reduction using prediction and aggregation techniques in IoT-based wireless sensor networks," *Journal of Network and Computer Applications*, vol. 211, p. 103556, 2023/02/01/ 2023, doi: <https://doi.org/10.1016/j.jnca.2022.103556>.
 - [309] S. De Haes and W. Van Grembergen, "Enterprise governance of IT," in *Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5*: Springer, 2015, pp. 11-43.
 - [310] K. Jaggi, "Advancing Cybersecurity Strategies: Balancing Threat Detection, Compliance, and Resilient Architectures," *SSRN Electronic Journal*, 2025. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5124287.
 - [311] A. O. Ikudabo, K. C. Nwafor, and C. C. Onyeje, "Mitigating cybersecurity risks in financial institutions: The role of AI and data analytics," *International Journal of Finance & Technology*, 2024. [Online]. Available: <https://www.researchgate.net/publication/385217807>.
 - [312] A. O. O. O. A. M. Ajayi, "Detecting Insider Threats in Banking Using AI-Driven Anomaly Detection," *Journal of Cybersecurity Intelligence*, 2024. [Online]. Available: <https://www.researchgate.net/publication/386276456>.
 - [313] H. Blake, "AI in Cybersecurity for Financial Institutions: Threat Detection and Prevention," *Journal of Financial Security Studies*, 2024. [Online]. Available: <https://www.researchgate.net/publication/389466057>.
 - [314] O. E. Ejiofor, "A Comprehensive Framework for Strengthening Financial Cybersecurity," *European Journal of Computer Science and Information Technology*, 2024. [Online]. Available: <https://www.researchgate.net/publication/381548436>.
 - [315] A. O. Omokanye, A. M. Ajayi, O. Olowu, A. O. Adeleye, E. C. Chianumba, and O. M. Omole, "AI-powered financial crime prevention with cybersecurity, IT, and data

- science in modern banking," *International Journal of Science and Research Archive*, vol. 13, no. 3, 2024.
- [316] I. P. I. G. I. E. O. M. Ijiga, "Harnessing Adversarial Machine Learning for Threat Detection," *Journal of Scientific Computing and Cyber Risk*, 2024. [Online]. Available: <https://www.researchgate.net/publication/380459159>.
 - [317] A. L. P. Gómez, L. F. Maimó, A. H. Celdrán, and F. J. G. Clemente, "VAASI: Crafting valid and abnormal adversarial samples for anomaly detection systems in industrial scenarios," (in English), *Journal of Information Security and Applications*, Article vol. 79, p. 13, Dec 2023, Art no. 103647, doi: 10.1016/j.jisa.2023.103647.
 - [318] V. Business, "2025 Data Breach Investigations Report," Verizon Business, 2025. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir/>
 - [319] E. U. A. f. Cybersecurity, "ENISA Threat Landscape 2024," European Union Agency for Cybersecurity, 2024. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf
 - [320] G. Noto. "Scammers siphon \$25M from engineering firm Arup via AI deepfake 'CFO'." <https://www.cfodive.com/news/scammers-siphon-25m-engineering-firm-arup-deepfake-cfo-ai/716501/> (accessed.
 - [321] G. Plimmer and K. Wiggins, *Arup lost \$25mn in Hong Kong deepfake video conference scam*. 2024.
 - [322] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in *2008 eighth ieee international conference on data mining*, 2008: IEEE, pp. 413-422.
 - [323] J. Zou, J. Zhang, and P. Jiang, "Credit card fraud detection using autoencoder neural network," *arXiv preprint arXiv:1908.11553*, 2019.
 - [324] N. Rosley, G.-K. Tong, K.-H. Ng, S. N. Kalid, and K.-C. Khor, "Autoencoders with reconstruction error and dimensionality reduction for credit card fraud detection," in *International Conference on Computer, Information Technology and Intelligent Computing (CITIC 2022)*, 2022: Atlantis Press, pp. 503-512.
 - [325] Y. Zhang and B. Duan, "Accounting Data Anomaly Detection and Prediction Based on Self-supervised Learning," *Front. Appl. Math. Stat.*, vol. 11, p. 1628652, 2025.
 - [326] A. Gueriani, H. Kheddar, and A. C. Mazari, "Deep reinforcement learning for intrusion detection in IoT: A survey," in *2023 2nd International Conference on Electronics, Energy and Measurement (IC2EM)*, 2023, vol. 1: IEEE, pp. 1-7.
 - [327] A. H. Ali *et al.*, "Unveiling machine learning strategies and considerations in intrusion detection systems: a comprehensive survey," *Front. Comput. Sci.-Switz*, vol. 6, p. 1387354, 2024.

- [328] I. Grissa and E. Abaoub, "Machine Learning for Anomaly Detection in Accounting Records: A Comprehensive Study," *International Journal For Multidisciplinary Research*, 2024-02-27 2024, doi: 10.36948/ijfmr.2024.v06i01.13477.
- [329] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," *arXiv preprint arXiv:1412.6572*, 2014.
- [330] S. Jang, S. Li, and Y. Sung, "Generative Adversarial Network for Global Image-Based Local Image to Improve Malware Classification Using Convolutional Neural Network," (in English), *Appl. Sci.-Basel*, Article vol. 10, no. 21, p. 14, Nov 2020, Art no. 7585, doi: 10.3390/app10217585.
- [331] S. M. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," in *Advances in Neural Information Processing Systems*, 2017, vol. 30.
- [332] M. T. Ribeiro, S. Singh, and C. Guestrin, "" Why should i trust you?" Explaining the predictions of any classifier," in *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining*, 2016, pp. 1135-1144.
- [333] L. Tornatzky and M. Fleischer, "The process of technology innovation, Lexington, MA," ed: Lexington books, 1990.
- [334] Y. K. Dwivedi, L. Hughes, A. K. Kar, A. M. Baabdullah, P. Grover, and R. Abbas, "Artificial intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice, and policy," *International Journal of Information Management*, vol. 57, p. 101994, 2019, doi: 10.1016/j.ijinfomgt.2019.08.002.
- [335] J. Kinyua and L. Awuah, "AI/ML in Security Orchestration, Automation and Response: Future Research Directions," *Intelligent Automation & Soft Computing*, vol. 28, no. 2, 2021.
- [336] H. Felemban, M. Sohail, and K. Ruikar, "Exploring the Readiness of Organisations to Adopt Artificial Intelligence," *Buildings*, vol. 14, no. 8, p. 2460, 2024. [Online]. Available: <https://www.mdpi.com/2075-5309/14/8/2460>.
- [337] M. Alles and G. L. Gray, ""The first mile problem": Deriving an endogenous demand for auditing in blockchain-based business processes," *International Journal of Accounting Information Systems*, vol. 38, p. 100465, 2020/09/01/ 2020, doi: <https://doi.org/10.1016/j.accinf.2020.100465>.
- [338] S. Raisch and S. Krakowski, "Artificial intelligence and management: The automation–augmentation paradox," *Academy of management review*, vol. 46, no. 1, pp. 192-210, 2021.
- [339] R. Setiawati, A. Kusmara, and T. Kuusk, "Managing Transparency Fairness Accountability in AI for Sustainable Human Resource Management," in *2025 4th International Conference on Creative Communication and Innovative Technology (ICCIT)*, 15-16 Aug. 2025 2025, pp. 1-7, doi: 10.1109/ICCIT65724.2025.11166968.

- [340] K. Owusu Kwateng, C. Amanor, and F. Tetteh, "Enterprise risk management and information technology security in the financial sector. *Information & Computer Security*, 30 (3), 422-451," ed, 2022.
- [341] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "RESEARCH METHODS & REPORTING-Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement-David Moher and colleagues introduce PRISMA, an update of the QUOROM guidelines for reporting systematic reviews and meta-analyses," *BMJ (CR)-print*, vol. 338, no. 7716, p. 332, 2009.
- [342] C. Okoli, "A guide to conducting a standalone systematic literature review," *Communications of the association for information systems*, vol. 37, 2015.
- [343] B. Kitchenham, "Procedures for Performing Systematic Reviews," *Keele, UK, Keele Univ.*, vol. 33, 08/01 2004.
- [344] A. S. Dina, M. A. B. Siddique, and D. Manivannan, "A Deep Learning approach for intrusion detection in Internet of Things using focal loss function," *Internet of Things*, vol. 22, 2023// 2023, doi: 10.1016/j.iot.2023.100699.
- [345] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41-50, 2018, doi: 10.1109/TETCI.2017.2772792.
- [346] R. R. Moeller, *COSO enterprise risk management: understanding the new integrated ERM framework*. John Wiley & Sons, 2007.
- [347] S. Mishra, "Exploring the impact of AI-based cyber security financial sector management," *Applied Sciences*, vol. 13, no. 10, p. 5875, 2023.
- [348] D. Appelbaum and R. Nehmer, "Designing and auditing accounting systems based on blockchain and distributed ledger principles," *Feliciano School of Business*, pp. 1-19, 2017.
- [349] H. BENNASAR, M. ESSAAIDI, A. BENDAHMANE, and J. BEN-OTHTMAN, "A Systematic Literature Review of Cloud Computing Cybersecurity," *Advances in Dynamical Systems and Applications*, vol. 16, no. 2, pp. 1883-1919, 2021.
- [350] M. D. A. M. Jony, M. S. Arafat, R. Islam, S. M. S. Rafi, M. S. Jalil, and F. Hossen, "AI-Powered Cybersecurity in Financial Institutions: Enhancing Resilience Against Emerging Digital Threats," *Advanced International Journal of Multidisciplinary Research*, 2024, doi: 10.62127/aijmr.2024.v02i06.1113.
- [351] F. Arute *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505-510, 2019.
- [352] E. Haapamäki and J. Sihvonen, "Cybersecurity in Accounting Research," Routledge, 2022, pp. 182-214.

- [353] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, 1994: Ieee, pp. 124-134.
- [354] A. Dwivedi, G. K. Saini, and U. I. Musa, "Cybersecurity and Prevention in the Quantum Era," in *2023 2nd International Conference for Innovation in Technology, INOCON 2023*, 2023: Institute of Electrical and Electronics Engineers Inc., doi: 10.1109/INOCON57975.2023.10101186. [Online]. Available: <https://ieeexplore.ieee.org/document/10101186>
- [355] L. Chen *et al.*, *Report on post-quantum cryptography*. US Department of Commerce, National Institute of Standards and Technology ..., 2016.
- [356] R. Böhme and G. Schwartz, "Modeling cyber-insurance: towards a unifying framework," in *WEIS*, 2010.
- [357] D. J. Bernstein, "Post-quantum cryptography," in *Encyclopedia of Cryptography, Security and Privacy*: Springer, 2025, pp. 1846-1847.
- [358] KPMG, "Quantum is coming — and bringing new cybersecurity threats with it," 2024. [Online]. Available: <https://kpmg.com/xx/en/our-insights/ai-and-technology/quantum-and-cybersecurity.html#:~:text=KPMG%20in%20Germany%20conducted%20research,5>
- [359] N. Abdelgaber and C. Nikolopoulos, "Overview on Quantum Computing and its Applications in Artificial Intelligence," in *2020 IEEE Third International Conference on Artificial Intelligence and Knowledge Engineering (AIKE)*, 9-13 Dec. 2020 2020, pp. 198-199, doi: 10.1109/AIKE48582.2020.00038. [Online]. Available: <https://ieeexplore.ieee.org/document/9355449/>
- [360] S. Rubinstein-Salzedo, *Cryptography*. Springer, 2018.
- [361] K. Denker and A. Y. Javaid, "Quantum Computing as a Threat to Modern Cryptography Techniques," ed. Athens: The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2019, pp. 3-8.
- [362] O. G. Abood and S. K. Guirguis, "A survey on cryptography algorithms," *International Journal of Scientific and Research Publications*, vol. 8, no. 7, pp. 495-516, 2018.
- [363] S. Dutta, B. Lanvin, and S. Wunsch-Vincent, "Global Innovation Index 2018: Energizing the World with Innovation," World Intellectual Property Organization (WIPO), INSEAD, and Cornell University, 2018. [Online]. Available: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2018.pdf
- [364] G. C. Index, "URL: <https://www.itu.int/en/ITU-D/Cybersecurity>," *Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf*, 2018.

- [365] J. J. Stankovic, I. Marjanovic, S. Drezgic, and Z. Popovic, "The digital competitiveness of European countries: A multiple-criteria approach," *Journal of Competitiveness*, vol. 13, no. 2, pp. 117-134, 2021.
- [366] A. Parthasarathy, "Quantum Supremacy: Here Now, or Hype?," 2019.
- [367] B. E. Baaquie, *Quantum finance: Path integrals and Hamiltonians for options and interest rates*. Cambridge University Press, 2007.
- [368] E. E. Haven, "A discussion on embedding the Black–Scholes option pricing model in a quantum physics setting," *Physica A: Statistical Mechanics and its Applications*, vol. 304, no. 3, pp. 507-524, 2002/02/15/ 2002, doi: [https://doi.org/10.1016/S0378-4371\(01\)00568-4](https://doi.org/10.1016/S0378-4371(01)00568-4).
- [369] S. Wiesner, "Conjugate coding," *ACM Sigact News*, vol. 15, no. 1, pp. 78-88, 1983.
- [370] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7-11, 2014/12/04/ 2014, doi: <https://doi.org/10.1016/j.tcs.2014.05.025>.
- [371] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661-663, 08/05/ 1991, doi: 10.1103/PhysRevLett.67.661.
- [372] I. Buluta and F. Nori, "Quantum Simulators," *Science*, vol. 326, no. 5949, pp. 108-111, 2009, doi: doi:10.1126/science.1177838.
- [373] I. M. Georgescu, S. Ashhab, and F. Nori, "Quantum simulation," *Reviews of Modern Physics*, vol. 86, no. 1, pp. 153-185, 03/10/ 2014, doi: 10.1103/RevModPhys.86.153.
- [374] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Review*, vol. 41, no. 2, pp. 303-332, 1999, doi: 10.1137/s0036144598347011.
- [375] R. Auer, P. Haene, and H. Holden, "BIS Papers," 2021.
- [376] D. J. Egger *et al.*, "Quantum Computing for Finance: State-of-the-Art and Future Prospects," (in English), *IEEE. Trans. Quantum. Eng.*, Article vol. 1, 2020, Art no. 3101724, doi: 10.1109/TQE.2020.3030314.
- [377] S. Boyson, "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems," *Technovation*, vol. 34, no. 7, pp. 342-353, 2014.
- [378] K. Dolui, A. Suresh, and B. Nikolic, "Spin pumping from antiferromagnetic insulator spin-orbit-proximitized by adjacent heavy metal: a first-principles Floquet-nonequilibrium Green function study," (in English), *J. Phys-Mater.*, Article vol. 5, 2022-07-01 2022, Art no. 034002, doi: 10.1088/2515-7639/ac6ae6.
- [379] F. L. Greitzer and D. A. Frincke, "Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation," in *Insider threats in cyber security*: Springer, 2010, pp. 85-113.
- [380] J. R. Nurse *et al.*, "Understanding insider threat: A framework for characterising attacks," in *2014 IEEE security and privacy workshops*, 2014: IEEE, pp. 214-228.

- [381] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Reviews of Modern Physics*, vol. 89, no. 1, p. 015004, 2017.
- [382] A. Da Veiga and J. H. Eloff, "A framework and assessment instrument for information security culture," *Computers & security*, vol. 29, no. 2, pp. 196-207, 2010.
- [383] R. Rahul *et al.*, "Cybersecurity Issues and Challenges in Quantum Computing," in *Topics in Artificial Intelligence Applied to Industry 4.0*: wiley, 2024, pp. 203-221.
- [384] R. Alluhaibi, "Quantum Machine Learning for Advanced Threat Detection in Cybersecurity," (in English), *Int. J. Safety Secur. Eng.*, Article vol. 14, no. 3, pp. 875-883, 2024, doi: 10.18280/ijssse.140319.
- [385] M. R. AL-Refaey, A. K. Tyagi, A. S. A.-M. AL-Ghamdi, and S. Kukreja, *Topics in Artificial Intelligence Applied to Industry 4.0*. John Wiley & Sons, 2024.
- [386] C. M. Filipe Beato. "How pioneering public-private collaboration in the financial sector can help secure its quantum future." World Economic Forum. <https://www.weforum.org/stories/2024/11/pioneering-public-private-collaboration-financial-sector-secure-quantum-future/> via @wef (accessed 01/03/2025, 2025).
- [387] C. Easttom, "Quantum computing and cryptography," in *Modern Cryptography: Applied Mathematics for Encryption and Information Security*: Springer, 2022, pp. 397-407.
- [388] C. Figgatt, D. Maslov, K. A. Landsman, N. M. Linke, S. Debnath, and C. Monroe, "Complete 3-qubit Grover search on a programmable quantum computer," *Nat. Commun.*, vol. 8, no. 1, p. 1918, 2017.
- [389] C. Lavor, L. R. U. Manssur, and R. Portugal, "Shor's Algorithm for Factoring Large Integers," *arXiv: Quantum Physics*, 2003.
- [390] D. Brennan, "Quantum computational supremacy: Security and vulnerability in a new paradigm," *Irish Communication Review*, vol. 16, no. 1, p. 10, 2018.
- [391] I. Pitowsky, "Quantum speed-up of computations," *Philosophy of Science*, vol. 69, no. S3, pp. S168-S177, 2002.
- [392] F. Grosshans, T. Lawson, F. Morain, and B. Smith, "Factoring safe semiprimes with a single quantum query," *arXiv preprint arXiv:1511.04385*, 2015.
- [393] N. I. o. Standards and Technology. "Post-Quantum Cryptography Standardization Process." <https://csrc.nist.gov/projects/post-quantum-cryptography> (accessed.
- [394] W. H. Delone and E. R. M. and, "The DeLone and McLean Model of Information Systems Success: A Ten-Year Update," *J. Manage. Inform. Syst.*, vol. 19, no. 4, pp. 9-30, 2003/04/01 2003, doi: 10.1080/07421222.2003.11045748.
- [395] W. W. Burke and G. H. Litwin, "A Causal Model of Organizational Performance and Change," *Journal of Management*, vol. 18, no. 3, pp. 523-545, 1992, doi: 10.1177/014920639201800306.

- [396] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly*, vol. 27, no. 3, pp. 425-478, 2003, doi: 10.2307/30036540.
- [397] V. Venkatesh and H. Bala, "Technology Acceptance Model 3 and a Research Agenda on Interventions," *Decision Sciences*, vol. 39, no. 2, pp. 273-315, 2008, doi: <https://doi.org/10.1111/j.1540-5915.2008.00192.x>.
- [398] Y. J. Liu, R. Zhang, and Y. B. Zhou, "Predicate encryption against master-key tampering attacks," (in English), *Cybersecurity*, Article vol. 2, no. 1, p. 20, 2019, Art no. 22, doi: 10.1186/s42400-019-0039-6.
- [399] K. Kaneko, K. Miyamoto, N. Takeda, and K. Yoshino, "Quantum pricing with a smile: implementation of local volatility model on quantum computer," (in English), *EPJ Quantum Technol.*, Article vol. 9, no. 1, p. 32, Dec 2022, Art no. 7, doi: 10.1140/epjqt/s40507-022-00125-2.
- [400] Y. J. Chang, W. T. Wang, H. Y. Chen, S. W. Liao, and C. R. Chang, "A novel approach for quantum financial simulation and quantum state preparation," (in English), *Quant. Mach. Intell.*, Article vol. 6, no. 1, p. 17, Jun 2024, Art no. 24, doi: 10.1007/s42484-024-00160-5.
- [401] E. Dri *et al.*, "A More General Quantum Credit Risk Analysis Framework," (in English), *Entropy*, Article vol. 25, no. 4, p. 14, Apr 2023, Art no. 593, doi: 10.3390/e25040593.
- [402] S. Thakkar, S. Kazdaghli, N. Mathur, I. Kerenidis, A. J. Ferreira-Martins, and S. Brito, "Improved financial forecasting via quantum machine learning," (in English), *Quant. Mach. Intell.*, Article vol. 6, no. 1, p. 19, Jun 2024, Art no. 27, doi: 10.1007/s42484-024-00157-0.
- [403] Y. J. Chen, T. W. Lin, C. W. Kuo, and K. Y. Tsai, "An Approach of Privacy-Preserved PQC-based Cyber-threat Intelligence System," in *Proceedings - 2024 8th International Conference on Cryptography, Security and Privacy, CSP 2024*, 2024: Institute of Electrical and Electronics Engineers Inc., pp. 1-4, doi: 10.1109/CSP62567.2024.00008. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/10600647>
- [404] M. Lazirko, "Quantum Computing Standards & Accounting Information Systems," *arXiv preprint arXiv:2311.11925*, 2023.
- [405] A. Nath, S. Maity, S. Banerjee, and R. Roy, "Quantum Key Distribution (QKD) for Symmetric Key Transfer," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2024-05-15 2024, doi: 10.32628/cseit24103105.
- [406] M. Teitsma, I. Ahmed, and J. van Velzen, "Quantum Organisational Readiness Levels," *arXiv preprint arXiv:2502.16489*, 2025.

- [407] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, p. 433, 2021.
- [408] S. Umbrello, Z. Seskir, and P. E. Vermaas, "Communities of quantum technologies: Stakeholder identification, legitimation, and interaction," 2024.
- [409] M. D. Adegbola, A. E. Adegbola, P. Amajuoyi, L. B. Benjamin, and K. B. Adeusi, "Quantum computing and financial risk management: A theoretical review and implications," *Computer Science & IT Research Journal*, 2024-06-07 2024, doi: 10.51594/csitrj.v5i6.1194.
- [410] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," presented at the Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984.
- [411] S. Pirandola *et al.*, "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012-1236, 2020. [Online]. Available: <https://doi.org/10.1364/AOP.361502>.
- [412] "The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration," *Annals of Internal Medicine*, vol. 151, no. 4, pp. W-65-W-94, 2009, doi: 10.7326/0003-4819-151-4-200908180-00136 %m 19622512.
- [413] E. M. Antman, J. Lau, B. Kupelnick, F. Mosteller, and T. C. Chalmers, "A comparison of results of meta-analyses of randomized control trials and recommendations of clinical experts: treatments for myocardial infarction," *Jama*, vol. 268, no. 2, pp. 240-248, 1992.
- [414] A. D. Oxman and G. H. Guyatt, "The science of reviewing research a," *Annals of the New York Academy of Sciences*, vol. 703, no. 1, pp. 125-134, 1993.
- [415] G. Lame, "Systematic Literature Reviews: An Introduction," *Proceedings of the Design Society: International Conference on Engineering Design*, vol. 1, no. 1, pp. 1633-1642, 2019, doi: 10.1017/dsi.2019.169.
- [416] M. Petticrew, "Systematic reviews from astronomy to zoology: myths and misconceptions," *Bmj*, vol. 322, no. 7278, pp. 98-101, 2001.
- [417] L. Bunesu and A. M. Vârtei, "Modern finance through quantum computing —A systematic literature review," (in English), *PLoS One*, Article vol. 19, no. 7 July, 2024, Art no. e0304317, doi: 10.1371/journal.pone.0304317.
- [418] R. Van Dinter, B. Tekinerdogan, and C. Catal, "Automation of systematic literature reviews: A systematic literature review," *Information and Software Technology*, vol. 136, p. 106589, 2021.
- [419] B. Barn, S. Barat, and T. Clark, "Conducting systematic literature reviews and systematic mapping studies," in *Proceedings of the 10th Innovations in Software Engineering Conference*, 2017, pp. 212-213.

- [420] J. Ramey and P. G. Rao, "The systematic literature review as a research genre," in *2011 IEEE International Professional Communication Conference*, 2011: IEEE, pp. 1-7.
- [421] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and P. Group, "Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement," *International journal of surgery*, vol. 8, no. 5, pp. 336-341, 2010.
- [422] M. L. Rethlefsen *et al.*, "PRISMA-S: an extension to the PRISMA Statement for Reporting Literature Searches in Systematic Reviews," *Systematic Reviews*, vol. 10, no. 1, p. 39, 2021/01/26 2021, doi: 10.1186/s13643-020-01542-z.
- [423] A. Pollock and E. Berge, "How to do a systematic review," *International Journal of Stroke*, vol. 13, no. 2, pp. 138-156, 2018, doi: 10.1177/1747493017743796.
- [424] J. J. Shuster, "Cochrane handbook for systematic reviews for interventions, Version 5.1. 0, published 3/2011. Julian PT Higgins and Sally Green, Editors," ed: Wiley Online Library, 2011.
- [425] J. B. Institute, "Joanna Briggs Institute reviewers' manual: 2014 edition," *Australia: The Joanna Briggs Institute*, pp. 88-91, 2014.
- [426] G. Wong, T. Greenhalgh, G. Westhorp, and R. Pawson, "Development of methodological guidance, publication standards and training materials for realist and meta-narrative reviews: the RAMESES (Realist And Meta-narrative Evidence Syntheses–Evolving Standards) project," 2015.
- [427] H. G. Gurbuz and B. Tekinerdogan, "Model-based testing for software safety: a systematic mapping study," *Softw. Qual. J.*, vol. 26, no. 4, pp. 1327-1372, 2018/12/01 2018, doi: 10.1007/s11219-017-9386-2.
- [428] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," ed: UK, 2007.
- [429] W. Mengist, T. Soromessa, and G. Legese, "Ecosystem services research in mountainous regions: A systematic literature review on current knowledge and research gaps," *Sci. Total Environ.*, vol. 702, p. 134581, 2020.
- [430] W. Mengist, T. Soromessa, and G. Legese, "Method for conducting systematic literature review and meta-analysis for environmental science research," *MethodsX*, vol. 7, p. 100777, 2020.
- [431] M. J. Grant and A. Booth, "A typology of reviews: an analysis of 14 review types and associated methodologies," *Health information & libraries journal*, vol. 26, no. 2, pp. 91-108, 2009.
- [432] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and P. Group*, "Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement," *Annals of internal medicine*, vol. 151, no. 4, pp. 264-269, 2009. [Online]. Available: <https://renhyd.org/index.php/renhyd/article/download/114/99>.

- [433] I. F. Del Amo, J. A. Erkoyuncu, R. Roy, R. Palmarini, and D. Onoufriou, "A systematic review of Augmented Reality content-related techniques for knowledge transfer in maintenance applications," *Comput. Ind.*, vol. 103, pp. 47-71, 2018.
- [434] R. Iyer and A. Bakshi, "Artificial Intelligence and Quantum Computing Techniques for Stock Market Predictions," in *Deep Learning Tools for Predicting Stock Market Movements*: wiley, 2024, pp. 123-146.
- [435] R. Cyriac, S. Eswaran, and S. Selvarajan, "Quantum Computing in Cryptographic Systems," *International Journal of Advanced IT Research and Development*, 2024, doi: 10.69942/1920184/20240101/03.
- [436] X. Ren, "Advantages, classic models, applications and future trends of machine learning in financial industry," in *Exploring the Financial Landscape in the Digital Age - Proceedings of the International Conference on Financial Management and the Digital Economy, ICFMDE 2023*, T. A. Maurer, Ed., 2024: CRC Press/Balkema, pp. 762-767, doi: 10.1201/9781003508816-110. [Online]. Available: <https://www.taylorfrancis.com/chapters/edit/10.1201/9781003508816-110/advantages-classic-models-applications-future-trends-machine-learning-financial-industry-xiang-ren>
- [437] O. A. Ajala, C. A. Arinze, O. C. Ofodile, C. C. Okoye, and A. I. Daraojimba, "Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods," *Magna Sci. Adv. Res. Rev*, vol. 10, no. 1, pp. 321-329, 2024.
- [438] R. Vadisetty, "The Effects of Cyber Security Attacks on Data Integrity in AI," in *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)*, 23-25 Nov. 2024 2024, pp. 1-6, doi: 10.1109/ICEC59683.2024.10837148.
- [439] M. Hasan, "Quantum Cryptography for Secure Communications and the Enhancement of U.S. Cybersecurity in the Quantum Age," *Advances in Social Sciences Research Journal*, 2024-10-29 2024, doi: 10.14738/assrj.1110.17764.
- [440] G. Seiler, "Quantum Computing and the Future of Encryption," *Scholarly Review Journal*, 2024-12-30 2024, doi: 10.70121/001c.127168.
- [441] S. Gupta and V. Sharma, "Effects of Quantum computing on Businesses," in *4th International Conference on Intelligent Engineering and Management, ICIEM 2023*, 2023: Institute of Electrical and Electronics Engineers Inc., doi: 10.1109/ICIEM59379.2023.10166880. [Online]. Available: <https://ieeexplore.ieee.org/document/10166880>
- [442] A. Fortin and S. Héroux, "Limited usefulness of firm-provided cybersecurity information in institutional investors' investment analysis," (in English), *Inf. Comput. Secur.*, Article vol. 31, no. 1, pp. 108-123, Feb 2023, doi: 10.1108/ics-07-2022-0122.

- [443] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations," *Sensors*, vol. 23, no. 15, p. 6666, 2023.
- [444] G. Mamatha, N. Dimri, and R. Sinha, "Post-Quantum Cryptography: Securing Digital Communication in the Quantum Era," *arXiv preprint arXiv:2403.11741*, 2024.
- [445] H. Hadi, Y. Cao, M. Alshara, N. Ahmad, M. Riaz, and J. Li, "Quantum Computing Challenges and Impact on Cyber Security," in *DIGITAL FORENSICS AND CYBER CRIME, PT 2, ICDF2C 2023*, 2024-01-01 2024, vol. 571, pp. 333-343, doi: 10.1007/978-3-031-56583-0_22. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-56583-0_22
- [446] C. Basha, K. Murugan, T. Suresh, V. Srirenga Nachiyar, S. Athimoolam, and C. K. Pappa, "Enhancing Healthcare Data Security Using Quantum Cryptography for Efficient and Robust Encryption," *Journal of Electrical Systems*, 2024-04-13 2024, doi: 10.52783/jes.2544.
- [447] P. Uppaluri, "Quantum Computing For Financial Systems," *International Journal of Advances in Engineering and Management*, 2025-01-01 2025, doi: 10.35629/5252-0701482491.
- [448] K. Bhosale, S. Ambre, Z. Valkova-Jarvis, A. Singh, and M. Nenova, "Quantum Technology: Unleashing the Power and Shaping the Future of Cybersecurity," *2023 Eight Junior Conference on Lighting (Lighting)*, pp. 1-4, 2023-09-23 2023, doi: 10.1109/Lighting59819.2023.10299447.
- [449] J. Demski, S. FitzGerald, Y. Ijiri, Y. Ijiri, and H. Lin, "Quantum information and accounting information: Their salient features and conceptual applications," *Journal of Accounting and Public Policy*, vol. 25, pp. 435-464, 2006-07-01 2006, doi: 10.1016/J.JACCPUBPOL.2006.05.004.
- [450] A. Vaishnavi and S. Pillai, "Cybersecurity in the Quantum Era-A Study of Perceived Risks in Conventional Cryptography and Discussion on Post Quantum Methods," in *Journal of Physics: Conference Series*, K. Loganathan, M. Mohanraj, P. Sakthivel, and M. Sivakumar, Eds., 2021, vol. 1964: IOP Publishing Ltd, 4 ed., doi: 10.1088/1742-6596/1964/4/042002. [Online]. Available: <https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042002/meta>
- [451] S. Héroux and A. Fortin, "How the three lines of defense can contribute to public firms' cybersecurity effectiveness," (in English), *Int. J. Discl. Gov.*, Article; Early Access p. 20, 2024 Feb 2024, doi: 10.1057/s41310-024-00226-7.
- [452] M. Saberi Kamrposhti *et al.*, "Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data," *Heliyon*, vol. 10, 2024-05-01 2024, doi: 10.1016/j.heliyon.2024.e31406.

- [453] C. I. Michael, T.-A. Campbell, I. P. Idoko, O. U. Bemologi, A. P. Anyebe, and I. I. Odeh, "Enhancing Cybersecurity Protocols in Financial Networks through Reinforcement Learning," *International Journal of Scientific Research and Modern Technology (IJSRMT)*, 2024, doi: 10.38124/ijsrmt.v3i9.58.
- [454] V. Ganapathy, "Quantum Machine Learning for Anomaly Detection in Cyber Security Audits," *Shodh Sari-An International Multidisciplinary Journal*, 2025-01-01 2025, doi: 10.59231/sari7784.
- [455] A. S. Nanda, "The Future of Cybersecurity in Fintech: Challenges, Trends and Best Practices," *International Journal of Science and Research (IJSR)*, 2024-07-05 2024, doi: 10.21275/sr24717223220.
- [456] A. K. Bishwas and M. Sen, "Strategic Roadmap for Quantum- Resistant Security: A Framework for Preparing Industries for the Quantum Threat," *ArXiv*, vol. abs/2411.09995, 2024-11-15 2024, doi: 10.48550/arXiv.2411.09995.
- [457] M. Shaleh, "The Transformative Implications of Technology on Accounting Practices," *Advances in Management & Financial Reporting*, 2024-05-31 2024, doi: 10.60079/amfr.v2i2.278.
- [458] S. O. Dawodu, T. O. Abrahams, S. K. Ewuga, S. Kaggwa, P. U. Uwaoma, and A. O. Hassan, "Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security," *World Journal of Advanced Research and Reviews*, 2023-12-30 2023, doi: 10.30574/wjarr.2023.20.3.2691.
- [459] N. Mousa and F. Shirazi, "A survey analysis of quantum computing adoption and the paradigm of privacy engineering," *Secur. Priv.*, vol. 7, 2024-06-07 2024, doi: 10.1002/spy2.419.
- [460] J. Martens *et al.*, "Acceptance and Development of Quantum Computing in the Netherlands and Germany: Barriers and Remedies From a Multistakeholder Perspective," *IEEE Trans. Eng. Manage.*, vol. 72, pp. 62-77, 2025, doi: 10.1109/TEM.2024.3493600.
- [461] N. T. P. Dung and N. T. H. Lien, "Factors affecting the stages of management accounting evolution: The developing market research," *Journal of Governance and Regulation*, 2024, doi: 10.22495/jgrv13i2siart20.
- [462] Y. J. Chang, M. F. Sie, S. W. Liao, and C. R. Chang, "The Prospects of Quantum Computing for Quantitative Finance and Beyond," (in English), *IEEE Nanotechnol. Mag.*, Article vol. 17, no. 2, pp. 31-37, 2023, doi: 10.1109/MNANO.2023.3249501.
- [463] M. A. Islam, S. K. Hasan, S. A. Priya, A. I. Asha, and N. M. Islam, "The Impact of Quantum Computing on Financial Risk Management: A Business Perspective," *International Journal For Multidisciplinary Research*, 2024-09-26 2024, doi: 10.36948/ijfmr.2024.v06i05.28080.

- [464] A. Bhasin and M. Tripathi, "Quantum Computing at an Inflection Point: Are we Ready for a New Paradigm," *IEEE Trans. Eng. Manage.*, vol. PP, pp. 1-12, 2021, doi: 10.1109/TEM.2021.3103904.
- [465] F. Shaikh, M. Sangole, V. Pareek, P. A. Patil, D. Takale, and S. Gupta, "Quantum Cryptographic Algorithms for Securing Financial Transactions," *Computer Fraud and Security*, 2024-11-14 2024, doi: 10.52710/cfs.32.
- [466] M.-L. How and S.-M. Cheah, "Business Renaissance: Opportunities and Challenges at the Dawn of the Quantum Computing Era," *Businesses*, 2023-11-09 2023, doi: 10.3390/businesses3040036.
- [467] B. Mehta, B. Tuscai, T. R. Wang, and K. Mahady, "Responsible Quantum Readiness: A Perspective from Financial Services Organization," in *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)*, 2024, vol. 2: IEEE, pp. 71-76.
- [468] R. Rahul *et al.*, "Cybersecurity Issues and Challenges in Quantum Computing," in *Topics in Artificial Intelligence Applied to Industry 4.0*, 2024, pp. 203-221.
- [469] M. A. Mohammed, C. De-Pablos-Heredero, and J. L. Montes Botella, "A Systematic Literature Review on the Revolutionary Impact of Blockchain in Modern Business," *Applied Sciences*, vol. 14, no. 23, p. 11077, 2024.
- [470] V. Venkatesh, J. Y. Thong, and X. Xu, *MIS Quarterly*, vol. 36, no. 1, p. 157, 2012.
- [471] D. J. Huang, W. Z. Zhong, J. Zhong, D. Jiang, and H. Wu, "Optimization and Implementation of Efficient and Universal Quantum Key Distribution," (in English), *J. Electr. Comput. Eng.*, Article vol. 2020, p. 9, May 2020, Art no. 3418780, doi: 10.1155/2020/3418780.
- [472] T. R. Peltier, *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC press, 2016.
- [473] N. Batarlienè and M. Meleniakas, "Claims Solutions Using a Blockchain System in International Logistics," *Sustainability*, vol. 13, no. 7, p. 3710, 2021. [Online]. Available: <https://www.mdpi.com/2071-1050/13/7/3710>.
- [474] I. Kalderemidis, A. Farao, P. Bountakas, S. Panda, and C. Xenakis, "GTM: Game Theoretic Methodology for optimal cybersecurity defending strategies and investments," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1-9.
- [475] D. J. Janvrin and T. Wang, "Implications of cybersecurity on accounting information," *Journal of Information Systems*, vol. 33, no. 3, pp. A1-A2, 2019.
- [476] A. Attiah, M. Chatterjee, and C. C. Zou, "A Game Theoretic Approach to Model Cyber Attack and Defense Strategies," in *2018 IEEE International Conference on Communications (ICC)*, 20-24 May 2018 2018, pp. 1-7, doi:

- 10.1109/ICC.2018.8422719. [Online]. Available: <https://ieeexplore.ieee.org/document/8422719/>
- [477] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *2010 43rd Hawaii International Conference on System Sciences*, 2010: IEEE, pp. 1-10.
 - [478] A. E. Chukwudi, E. Udoka, and I. Charles, "Game theory basics and its application in cyber security," *Advances in Wireless Communications and Networks*, vol. 3, no. 4, pp. 45-49, 2017.
 - [479] Y. Wang, Y. Wang, J. Liu, Z. Huang, and P. Xie, "A Survey of Game Theoretic Methods for Cyber Security," in *2016 IEEE First International Conference on Data Science in Cyberspace (DSC)*, 13-16 June 2016 2016: IEEE, pp. 631-636, doi: 10.1109/DSC.2016.90.
 - [480] J. Jing, "Applications of Game Theory and Advanced Machine Learning Methods for Adaptive Cyberdefense Strategies in the Digital Music Industry," (in eng), *Comput Intell Neurosci*, vol. 2022, p. 2266171, 2022, doi: 10.1155/2022/2266171.
 - [481] K. Xing, A. Li, R. Jiang, and Y. Jia, "A review of apt attack detection methods and defense strategies," in *2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC)*, 2020: IEEE, pp. 67-70.
 - [482] M. N. A. Khalid, A. A. Al-Kadhimi, and M. M. Singh, "Recent developments in game-theory approaches for the detection and defense against advanced persistent threats (APTs): a systematic review," *Mathematics*, vol. 11, no. 6, p. 1353, 2023.
 - [483] K.-w. Lye and J. M. Wing, "Game strategies in network security," *Int. J. Inf. Secur.*, vol. 4, pp. 71-86, 2005.
 - [484] H. Wu, "Mixed nash equilibrium and its application in two-player zero-Sum games," *Theoretical and Natural Science*, vol. 26, pp. 158-163, 2023.
 - [485] B. C. Soper, *Non-zero-sum, adversarial detection games in network security*. University of California, Santa Cruz, 2015.
 - [486] A. Ait Temghart, M. Marwan, and M. Baslam, "Stackelberg security game for optimizing cybersecurity decisions in cloud computing," *Secur. Commun. Netw.*, vol. 2023, no. 1, p. 2811038, 2023.
 - [487] J. Paul and A. R. Criado, "The art of writing literature review: What do we know and what do we need to know?," *International Business Review*, vol. 29, no. 4, p. 101717, 2020/08/01/ 2020, doi: <https://doi.org/10.1016/j.ibusrev.2020.101717>.
 - [488] A. Kumar, J. Paul, and A. B. Unnithan, "'Masstige' marketing: A review, synthesis and research agenda," *Journal of Business Research*, vol. 113, pp. 384-398, 2020/05/01/ 2020, doi: <https://doi.org/10.1016/j.jbusres.2019.09.030>.

- [489] R. W. Palmatier, M. B. Houston, and J. Hulland, "Review articles: purpose, process, and structure," *Journal of the Academy of Marketing Science*, vol. 46, no. 1, pp. 1-5, 2018/01/01 2018, doi: 10.1007/s11747-017-0563-4.
- [490] J. Hulland and M. B. Houston, "Why systematic review papers and meta-analyses matter: an introduction to the special issue on generalizations in marketing," *Journal of the Academy of Marketing Science*, vol. 48, no. 3, pp. 351-359, 2020/05/01 2020, doi: 10.1007/s11747-020-00721-7.
- [491] D. J. Bem, "Writing a review article for Psychological Bulletin," *Psychological Bulletin*, vol. 118, no. 2, p. 172, 1995.
- [492] G. Srivastava, R. M. Parizi, and A. Dehghantanha, "The future of blockchain technology in healthcare internet of things security," *Blockchain cybersecurity, trust and privacy*, pp. 161-184, 2020.
- [493] H. Zhang, J. Tan, X. Liu, S. Huang, H. Hu, and Y. Zhang, "Cybersecurity Threat Assessment Integrating Qualitative Differential and Evolutionary Games," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 3, pp. 3425-3437, 2022.
- [494] C. T. Do *et al.*, "Game Theory for Cyber Security and Privacy," *ACM Comput. Surv.*, vol. 50, no. 2, p. Article 30, 2017, doi: 10.1145/3057268.
- [495] Q. Zhu and S. Rass, "Game theory meets network security: A tutorial," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 2163-2165.
- [496] D. Hermanowski, "Open source security information management system supporting it security audit," in *2015 IEEE 2nd International Conference on Cybernetics (Cybconf)*, 2015: IEEE, pp. 336-341.
- [497] J. Shin, S.-H. Choi, P. Liu, and Y.-H. Choi, "Unsupervised multi-stage attack detection framework without details on single-stage attacks," *Future Generation Computer Systems*, vol. 100, pp. 811-825, 2019.
- [498] A. Migdalas, "Applications of game theory in finance and managerial accounting," *Operational Research*, vol. 2, pp. 209-241, 2002.
- [499] R. Myerson, "Game Theory: Analysis of Conflict, Harvard University Press, Cambridge, MA," *London England*, 1991.
- [500] H. Gintis, *Game theory evolving: A problem-centered introduction to modeling strategic behavior*. Princeton university press, 2000.
- [501] J. von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior* (null). 1944, p. null.
- [502] D. Palko *et al.*, "Cyber Security Risk Modeling in Distributed Information Systems," *Applied Sciences*, vol. 13, no. 4, p. 2393, 2023.
- [503] J. Von Neumann and O. Morgenstern, "Theory of games and economic behavior, 2nd rev," 1947.

- [504] H. Von Stackelberg, *Market structure and equilibrium*. Springer Science & Business Media, 2010.
- [505] M. Tambe, *Security and game theory: algorithms, deployed systems, lessons learned*. Cambridge university press, 2011.
- [506] H. Alqahtani and M. Kavakli-Thorne, "Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR)," *Information*, vol. 11, no. 2, p. 121, 2020. [Online]. Available: <https://www.mdpi.com/2078-2489/11/2/121>.
- [507] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decis. Support Syst.*, vol. 86, pp. 13-23, 2016/06/01/ 2016, doi: <https://doi.org/10.1016/j.dss.2016.02.012>.
- [508] E. Ho, A. Rajagopalan, A. Skvortsov, S. Arulampalam, and M. Piraveenan, "Game Theory in Defence Applications: A Review," *Sensors*, vol. 22, no. 3, p. 1032, 2022. [Online]. Available: <https://www.mdpi.com/1424-8220/22/3/1032>.
- [509] O. O. Ogunbodede, "Game Theory Classification in Cybersecurity: A Survey," *Applied and Computational Engineering*, pp. 670-678, 2023.
- [510] Y. Yuan, F. Sun, and H. Liu, "Resilient control of cyber-physical systems against intelligent attacker: a hierarchal stackelberg game approach," *International Journal of Systems Science*, vol. 47, no. 9, pp. 2067-2077, 2016.
- [511] C. A. Kamhoua, C. D. Kiekintveld, F. Fang, and Q. Zhu, *Game theory and machine learning for cyber security*. John Wiley & Sons, 2021.
- [512] K. Wang, L. Yuan, T. Miyazaki, Y. Chen, and Y. Zhang, "Jamming and eavesdropping defense in green cyber-physical transportation systems using a Stackelberg game," *IEEE Trans. Ind. Inform.*, vol. 14, no. 9, pp. 4232-4242, 2018.
- [513] M. Zhu and S. Martinez, "Stackelberg-game analysis of correlated attacks in cyber-physical systems," in *Proceedings of the 2011 American Control Conference*, 2011: IEEE, pp. 4063-4068.
- [514] Z. Wang, H. Zhu, and L. Sun, "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods," *IEEE Access*, vol. 9, pp. 11895-11910, 2021, doi: 10.1109/ACCESS.2021.3051633.
- [515] S. Abraham and S. Nair, "Predictive cyber-security analytics framework: A non-homogenous markov model for security quantification," *arXiv preprint arXiv:1501.01901*, 2015.
- [516] S. Yi *et al.*, "Overview on attack graph generation and visualization technology," in *2013 International Conference on Anti-Counterfeiting, Security and Identification (ASID)*, 2013: IEEE, pp. 1-6.
- [517] D. Goktas, J. Zhao, and A. Greenwald, "Zero-Sum Stochastic Stackelberg Games," *ArXiv*, vol. abs/2211.13847, 2022-11-25 2022, doi: 10.48550/arXiv.2211.13847.

- [518] Y. A. Wu, H. Wu, H. S. Kang, and H. Li, "Layout Optimization of a Tidal Current Turbine Array Based on Quantum Discrete Particle Swarm Algorithm," (in English), *J. Mar. Sci. Eng.*, Article vol. 11, no. 10, p. 17, Oct 2023, Art no. 1994, doi: 10.3390/jmse11101994.
- [519] I. Sharafaldin, A. Lashkari, and A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization, 4th Int. Conf. on Information Systems Security and Privacy (ICISSP), 2018," ed.
- [520] J. Glasser and B. Lindauer, "Bridging the Gap: A Pragmatic Approach to Generating Insider Threat Data," presented at the 2013 IEEE CS Security and Privacy Workshops (SPW2013), 2013. [Online]. Available: <https://doi.ieeecomputersociety.org/10.1109/SPW.2013.37>.
- [521] M. Alazab, S. Alhyari, A. Awajan, and A. B. Abdallah, "Blockchain technology in supply chain management: an empirical study of the factors affecting user adoption/acceptance," (in English), *Cluster Comput.*, Article vol. 24, no. 1, pp. 83-101, Mar 2021, doi: 10.1007/s10586-020-03200-4.
- [522] A. Roy, D. S. Kim, and K. S. Trivedi, "Scalable optimal countermeasure selection using implicit enumeration on attack countermeasure trees," in *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012)*, 2012: IEEE, pp. 1-12.
- [523] Y. Bai, C. Jin, H. Wang, and C. Xiong, "Sample-Efficient Learning of Stackelberg Equilibria in General-Sum Games," in *Neural Information Processing Systems*, 2021.
- [524] M. B. Costa, "A review of Machine Learning Algorithms used for Cyber Attacks," 2024.
- [525] D. Kumar and K. P. Kumar, "Artificial Intelligence based Cyber Security Threats Identification in Financial Institutions Using Machine Learning Approach," in *2023 2nd International Conference for Innovation in Technology (INOCON)*, 3-5 March 2023 2023, pp. 1-6, doi: 10.1109/INOCON57975.2023.10100967.
- [526] D. P. F. Möller, "Cybersecurity in Digital Transformation," in *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*. Cham: Springer Nature Switzerland, 2023, pp. 1-70.
- [527] R. Reyes-Acosta, C. Dominguez-Baez, R. Mendoza-Gonzalez, and M. Vargas Martin, "Analysis of machine learning-based approaches for securing the Internet of Things in the smart industry: a multivocal state of knowledge review," *Int. J. Inf. Secur.*, vol. 24, no. 1, p. 31, 2024/11/26 2024, doi: 10.1007/s10207-024-00935-8.
- [528] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and T. Sohail, "The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities," *Journal of Accounting and Public Policy*, vol. 25, no. 5, pp. 503-530, 2006.

- [529] W. G. No and M. A. Vasarhelyi, "Cybersecurity and continuous assurance," *Journal of Emerging Technologies in Accounting*, vol. 14, no. 1, pp. 1-12, 2017.
- [530] S. Duary, P. Choudhury, S. Mishra, V. Sharma, D. D. Rao, and A. P. Aderemi, "Cybersecurity Threats Detection in Intelligent Networks using Predictive Analytics Approaches," in *2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM)*, 21-23 Feb. 2024 2024, pp. 1-5, doi: 10.1109/ICIPTM59628.2024.10563348.
- [531] I. H. Sarker, H. Janicke, A. Mohsin, A. Gill, and L. Maglaras, "Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects," *ICT Express*, vol. 10, no. 4, pp. 935-958, 2024/08/01/ 2024, doi: <https://doi.org/10.1016/j.ict.2024.05.007>.
- [532] M. A. Talukder *et al.*, "Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction," *J. Big Data*, vol. 11, no. 1, p. 33, 2024.
- [533] I. H. Sarker, A. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *J. Big Data*, vol. 7, pp. 1-29, 2020.
- [534] M. A. Talukder *et al.*, "A dependable hybrid machine learning model for network intrusion detection," *Journal of Information Security and Applications*, vol. 72, p. 103405, 2023.
- [535] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT security: current solutions and future challenges," *IEEE Commun. Surv. Tutor.*, vol. 22, pp. 1686-1721, 2020// 2020, doi: 10.1109/COMST.2020.2986444.
- [536] S. Mishra and A. K. Tyagi, "The role of machine learning techniques in internet of things-based cloud applications," *Artificial intelligence-based internet of things systems*, pp. 105-135, 2022.
- [537] W. Suyono, E. Puspa, S. Anugrah, and R. Firnanda, "Artificial Intelligence in Auditing: A Systematic Review of Tools, Applications, and Challenges," *RIGGS: Journal of Artificial Intelligence and Digital Business*, vol. 4, pp. 3393-3401, 06/18 2025, doi: 10.31004/riggs.v4i2.1024.
- [538] R. P. Bostrom and J. S. Heinen, "MIS Problems and Failures: A Socio- Technical Perspective: Part I: The Causes," *Management Information Systems Quarterly*, vol. 1, no. 3, pp. 17-32, 1977, doi: 10.2307/248710.
- [539] M. R. Faraji, F. Shikder, M. H. Hasan, M. M. Islam, and U. K. Akter, "Examining the role of artificial intelligence in cyber security (CS): A systematic review for preventing prospective solutions in financial transactions," *International Journal*, vol. 5, no. 10, pp. 4766-4782, 2024.

- [540] Y. Zhang, F. Xiong, Y. Xie, X. Fan, and H. Gu, "The impact of artificial intelligence and blockchain on the accounting profession," *IEEE Access*, vol. 8, pp. 110461-110477, 2020.
- [541] A. Adewumi, S. Ewim, N. Sam-Bulya, and O. Ajani, "Enhancing financial fraud detection using adaptive machine learning models and business analytics," *International Journal of Scientific Research Updates*, vol. 8, no. 02, pp. 012-021, 2024.
- [542] M. A. K. Achakzai and J. Peng, "Detecting financial statement fraud using dynamic ensemble machine learning," *International Review of Financial Analysis*, vol. 89, p. 102827, 2023/10/01/ 2023, doi: <https://doi.org/10.1016/j.irfa.2023.102827>.
- [543] M. Zhu, Y. Zhang, Y. Gong, C. Xu, and Y. Xiang, "Enhancing credit card fraud detection a neural network and smote integrated approach," *arXiv preprint arXiv:2405.00026*, 2024.
- [544] S. Ramzan and M. Lokanan, "The application of machine learning to study fraud in the accounting literature," *Journal of Accounting Literature*, vol. 47, no. 3, pp. 570-596, 2024, doi: 10.1108/jal-11-2022-0112.
- [545] N. K. Athukorale *et al.*, "Evaluating Advanced Cybersecurity Technologies for Cloud Environments," 2025.
- [546] S. AlBenJasim, T. Dargahi, H. Takruri, and R. Al-Zaidi, "FinTech Cybersecurity Challenges and Regulations: Bahrain Case Study," *J. Comput. Inf. Syst.*, vol. 64, no. 6, pp. 835-851, 2024/11/01 2024, doi: 10.1080/08874417.2023.2251455.
- [547] A. Morshed and L. T. Khrais, "Cybersecurity in Digital Accounting Systems: Challenges and Solutions in the Arab Gulf Region," *Journal of Risk and Financial Management*, vol. 18, no. 1, p. 41, 2025. [Online]. Available: <https://www.mdpi.com/1911-8074/18/1/41>.
- [548] A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 9, no. 4, p. e1306, 2019.
- [549] A. Dal Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, "Calibrating probability with undersampling for unbalanced classification," in *2015 IEEE symposium series on computational intelligence*, 2015: IEEE, pp. 159-166.
- [550] M. Alles, I. Munoko, and M. Vasarhelyi, "Ethics and the future of artificial intelligence in auditing," in *Artificial Intelligence in Accounting*: Routledge, 2022, pp. 217-230.
- [551] C. Rudin, C. Chen, Z. Chen, H. Huang, L. Semenova, and C. Zhong, "Interpretable machine learning: Fundamental principles and 10 grand challenges," *Statistic Surveys*, vol. 16, pp. 1-85, 2022.

- [552] F. Doshi-Velez and B. Kim, "Towards a rigorous science of interpretable machine learning," *arXiv preprint arXiv:1702.08608*, 2017.
- [553] S. A. Wadho, A. F. Meghji, A. Yichiet, R. Kumar, and F. Shaikh, "Encryption Techniques and Algorithms to Combat Cybersecurity Attacks: A Review," *VAWKUM Transactions on Computer Sciences*, 2023, doi: 10.21015/vtcs.v11i1.1521.
- [554] O. O. Ajakaye, A. G. Olanrewaju, D. Fawehinmi, R. Afolabi, and G. M. Pius-Kiate, "Integrating Artificial Intelligence in organizational cybersecurity: Enhancing consumer data protection in the U.S. Fintech Sector," *World Journal of Advanced Research and Reviews*, 2025-04-30 2025, doi: 10.30574/wjarr.2025.26.1.1421.
- [555] M. A. S. Shazly, "The Impact of Artificial Intelligence and Cyber Security on Audit Quality," vol. 15, no. 3, pp. 1-13, 2023.
- [556] C. Phua, V. Lee, K. Smith, and R. Gayler, "A comprehensive survey of data mining-based fraud detection research," *arXiv preprint arXiv:1009.6119*, 2010.
- [557] T. Chen and C. Guestrin, "Xgboost: A scalable tree boosting system," in *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining*, 2016, pp. 785-794.
- [558] R. K. Yin, *Case Study Research and Applications: Design and Methods*. Sage Publications, 2018.
- [559] J. W. Creswell and J. D. Creswell, *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications, 2017.
- [560] J. W. Creswell and J. D. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Thousand Oaks, CA: SAGE Publications, 2018.
- [561] M. Saunders, P. Lewis, and A. Thornhill, *Research Methods for Business Students*. Harlow, UK: Pearson Education Limited, 2019.
- [562] A. Bryman, *Social Research Methods*. Oxford: Oxford University Press, 2016.
- [563] L. Breiman, "Random forests," *Mach. Learn.*, vol. 45, no. 1, pp. 5-32, 2001.
- [564] D. J. Hand, "Classifier technology and the illusion of progress," 2006.
- [565] C. Rudin, "Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead," *Nature machine intelligence*, vol. 1, no. 5, pp. 206-215, 2019.
- [566] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016," in "General Data Protection Regulation (GDPR)," Official Journal of the European Union, 2016. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [567] E. A. Lopez-Rojas, "Applying simulation to the problem of detecting financial fraud," Blekinge Tekniska Högskola, 2016.

- [568] Z. Xiao, "IEEE-CIS Fraud Detection Based on XGB," Singapore, 2024: Springer Nature Singapore, in Proceedings of the 7th International Conference on Economic Management and Green Development, pp. 1785-1796.
- [569] X. A. Zhang and J. Borden, "How to communicate cyber-risk? An examination of behavioral recommendations in cybersecurity crises," (in English), *J. Risk Res.*, Article vol. 23, no. 10, pp. 1336-1352, Oct 2020, doi: 10.1080/13669877.2019.1646315.
- [570] F. Carcillo, A. Dal Pozzolo, Y.-A. Le Borgne, O. Caelen, Y. Mazzer, and G. Bontempi, "Scarff: a scalable framework for streaming credit card fraud detection with spark," *Information fusion*, vol. 41, pp. 182-194, 2018.
- [571] K. Sengupta and P. K. Das, "Detection of financial fraud: comparisons of some tree-based machine learning approaches," *Journal of Data, Information and Management*, vol. 5, no. 1, pp. 23-37, 2023/06/01 2023, doi: 10.1007/s42488-023-00086-w.
- [572] R. J. Little and D. B. Rubin, *Statistical analysis with missing data*. John Wiley & Sons, 2019.
- [573] B. Iglewicz and D. C. Hoaglin, *Volume 16: how to detect and handle outliers*. Quality Press, 1993.
- [574] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, p. Article 15, 2009, doi: 10.1145/1541880.1541882.
- [575] J. Brownlee, *Machine learning mastery with Python: understand your data, create accurate models, and work projects end-to-end*. Machine Learning Mastery, 2016.
- [576] G. James, D. Witten, T. Hastie, and R. Tibshirani, *An introduction to statistical learning: with applications in R*. Springer, 2013.
- [577] J. Jurgovsky *et al.*, "Sequence classification for credit-card fraud detection," *Expert Systems with Applications*, vol. 100, pp. 234-245, 2018/06/15/ 2018, doi: <https://doi.org/10.1016/j.eswa.2018.01.037>.
- [578] J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques*. Morgan Kaufmann, 2022.
- [579] S. Patro and K. K. Sahu, "Normalization: A preprocessing stage," *arXiv preprint arXiv:1503.06462*, 2015.
- [580] H. He and E. A. Garcia, "Learning from Imbalanced Data," *IEEE Trans. Knowl. Data Eng.*, vol. 21, no. 9, pp. 1263-1284, 2009, doi: 10.1109/TKDE.2008.239.
- [581] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: synthetic minority over-sampling technique," *Journal of artificial intelligence research*, vol. 16, pp. 321-357, 2002.
- [582] A. D. Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy," *IEEE Trans.*

- Neural Netw. Learn. Syst.*, vol. 29, no. 8, pp. 3784-3797, 2018, doi: 10.1109/TNNLS.2017.2736643.
- [583] G. Haixiang, L. Yijing, J. Shang, G. Mingyun, H. Yuanyue, and G. Bing, "Learning from class-imbalanced data: Review of methods and applications," *Expert Systems with Applications*, vol. 73, pp. 220-239, 2017/05/01/ 2017, doi: <https://doi.org/10.1016/j.eswa.2016.12.035>.
- [584] A. K. Jain, R. P. W. Duin, and J. Mao, "Statistical pattern recognition: A review," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 1, pp. 4-37, 2005.
- [585] R. Kohavi, "A study of cross-validation and bootstrap for accuracy estimation and model selection," in *Proceedings of the 14th International Joint Conference on Artificial Intelligence*, 1995, pp. 1137-1143.
- [586] D. W. Hosmer Jr, S. Lemeshow, and R. X. Sturdivant, *Applied logistic regression*. John Wiley & Sons, 2013.
- [587] T. G. Dietterich, "Ensemble methods in machine learning," in *International workshop on multiple classifier systems*, 2000: Springer, pp. 1-15.
- [588] M. Sokolova and G. Lapalme, "A systematic analysis of performance measures for classification tasks," *Information Processing & Management*, vol. 45, no. 4, pp. 427-437, 2009.
- [589] D. M. Powers, "Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation," *arXiv preprint arXiv:2010.16061*, 2020.
- [590] T. Fawcett, "An introduction to ROC analysis," *Pattern Recognit. Lett.*, vol. 27, no. 8, pp. 861-874, 2006/06/01/ 2006, doi: <https://doi.org/10.1016/j.patrec.2005.10.010>.
- [591] J. Davis and M. Goadrich, "The relationship between Precision-Recall and ROC curves," presented at the Proceedings of the 23rd international conference on Machine learning, Pittsburgh, Pennsylvania, USA, 2006. [Online]. Available: <https://doi.org/10.1145/1143844.1143874>.
- [592] N. Chinchor, "MUC-4 evaluation metrics," presented at the Proceedings of the 4th conference on Message understanding, McLean, Virginia, 1992. [Online]. Available: <https://doi.org/10.3115/1072064.1072067>.
- [593] A. P. Bradley, "The use of the area under the ROC curve in the evaluation of machine learning algorithms," *Pattern Recognit.*, vol. 30, no. 7, pp. 1145-1159, 1997/07/01/ 1997, doi: [https://doi.org/10.1016/S0031-3203\(96\)00142-2](https://doi.org/10.1016/S0031-3203(96)00142-2).
- [594] T. Saito and M. Rehmsmeier, "The Precision-Recall Plot Is More Informative than the ROC Plot When Evaluating Binary Classifiers on Imbalanced Datasets," *PLoS One*, vol. 10, no. 3, p. e0118432, 2015, doi: 10.1371/journal.pone.0118432.

- [595] D. Chicco and G. Jurman, "The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation," *BMC Genomics*, vol. 21, no. 1, p. 6, 2020/01/02 2020, doi: 10.1186/s12864-019-6413-7.
- [596] S. Amershi, M. Cakmak, W. B. Knox, and T. Kulesza, "Power to the people: The role of humans in interactive machine learning," *AI magazine*, vol. 35, no. 4, pp. 105-120, 2014.
- [597] D. W. Hosmer, S. Lemeshow, and R. X. Sturdivant, *Applied Logistic Regression*. Hoboken, NJ: Wiley, 2013.
- [598] Y. Xin, "Machine Learning and Deep Learning methods for cybersecurity," *IEEE Access*, vol. 6, 2018// 2018, doi: 10.1109/ACCESS.2018.2836950.
- [599] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153-1176, 2016, doi: 10.1109/COMST.2015.2494502.
- [600] F. Pedregosa *et al.*, "Scikit-learn: Machine learning in Python," *the Journal of machine Learning research*, vol. 12, pp. 2825-2830, 2011.
- [601] M. Vasarhelyi and D. O'Leary, "Artificial Intelligence in Accounting and Auditing: Creating Value with AI, Volume 5," 02/24 2023.
- [602] E. Lopez-Rojas, A. Elmir, and S. Axelsson, "PaySim: A financial mobile money simulator for fraud detection," in *28th European Modeling and Simulation Symposium, EMSS, Larnaca*, 2016: Dime University of Genoa, pp. 249-255.
- [603] P. Hajek, M. Z. Abedin, and U. Sivarajah, "Fraud Detection in Mobile Payment Systems using an XGBoost-based Framework," (in eng), *Inf Syst Front*, pp. 1-19, Oct 14 2022, doi: 10.1007/s10796-022-10346-6.
- [604] G. Shmueli, "To explain or to predict?," *Statistical science*, pp. 289-310, 2010.
- [605] N. Kshetri, C. S. Bhushal, P. S. Pandey, and Vasudha, "BCT-CS: Blockchain Technology Applications for Cyber Defense and Cybersecurity: A Survey and Solutions," (in English), *Int. J. Adv. Comput. Sci. Appl.*, Article vol. 13, no. 11, pp. 364-370, Nov 2022. [Online]. Available: <Go to ISI>://WOS:000926520800001.
- [606] H. Cavusoglu, B. Mishra, and S. Raghunathan, "A model for evaluating IT security investments," *Communications of the ACM*, vol. 47, no. 7, pp. 87-92, 2004.
- [607] O. B. Onyenahazi, "Integrating Artificial Intelligence in Financial Auditing," *ResearchGate Preprint*, 2024. [Online]. Available: <https://www.researchgate.net/publication/393330353>.
- [608] A. K. Dohare, "A Hybrid Machine Learning Framework for Financial Fraud Detection," *EKSPLORIUM – Bulletin of Advanced Material Technology*, 2025. [Online]. Available: <https://eksplorium.com/index.php/journal/article/view/215>.
- [609] S. Molnar, *Interpretable Machine Learning*. Leanpub, 2022.

- [610] G. Carnegie, L. Parker, and E. Tsahuridu, "It's 2020: what is accounting today?," *Australian Accounting Review*, vol. 31, no. 1, pp. 65-73, 2021.
- [611] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research1," *MIS quarterly*, vol. 28, no. 1, pp. 75-106, 2004.
- [612] A. M. Rozario and M. A. Vasarhelyi, "Auditing with Smart Contracts," *International Journal of Digital Accounting Research*, vol. 18, 2018.
- [613] A. H. Anwar, C. Kamhoua, and N. Leslie, "A game-theoretic framework for dynamic cyber deception in internet of battlefield things," presented at the Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Houston, Texas, USA, 2020. [Online]. Available: <https://doi.org/10.1145/3360774.3368204>.
- [614] C. Kanodia, "Game theory models in accounting," in *Game theory and business applications*: Springer, 2013, pp. 43-79.
- [615] F. Anwar, R. Mir, R. Olanrewaju, B. Khan, and B. R. Pampori, "A Comprehensive Insight into Game Theory in relevance to Cyber Security," *Indonesian Journal of Electrical Engineering and Informatics (IJEI)*, 2020-03-11 2020, doi: 10.11591/IJEI.V8I1.1810.
- [616] D. Tapscott and A. Tapscott, *MIT Sloan Manage Rev*, vol. 58, no. null, p. 10, 2017.
- [617] B. Collins, S. Xu, and P. Brown, "Game-Theoretic Cybersecurity: the Good, the Bad and the Ugly," 2024-01-24 2024. [Online]. Available: <https://consensus.app/papers/gametheoretic-cybersecurity-the-good-the-bad-and-the-ugly-collins-xu/72462f3dde8a5ef8b6fe901fd3267791/>.
- [618] M. J. Osborne and A. Rubinstein, *A course in game theory*. MIT press, 1994.
- [619] S. Tadelis, *Game theory: an introduction*. Princeton university press, 2013.
- [620] T. Alpcan and T. Başar, *Network security: A decision and game-theoretic approach*. Cambridge University Press, 2010.
- [621] Q. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 46-65, 2015.
- [622] J. W. Cresswell, *Qualitative inquiry and research design: choosing among five traditions* (null). 1996, p. null.
- [623] C. W. Lee and S. Madnick, "Cybersafety Approach to Cybersecurity Analysis and Mitigation for Mobility-as-a-Service and Internet of Vehicles," (in English), *Electronics*, Article vol. 10, no. 10, p. 22, May 2021, Art no. 1220, doi: 10.3390/electronics10101220.
- [624] S. Gregor and A. R. Hevner, "Positioning and presenting design science research for maximum impact1," *MIS quarterly*, vol. 37, no. 2, pp. 337-355, 2013.

- [625] O. Onabowale, "AI and real-time financial decision support," *International Journal of Advance Research Publication and Reviews*, vol. 2, no. 6, pp. 329-350, 2025.
- [626] E. Kurshan, D. Mehta, and T. Balch, "AI versus AI in Financial Crimes & Detection: GenAI Crime Waves to Co-Evolutionary AI," in *Proceedings of the 5th ACM International Conference on AI in Finance*, 2024, pp. 745-751.
- [627] H. Singh, "Managing the Quantum Cybersecurity Threat: Harvest Now, Decrypt Later," in *Quantum Computing*: CRC Press, 2024, pp. 142-158.
- [628] S. G. Finlayson, J. D. Bowers, J. Ito, J. L. Zittrain, A. L. Beam, and I. S. Kohane, "Adversarial attacks on medical machine learning," *Science*, vol. 363, no. 6433, pp. 1287-1289, 2019, doi: doi:10.1126/science.aaw4399.
- [629] A. Jokiniemi, "NIST's Module-Lattice-Based Key-Encapsulation Mechanism and its security," 2025.
- [630] L. Moura, A. Barcaui, and R. Payer, "AI and Financial Fraud Prevention: Mapping the Trends and Challenges Through a Bibliometric Lens," *Journal of Risk and Financial Management*, vol. 18, no. 6, p. 323, 2025. [Online]. Available: <https://www.mdpi.com/1911-8074/18/6/323>.
- [631] D. B. Vuković, S. Dekpo-Adza, and S. Matović, "AI integration in financial services: a systematic review of trends and regulatory challenges," *Humanities and Social Sciences Communications*, vol. 12, no. 1, p. 562, 2025/04/22 2025, doi: 10.1057/s41599-025-04850-8.
- [632] I. Auditing and A. S. Board, "ISA 315 (Revised). Identifying and assessing the risks of material misstatement," 2019.
- [633] A. Anis, "Blockchain in accounting and auditing: unveiling challenges and unleashing opportunities for digital transformation in Egypt," *Journal of Humanities and Applied Social Sciences*, vol. 5, no. 4, pp. 359-380, 2023, doi: 10.1108/jhass-06-2023-0072.
- [634] G. Alagic, Q. Dang, D. Moody, A. Robinson, H. Silberg, and D. Smith-Tone, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," 2024.
- [635] N. AI, "Artificial intelligence risk management framework (AI RMF 1.0)," URL: <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai>, pp. 100-1, 2023.
- [636] T. Pro. "Cyber resilience in the post-quantum era: the time of crypto-agility." <https://www.techradar.com/pro/cyber-resilience-in-the-post-quantum-era-the-time-of-crypto-agility> (accessed.
- [637] O. Borchert, S. Connelly, S. Mitchell, and S. Rose, "Zero trust architecture," *National Institute of Standards and Technology, Tech. Rep. NIST Special Publication (SP)*, pp. 800-207, 2020.
- [638] M. CISA, "Shifting the balance of cybersecurity risk: Principles and approaches for security-by-design and-default," ed: Cybersecurity and Infrastructure Security Agency, 2023.

- [639] S. Watkins, "ISO/IEC 27001: 2022: An introduction to information security and the ISMS standard," 2022.
- [640] AICPA, *Guide: SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*. John Wiley & Sons, 2018.
- [641] S. M. Mintz and W. F. Miller, "Do PCAOB Audit Inspections and ICFR Assessments Protect the Public Interest?," *The CPA Journal*, vol. 93, no. 3/4, pp. 32-38, 2023.
- [642] S. Arping and Z. Sautner, "Did SOX Section 404 make firms less opaque? Evidence from cross-listed firms," *Contemporary Accounting Research*, vol. 30, no. 3, pp. 1133-1165, 2013.
- [643] H. H. Shadan and S. Islam, "Quantum Computing and Cybersecurity in Accounting and Finance: Current and Future Challenges and the Opportunities for Securing Accounting and Finance Systems in the Post-Quantum World," *arXiv preprint arXiv:2506.12096*, 2025.
- [644] V. Le, "Integrating blockchain and machine learning for continuous auditing: challenges and strategies," 2024.
- [645] B. J. Mary, "Towards a Smart Cybersecurity Accounting Framework: Preparing Financial Infrastructure for Quantum Threats," 2024.