Comprehensive analysis of services towards Data Aggregation, Data Fusion and enhancing security in IoT-based smart home

EAI Endorsed Transactions
on Internet of Things

Research Article EAI.EU

Comprehensive analysis of services towards Data Aggregation, Data Fusion and enhancing security in IoT-based smart home

Arun Kumar Rana[1*], Sumit Kumar[2], Vikram Bali[1] , Rashmi Prava Das[3], Sardar M. N. Islam[4], Debendra Muduli[5], Ritu Dewan[1], Anurag Singh[6]

[1]Galgotias College of Engineering & Technology, Greater Noida 201310, India
[2]Department of Computer Science and Engineering, Panipat Institute of Engineering and Technology, Panipat 132102, India
[3]Department of Computer Science and Engineering, CV Raman Global University, Bhubaneswar 752054, India
[4]ISILC, & Decision Sciences and Modelling Program, Victoria University, Australia
[5]Department of Computer Science and Engineering, CV Raman Global University, Bhubaneswar 752054, India
[6]Electrical & Electronics Engineering Department, G L Bajaj Institute of Technology and Management Greater Noida, India

Abstract

Data aggregation and sensors data fusion would be very helpful in a number of developing fields, including deep learning, driverless cars, smart cities, and the Internet of Things (IoT). An advanced smart home application will test the upgraded Constrained Application Protocol (CoAP) using Contiki Cooja. Smart home can enhance people's comfort. Secure authentication between the transmitter and recipient nodes is essential for providing IoT services. In many IoT applications, device data are critical. Current encryption techniques use complicated arithmetic for security. However, these arithmetic techniques waste power. Hash algorithms can authenticate these IoT applications. Mobile protection issues must be treated seriously, because smart systems are automatically regulated. CoAP lets sensors send and receive server data with an energy-efficient hash function to increase security and speed. SHA224, SHA-1, and SHA256 were tested by the CoAP protocol. Proposed model showed that SHA 224 starts secure sessions faster than SHA-256 and SHA-1. The ChaCha ci. This study proposed enhanced ChaCha, a stream cipher for low-duty-cycle IoT devices. For wireless connections between the IoT gateway and sensors with a maximum throughput of 1.5 Mbps, the proposed model employs a wireless error rate (WER) of 0.05; the throughput rises with an increase in the transmission data rate.

Keywords: Internet of Things (IoT), Constraint Application Protocol (CoAP), Hash function, Privacy, Security; ChaCha, Data fusion

Received on 21 July 2024, accepted on 6 September 2024, published on 2 October 2024

doi: 10.4108/eetiot.6703

1. Introduction

In the twenty-first century, the Internet of Things (IoT) has emerged as one of the most influential and pervasive modes of communication. Connected items are those that have sensors and other technology built into them, allowing them to communicate with other devices through the internet [1].

Any object that has processing and communication capabilities may be connected to the Internet in an IoT environment. The Internet has become more flexible and has a wider range of applications thanks to the IoT. As a result, the IoT has become more valuable in a number of industries. More and more smart homes are using the IoT to automate household appliances for user pleasure and convenience. IoT-based smart home infrastructures have changed the way people live by providing users with access to their smart devices, regardless of time or location. Home automation technologies have advanced significantly in recent years, with facilities and methods for sharing

[*]Corresponding author. Email: arunkumar@galgotiacollege.edu

knowledge and resources with appliances. The confidentiality, integrity, and availability of systems may be jeopardized in the Internet of Things if proper authentication is not in place. This is due to the fact that an adversary who successfully authenticates as a valid user will have access to all of the user's data and will be able to read, edit, and delete data in the same ways that the user can, jeopardizing availability, integrity, and confidentiality [2]. One of the biggest challenges in the Internet of Things is still user identification and authentication. The most popular method for user identification and authentication in electronic systems at the moment is username/password pairs, while additional methods like shared keys, digital certificates, or biometric credentials may be employed [3]. However, many of the physical interfaces for interaction via which passwords and usernames are provided will be eliminated in the pervasive vision of the Internet of Things [4].

The Internet of Things and Blockchain are two technologies that have gained prominence since their inception. In the near future, IoT will have an impact on practically all of the devices we use every day. As this technology becomes more widely used, so does the risk of abuse. Existing technology are insufficient to cope with this. So, blockchain has emerged as an efficient alternative for addressing IoT security challenges. The Internet of Things enables devices throughout the internet to communicate data to private blockchain networks, resulting in tamper-resistant records of shared transactions. IBM Blockchain® enables your business partners to exchange and access IoT data with you while eliminating the need for central control and administration [5]. Each transaction may be validated to avoid conflicts and increase confidence among all permissioned network users. All nodes linked via the internet work together to preserve all transactions done on a blockchain network, and the legitimacy of a transaction is verified by a protocol. Securing the network of IoT devices using a blockchain network decentralizes the system, meaning there is no one authority that may authorize any transaction. Each gadget will have a copy of the ever-expanding chain of data. This implies that if someone wants to use the device and conduct a transaction, all members of the network must validate it.

In the Internet of Things, the Constrained Application Protocol (CoAP) is a web data transfer protocol that runs over User Datagram Protocol (UDP) that is utilised with limited nodes and networks. This protocol is used for M2M communications [6], which includes applications like smart parking and smart homes. Since the CoAP protocol mimics the functionality of HTTP over a conventional network [7], and since HTTP itself is not secure, additional protocols must be used to encrypt data in transit. These alternatives include Transport Layer Security (TLS), Secure Socket Shell (SSH), and Internet Protocol Security (IPsec). Datagram Transport Layer Security (DTLS) is one method of protecting the CoAP; it regulates key management, data privacy, and data authentication. When used with DTLS, CoAP functions similarly to the HTTP protocol. CoAP is similar to the HTTP protocol when used with the DTLS protocol. While DTLS is not ideal for all IoT devices, IPsec with CoAP in the right environment can take use of the device's native link-layer hardware security. It is more expensive to implement a DTLS certificate and DTLS has a longer delay compared to other safe encryption techniques [8].

Standardized cryptographic algorithms are typically resistant to cryptanalysis, which is the process by which an attacker tries to discover the secret key by looking at a set of inputs and the matching outputs of an algorithm. A class of physical attacks against the hardware implementation of the techniques known as side-channel analysis (SCA) has been made possible, however, by the physical exposure of IoT and mobile devices in unprotected surroundings to potential adversaries [9]. Lightweight cryptography (LWC) is undergoing a multi-year process of standardisation at the United States' National Institute of Standards and Technology (NIST), where authenticated cyphers are evaluated for their ease of implementation on low-resource platforms and their compatibility with side-channel defences [10].

ChaCha is a fast stream cypher optimised for use in computer programmes. The cypher can be easily implemented with minimal overhead and may be used with a variety of different architectures [11]. It features a rapid and easy key setup and overall performance, and it was made to avoid information leaking through side-channel analysis. This cypher is a modification of Salsa20, which is included in the eS-TREAM portfolio [12]. Therefore, in order to replace Rivest Cypher 4 (RC4) and solve the aforementioned problems, a new stream cypher is required. In this research, we introduce a fast, platform-independent, and easy-to-implement secure stream cypher for TLS and DTLS that is also resistant to software side-channel attacks.

1.1 Objective, Motivation and Contributions

Consequently, a technological architecture with the primary goal of guaranteeing scalability, application compatibility, and data transfer protection is put forth to mitigate such concerns. In order to do this, the CoAP protocol evaluated SHA224, SHA-1, and SHA256, and expert opinion was used to confirm the results. In order to reduce the power consumption of IoT devices with Chacha security, this study integrates the CoAP protocol with IoT. This contribution is motivated by the fact that IoT devices may efficiently reduce power consumption, supply highly secure information, and offer low-cost solutions to the IoT network for smart homes in emergency scenarios. This paper’s contribution can be summarized as follows:

- It discusses the latest papers investigating the intermingling of smart homes with various IoT applications.
- It proposes a secure SHA224, which is used with the CoAP protocol to enhance the security in a smart home.

- It proposes solutions using the CoAP for energy reduction and improves security when compared with an existing algorithm in a smart home.
- It proposes a new ChaCha stream cipher procedure for safeguarding the data on IoT devices with low duty cycles.
- It proposes an IoT-based framework that achieves an outstanding performance by meeting all the necessary security requirements.
- The proposed technique Chacha stream cipher has a computation time of 0.221 ms, as evidenced by the test results.

The remainder of the paper is as follows: Section 2 presents the literature survey, which examines how specialists utilize the related proposed frameworks. Section 3 discusses the IoT-based smart home design framework. Section 4 states the proposed methodology. Section 5 discuss discusses the performance evaluation. The paper is concluded in Section 6.

2. Related Works

IoT inventions provide a variety of smart home solutions to make life more comfortable and ecologically safe. On the other hand, they raise a slew of issues. The papers [13] demonstrated ZigBee home automation control technology use wireless data transmission technology. Depending on the code and technique used in the other example, such a framework has several disadvantages. Wireless networking technologies, such as wireless fidelity (Wi-Fi), are used in some prospective smart homes [14]. In the age of the Internet of Things, the physical exposure of devices to adversaries in unprotected contexts mandates the examination of cryptographic hardware implementations against side-channel analysis (SCA). Round 2 of the U.S. competition accepted the Ascon verified cypher. In that work, they assessed Ascon’s susceptibility to passive and aggressive SCA assaults. They showed a successful statistical ineffective fault analysis (SIFA) attack, employing voltage glitches on the supply pin of the FPGA device using a lightweight implementation of Ascon on an Artix-7 Field Programmable Gate Array (FPGA) [15].

Wellness, life support, safety, and sustainability are all available in the modern smart house. Now, revolutionary home technologies like IoT, AI, and blockchains rely heavily on automation engineering. Keywords related to "smart home" on Baidu, TMall, and Know the Topic were extracted using big data and analysed so that the authors [16] could learn about the Chinese smart home market. Most searches for "smart home" are in Beijing and Shenzhen. The three most often used smart devices are toilets, speakers, and televisions. People in their thirties and forties are the most likely to look for information on smart homes online. The elderly require infrastructures that allow them to age in situ. To investigate the senior housing market, the factors driving downsizing, and policy responses, this research conducted in-depth interviews with both individuals and small groups.

Residents and staff at two large Hong Kong assisted living facilities were surveyed. The findings were more trustworthy and reliable due to the implementation of a methodological triangulation that included interviews, records, and other forms of communication [17]. The elderly typically move from bigger homes to smaller ones to reduce their housing costs and help families with growing families find affordable accommodation. The software relies on freely available source code. The author also gave the thumbs up to the hardware used in IoT nodes. In [18], it was shown how to authenticate a safe low-cost IoT system. As the capabilities of attackers have grown, the edge devices of IoT infrastructures have become more vulnerable to forgery and piracy. A key worry is establishing the authenticity of such devices since an adversary can install a backdoor to overcome security and/or disclose sensitive information through an unprotected communication connection.

Such devices' credibility might be called into question if they are fake, broken, or of low quality. Despite the PUF's extreme unreliability, a new identification (ID) matching technique is offered to verify an edge device's genuineness. The authors of [19] demonstrated a safe Internet of Things (IoT) smart home framework. Wireless sensor networks (WSNs) provide several advantages over more conventional systems when used for a wide range of purposes, including smart homes, healthcare, environmental monitoring, and house and land protection. Together, WSNs and IP form the Internet of Things (IoT), which links commonplace objects together online. Consequently, two of the biggest problems with WSNs are (i) ensuring data is secure while being transmitted between a large number of sensor nodes using only a small number of low-power nodes, and (ii) addressing the security concerns that arise when transmitting data over a large distance in a variety of extreme and potentially dangerous environments. To manage security alerts including data qualification, leakage, and code development, the security framework in [20] introduced an authenticity system that made use of signature and access control techniques. Access control to protect home computer modules in an intelligent house was presented with the security architecture in this article.

Because Internet of Things apps are becoming more intertwined with their users' identities and because they operate, process, and store a variety of data types, data protection is an essential subject that has to be investigated in the context of the Internet of Things. The research presented in the article (21), which was titled "Covering a Wide Range of Security and Privacy Issues," focused particularly on applications that operate on low-resource platforms. The author of [22] researched the application of cryptographic bricks, hacking algorithms, message authentication codes, signature techniques, and crucial exchange protocols on cutting-edge systems that have resource limitations. The authors identified the best hash function to increase security for the constrained application protocol without negatively impacting speed. The author of this study [23] focused their attention on the difficulties associated with maintaining privacy and the solutions to these difficulties. The Internet of Things, on the other hand, does away with the interaction between humans and machines and makes the system more intelligent. The anonymity of this contact, on the other hand, is not yet guaranteed, and the full assurance of device-to-device communication is not yet available. Recent research has resulted in the development of a lightweight and host-based denial of service (DoS) anomaly detection and defence method for resource-constrained Internet of Things devices. Their method was centred on warding against denial of service assaults on Internet of Things devices [24].

To ensure a high level of security, current encryption systems are built with a high level of arithmetic complexity. These arithmetic procedures, however, cause issues with efficiency and power usage. Thus, to enhance security and efficiency, in this paper, we used the SHA224. In addition, the goal of this research was to propose a low-power, lightweight stream cipher technique for safeguarding the information sent between cloud nodes as a backend real-time database and IoT devices. To further tighten the security of the Internet of Things, a new ChaCha stream cypher technique has been developed. Furthermore, in order to protect the network against critical security attacks and threats, the proposed IoT framework complies with all security requirements, including confidentiality, privacy, integrity, data freshness, secure localization, non-repudiation, availability, access control, trustworthiness, and authentication. Table 1 displays a comparison of similar tasks.

Table 1. Related work comparison

Author (s)	Energy	Security	Quality of Service
Bassoli et al. [13]	×	×	
Wenbo et al. [14]	×	×	
Sarker et al. [15]		×	
Peng et al. [16]			×
Li et al. [17]		×	×
Guin et al. [18]	×	×	
Pirbhulal et al. [19]			
Kang et al. [20]		×	×
Lachner et al. [21]			×
Patil et al. [22]		×	
Dhiman et al. [23]		×	
Kponyo et al. [24]	×	×	
Proposed work		×	×

3. Proposed Architecture

Cameras, appliances, and actuators are all examples of non-intelligent components that must be included to a smart home system. A sensor generates data, but it has little practical application in a domestic setting by itself. A thermostat is also not regarded to be intelligent if the homeowner must manually adjust the setting in response to changes in the ambient temperature, humidity, and other factors. Keeping the temperature stable requires automation rather than "smartness." When all environmental data are processed and assessed collectively, patterns are retrieved, and choices are made without the assistance of the user, only then can we say that an ecosystem is intelligent [25].

How sensors communicate, where and how data on sensor and equipment usage patterns are kept, how patterns in the data are analysed, and how devices are managed by the customer and vice versa all contribute to the overall structure of a smart home. To efficiently manage home gadgets and supply users with cutting-edge services, a "smart home" requires a sophisticated, heterogeneous infrastructure comprised of sensors, connections, and apps. A generic design for a smart house that uses the cloud is presented in Figure 1. The terminal devices, sensors, computers, and actuators that make up the internal network. It is simpler to connect private networks to the Internet when these gadgets talk to a gateway located at the network's edge [26].

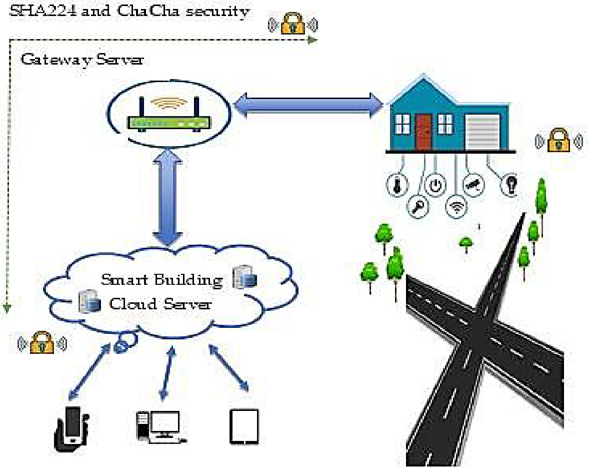


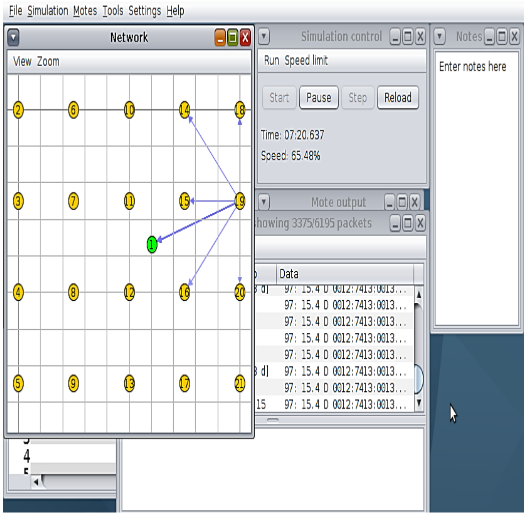
Figure 1. Proposed architecture.

The heterogeneous data from sensors may be converted into a common format by a smart home gateway architecture set up in terms of established communication protocols. The gateway is a universal device that facilitates communication between disparate endpoints by supporting many communication protocols. Any calculation may be performed efficiently at the network's edge before the data is sent to the cloud. All communication between the end devices and the outside world is screened before instructions are delivered to the end devices thanks to the gateway, which adds another layer of protection to the smart home network. Effectively, this will incorporate means to enhance usability, stability, and security while making use of increased processing power and a scalable architecture. Data visualisation, smart home device administration, and user authentication and job assignment are just some of the many external services that may be integrated with the cloud. For smart homes using the Raspberry Pi, Perl scripts are an excellent option for monitoring devices that can be queried or remotely modified on the Pi. Using your voice, you can control the lights, record TV shows, and even hear who's calling you. For the free software project NodeMCU, there are schematics for prototype boards available for download. The NodeMCU ESP8266 WiFi Module will take commands from a smartphone via the internet. Encoding the ON/OFF signal and sending it to the server requires the best IoT platform available. board esp8266 [27]. One of the most significant benefits of smart home automation systems is their ease of administration and control from a variety of devices, including smartphones, laptops and desktops, tablets, smart watches, and voice assistants. Home automation systems provide numerous advantages, including increased safety through appliance and lighting control, home security through automated door locks, increased awareness through security cameras, increased convenience through temperature adjustment, time savings, control, and cost savings.

4. Proposed Methodology

Because IoT devices require drivers to upload programs and function normally, this paper considered the Contiki operating system (OS). It is a powerful operating system designed for wireless sensor network devices such as the Zolertia Z1, Tmote, Sky mote, and others. For academics, developers, enthusiasts, and hobbyists, the Zolertia Z1, Tmote, and Sky mote modules provide a general-purpose development platform for IoT networks. This operation includes numerous examples and features, such as calculating the power consumption of connected devices or the entire network, monitoring the received signal strength indicator (RSSI) value of the targeted device, and so on. With the power consumption program, it is possible to analyze the power consumption of low-powered devices. This module will check the ongoing power consumption on a regular basis [28]. It is a famous, open-source IoT-programming working framework dependent on the C programming language and disseminated under the Berkeley Software Distribution (BSD) permit. Contiki is a low-power, remote Internet of Things working framework that is organized and memory-restricted.

Contiki is a low-power Radio Frequency Identification (RFID) chip that can be used in remote correspondences with an astounding effectiveness and security. Contiki is modified to utilize the Cooja network test system, incorporating essential C libraries for RFID chips and sensors. The backend C projects, just as the header records that go with them, can be changed and recompiled to create the vital outcomes for booking, overseeing, and observing far-off IoT gadgets. Contiki works by acquainting lightweight conventions with Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) networks to associate low-power chips with radio-recurrence chips without causing execution issues. Numerous assets are addressed by an actual element (i.e., thing) in CoAP, which addresses the information observed from the sensors or activities available to the actuators. Figure 2 shows Cooja's window, which is filled with the primary simulation tools. Here is a quick rundown of each tool's functionality:



```
Time: 07:20.637
Speed: 65.48%
```

```
showing 3375/6195 packets
97: 15.4 D 0012:7413:0013...
97: 15.4 D 0012:7413:0013...
97: 15.4 D 0012:7413:0013...
97: 15.4 D 0012:7413:0013...
97: 15.4 D 0012:7413:0013...
97: 15.4 D 0012:7413:0013...
97: 15.4 D 0012:7413:0013...
97: 15.4 D 0012:7413:0013...
```

Figure 2. Contiki cooja simulator [28].

Simulation Control: From this panel, you may initiate, halt, resume, or carry out simulation steps. Both the execution time and the simulation speed are shown. Events can be executed several times faster than they might be in real time.

Network: Every node's location inside the network is shown. Every node's state may be shown, together with information on its addresses, outputs, LEDs, and mote IDs. Initially, this window is empty, and we have to populate it with our sensors**.**

The mote output: displays every serial interface output on the node. It is possible to activate one Mote output window per simulation node.

Timeline: A simulation timeline shows messages and events like log outputs, channel changes, LED changes, and so on.

Continue reading to learn how to utilise Contiki and Cooja to customise IPv6 conventions. In the current IoT context, the CoAP protocol is highly helpful. Security and honesty are the key challenges in an IoT-based system where capture-free communication is necessary. This work presents an upgrade to the CoAP protocol that provides authentication and integrity to the protocol without using DTLS, which is sluggish, wasteful, and necessitates a complex initial handshake. When compared to the DTLS protocol, the proposed improvement would decrease power consumption, increase performance, and lower installation costs. The suggested improvement uses lightweight authentication by inserting a short Message Authentication Code (MAC) and using the same message structure, which requires less computing effort.

4.1. Values Captured Process

As shown below, the sensor and controller will use a variety of protocols to authenticate the data that is exchanged between them in order to safeguard it via the CoAP protocol. The sensor performs the following actions: Before sending the message through the CoAP protocol, the sequence-id value of the sensor is first concatenated with the payload element. Next, using the PSK based on the SHA hash technique, the hash value for the hash-based message authentication (HMAC) will be determined. The original payload value and the hashed value are then concatenated. A kind of message authentication code (MAC) known as a hash-based message authentication code (HMAC) is one that employs a secret cryptographic key and a cryptographic hash function. By assigning the key exchange to the people involved in communication, who are responsible for establishing and using a reliable channel to agree on the key prior to contact, it eliminates the need for an intricate public key infrastructure.

$$\text{HMAC}(K, m) = H((K' \oplus \text{opad}) \,||\, H((K' \oplus \text{opad}) \,||\, M)) \quad (1)$$

$$K' = \begin{cases} H(K) & K \text{ is larger than block size} \\ K & \text{otherwise} \end{cases} \quad (2).$$

where H is a cryptographic hash function
m is the message to be authenticated
K is the secret key
K' is a block-sized key derived from the secret key,
K; either by padding to the right with 0 s up to the block size or by hashing down to less than or equal to the block size first and then padding to the right with zeros
|| denotes concatenation
⊕ denotes bitwise exclusive or (XOR)
opad is the block-sized outer padding, consisting of repeated bytes valued at 0 × 5c
ipad is the block-sized inner padding, consisting of repeated bytes valued 0 × 36

Lastly, the CoAP will be used to send the payload portion of the final output message. After that, because the wireless sensors are synchronised, the controller uses the Pre-Shared Key Transport Protocol (PSK) based on the SHA hash function to compute the hash value of the message section when it receives a message from the sensor. If the calculated hash value and the supplied hash value are same, this value will be handled. Should this not be done, the message will be deleted.

4.2. Security Algorithm

A different security algorithm is explained below.

4.2.1. Secure Hash Algorithm

This is a cryptographic hash algorithm that generates a 160-bit (20-byte) hash value from the input. The message digest name given to the hash value is therefore commonly given as a hexadecimal number of 40 digits [29].

4.2.2. SHA-256 Algorithm

The National Security Agency created the SHA-256 algorithm as a variation of SHA-2, which succeeded SHA-1. SHA-256 is a patented cryptographic hash algorithm that generates a 256-bit value. Cryptographic hashing involves modifying hashed data in such a manner that they become fully illegible. Converting the 256-bit hash stated above back into its original 512-bit version would be nearly impossible. So, why would you want to send an unrecoverable scrambled message? The most typical reason is to double-check the substance of confidential information. For example, hashing is used to verify the integrity of secure messages and data [30].

4.2.3. SHA-224

Because SHA-224 is based on SHA-256, computing an SHA-224 or SHA-256 digest message's digest value takes about the same amount of time. SHA-224 is a reasonable choice for a one-way hash function that gives 112 bits of security, even though SHA-256 and SHA-224 have essentially an identical computational complexity. A truncated SHA-256 message digest value cannot be confused with an SHA-224 message digest value computed on the same data, since a different start value is used [31].

4.2.4. ChaCha

ChaCha employs the most widely accepted method of combining encryption and authentication. It is made with an AEAD Authenticated Encryption with Associated Data structure (AEAD). AEAD is a method for combining the properties of encryption and authentication by combining a cipher and an authenticator. Previously, this would have been performed using two distinct algorithms, usually a block cipher and an HMAC.

5. Results and Discussion

The CoAP is a specialised web transmission protocol designed for usage with constrained networks and fewer nodes in the Internet of Things. The CoAP protocol is intended to make it simple for regulated devices to connect to the Internet of Things, even via networks that are restricted and have poor availability and bandwidth [32]. It is often used for machine-to-machine (M2M) building automation and smart energy systems [33]. IoT devices like sensors and actuators may communicate thanks to the CoAP, which functions as a form of HTTP for limited devices [34]. By passing along their data, these sensors and actuators are controlled and function as a component of a device. The protocol was built with a low power usage and low overhead network for religiousness in low bandwidth and high congestion. The improved protocol was tested using the Contiki cooja operating system (OS), using the simulation of an intelligent home application (see Figure 3) [35].

Based on the digested message size, block size, maximum message size, number of rounds in the hash algorithm, and operations carried out to hash the message, Table 2 illustrates the differences between these three hash algorithms [36–37]. Table 3 provides the simulation parameters. Simply right-click any mote and choose "Change transmission ranges" to adjust the motes' interference and transmission ranges. It is necessary to refresh the simulation after adjusting the range. An illustration of this network, with a transmission range of 50 meters and an interference range of 50 meters, pausing during the exchange of greetings. Any printouts from the motes will be shown in the Mote Output window. This may be quite helpful in more complicated networks that need for a more detailed examination of the data since it allows for different levels of modification to the motes' real source code, which results in messages that can be seen in this window. Any print messages that are utilized to determine the code flow will also display here.

Table 2. The differences between three hash algorithms

Hash Algorithm and Difference	Output Bits	Max Message Size	Number of Rounds	Operations	Block Size
SHA-1	160	264–1	80	And, Xor, Rot, Add (mod 232), Or	512
SHA224	224	264–1	64	And, Xor, Rot, Add (mod 232), Or, Shr	512
SHA256	**256**	**2128 –1**	**80**	**And, Xor, Rot, Add (mod 264), Or, Shr**	**1024**

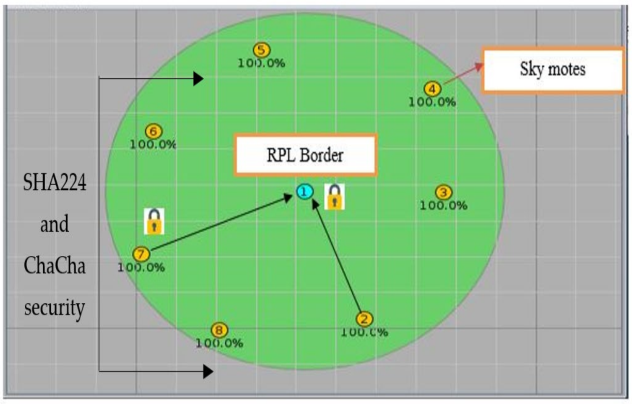


Figure 3. Shows 7 sensors (Sky mote in orange color) with one border router controller (sky blue color).

The likelihood of effective transmission and acknowledgment is defined as $P_{ack,trans}$ and given by:

$$P_{ack,trans} = P_{ack|trans,low}P_{trans|low}P_{low}P_{ack|trans,high}P_{trans|high}P_{high} \quad (3)$$

where $P_{ack|trans,high}$ and $P_{ack|trans,low}$ are the restrictive probabilities of effective affirmation, given a fruitful transmission for the direct in the high and low misfortune states individually; $P_{trans|high}$ and $P_{trans|low}$ are the contingent probabilities of effective transmission for the divert in the low and high misfortune states separately; and P_{high} and P_{low} are the consistent state channel probabilities.

The general likelihood of accomplishment or confirmable (P_{con}) after R = K retransmissions of a parcel outline follows a mathematical circulation with the Probability Mass Function (PMF), given by:

$$P_{con}(R = K) = P_{ack,trans}(1 - P_{ack,trans})^{k} \quad (4)$$

Table 3. Reproduction parameters

Parameter	Value
OS	Contiki 2.7
Communication Range	50 m
Simulation Time	95 min
Topology	Random
MAC Layer	802.15.4
Packet Size	56 byte
Packet Rate	4P/s
Interference Range	55 m
Interference Range	55 m
Computer	RAM 8GB
Routing Protocol	CoAP
Node Type	Skymote
Number of Nodes	8
WER	0.01–0.05

The known previous and conditional information are combined to generate the categorization results. To appropriately collect and assess data from the receiver, one may utilise the probabilities of each feature value impacting a certain class that is thought to be independent of the others. This will lessen the stress on the network while simultaneously having fast classification speeds, high accuracy, reliable classification efficiency, insensitivity to missing data, and quick and efficient acquisition of classification results. Once the data packets are received, the receiver analyses each priority data packet's loss probability statistically to identify the kind of packet loss. Since a packet may be retransmitted up to N times before it is deemed lost, the likelihood of loss is provided by:

$$P_{con}(loss) = 1 - \sum_{k=0}^{\infty} P_{con}(R = K) \; = 1 - P_{ack,trans} \sum_{k=0}^{N} (1 - P_{ack,trans})^{k} = (1 - P_{ack,trans})^{N+1} \quad (5)$$

$$E(latency) = (min[\Delta \frac{(1-P_{ack,trans})P_{ack,trans}}{2P_{ack,trans}-1}, \Delta 2^{N+1} - 1, Exchange\_Lifetime) \quad (6)$$

where Δ is the CoAP basic starting break and Exchange_lifetime is, in accordance with the CoAP criteria, the time interval between the start of sending a comparable message and when an acknowledgement is currently not required. Each parcel is lost if, like with most severe dormancy, it is reached. It is customizable and considers the basic action. SHA-256 computes a 256-bit hash value from 512-bit message blocks that have been buffered, with a maximum message size of 264-1 pieces.

With the use of a passcode consisting of 8 to 63 legible American Standard Code for Information Interchange (ASCII) characters, or a string of 64 hexadecimal integers, PSK is a client authentication approach that creates unique encryption keys for each wireless client. For Juniper Networks wireless networks using Wi-Fi Protected Access (WPA) and WPA2 encryption, PSK is one of two potential authentication methods. Since 802.1X authentication is more common and safe, PSK is not the default authentication method when creating an IoT service profile. An encryption key employing PSK, which does not need 802.1X authentication, may be substituted with a string of 64 hexadecimal integers or a pass of 8 to 63 readable ASCII characters on each Internet of Things node. The intricacy of the server is advantageous for networks in smart homes. A few advantages of employing PSK authentication are as follows:

- Unlike 802.1X authentication, which needs a RADIUS server, PSK authentication is straightforward to set up.
- To accommodate all customers, you can utilize both WPA/WPA2 and PSK at the same time.

In this paper, an enhancement to the CoAP protocol is proposed by adding the integrity to a hash function to check the integrity of the message, in order to decide whether any change has been made to the real message by comparing the original message digest with the message digest received. Hashing is an algorithmic function that maps a fixed-length output to information of any size. People often call this one-way encryption, but it is not exactly true. It produces a hash value when you hash something, which is the fixed-length output that we just described. Two separate pieces of information can never generate the same hash value. The pseudo-code of the proposed Algorithm 1 is shown below, and Table 4 illustrates the symbols in the pseudo-code.

Algorithms 1 pseudo-code of the proposed algorithm

```
Start
        S: computer Ptemp1 = Porig || Seq
        S: computer Hvalue = H(Ptemp1, PSK)
        S: computer Pnew=Ptemp || Hvalue
        S: send Pnew to controller
        c: Compute Hvalue = H(Ptemp2, PSK)
        IF Hvalue = Hvalue THEN
              Authenticate
              Complete process
        ELSE
              Unauthnticate
              Discard
        End-IF
END
```

In particular, different hash values can result from even the slightest tweak to a piece of data. If they are the same, then no modifications are made to the message. Otherwise, the message is a tamper. The SHA224, SHA1, and SHA256 are three related forms of the hash functions evaluated. The proposed security algorithm is based on a simple and efficient key generation procedure. As a result, the time required for the key creation and encryption is reduced. Because IoT sensor nodes are small and have limited power, it is critical to employ a security solution that is less time-intensive. The amount of energy consumed is related to the amount of time it takes to process the data. To put it another way, the longer it takes to encrypt a message, the more energy it takes [38-44].

Table 5 demonstrates the effects of the CoAP protocol implementation of hash functions, displays the energy needed for the Central Processing Unit (CPU) to execute the operation, and the time of performance of each task. The SHA 224 takes a fairly short amount of time to implement.

Table 4. Pseudo Code Symbols

Symbol	Definition
Hvalue	Sensor Hash Value
Seq	Sequence number
Ptemp	Temporary Payload
Pnew	New Payload
CLK	Clock value
||	Concatenate
s	Sensor or mote
c	Controller

PSK	Pre-Shared Key
Porig	Original Payload
s	Sensor or mote

In addition, because this method does not employ complex key creation techniques, SHA 224 uses fewer resources to encrypt data.

Table 5. Enhancement Results

S. NO.	Energy Consumption (J/B)	SHA224	SHA1	SHA256
1	ENERGY_TYPE_CPU	163,300	163,801	168,861
	EXECUTION_TIME	11	16	18
2	ENERGY_TYPE_CPU	125,228	163,840	159,975
	EXECUTION_TIME	16	31	29
3	ENERGY_TYPE_CPU	110,026	163,880	168,790
	EXECUTION_TIME	16	26	27
4	ENERGY_TYPE_CPU	142,270	163,840	163,880
	EXECUTION_TIME	21	36	37
5	ENERGY_TYPE_CPU	150,400	163,856	163,380
	EXECUTION_TIME	12	21	20

Lastly, this research compares the energy use of the SHA 224 algorithm to that of the hash algorithms SHA 256 and SHA 1.

Any size message may be fed into a hash function, and it will produce a fixed-size result. A little alteration may affect how the original text computes a different hash result. Tests of the consistency of data transit between nodes is their main purpose. SHA224 runs faster than other hash functions; Figure 4 displays the hash function's run time, with the trial number shown on the x-axis.

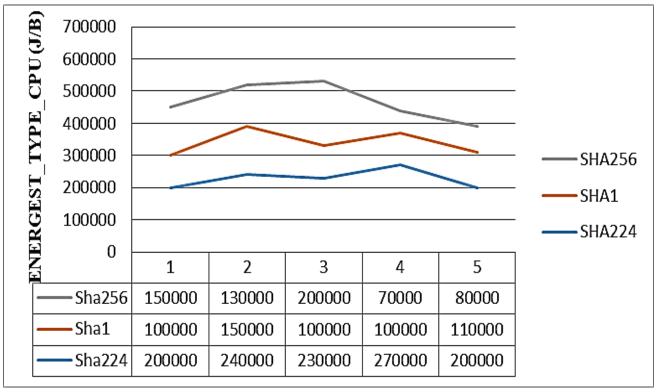


Figure 4. The hash function for calculation of Energy consumption

In this paper, the suggested SHA 224 is evaluated in terms of its execution time against hash algorithms such as SHA 256 and SHA-1. SHA 224 is a new hash algorithm that uses more calculation steps than SHA 256 or SHA-1 in less time. SHA224 is also thought to be more resistant to collisions than SHA 256 and SHA-1. Figure 5 shows that the sha224 takes a low amount of CPU resources, and the x-axis shows the trail number.

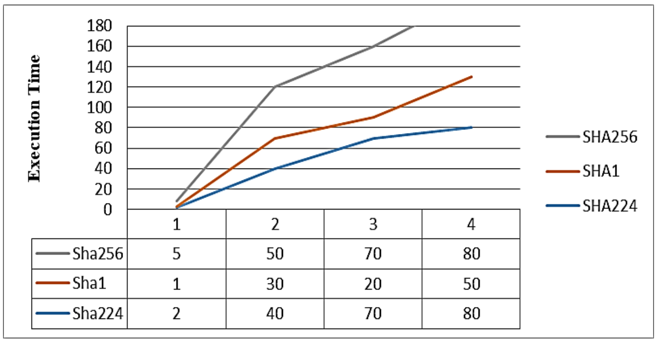


Figure 5. Execution Time of the Hashed Function

The suggested SHA 224 algorithm requires less energy to implement than traditional security methods, as shown by Figures 4 and 5. Moreover, SHA 224 uses less energy as it uses a straightforward and effective key generation procedure. Therefore, low-power Wi-Fi in WSNs with the Internet and the proposed SHA 224 are used by the proposed secure IoT-based home automation to provide effective and secure data transmission between several nodes over a wide coverage area.

To achieve a more apparent performance with sufficient loss packets to analyse the impact of the transmission data rate on the throughput performance, the suggested technique uses a wireless error rate (WER) of 0.05 for the wireless connections between the IoT gateway and sensors. Figure 6 shows the average throughput vs the transmission data rate. It can be shown that up to 1.5 Mbps, the throughput increases as the transmission data rate increases, but afterwards decreases. The performance of the network clearly decreases as the congestion loss increases. However, with the same transmission data rate, our proposed SHA224 algorithm continues to surpass the competition.

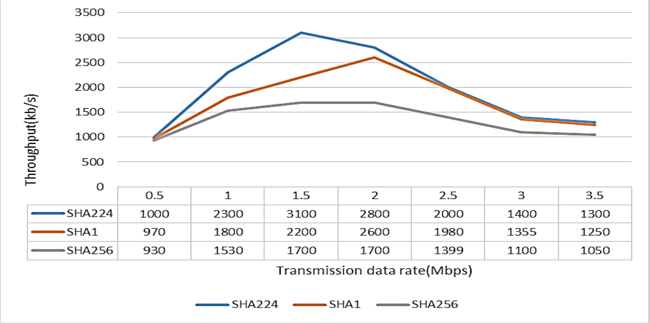


Figure 6. Throughput versus transmission data rate

In order to provide a high level of security, current encryption techniques are developed with the complexity of an arithmetic operation. These mathematical operations bring forth issues with efficiency and power usage, though.

According to Figures 7 and 8, the application of the updating inputs in the columns is switched from diagonals to zigzags before the alternate form. This new updating process order causes a greater dissemination of the inputs, which raises the difficulty of defense against attacks. One of these methods, the ChaCha cypher, has gained notoriety when Google used it in a number of applications. The two counterwords are set to zero, and the key and nonce are given. The 64-byte output's first 32 bytes are saved and used as the Poly1305 one-time key. The remaining output is discarded. The plaintext is encrypted by overflowing into the second counterword and incrementing the first counter word after each block by XORing it with the output of the ChaCha20 function invocations as required. In actuality, the TLS plaintext size constraints ensure that the first counter word never overflows. The proposed cipher suites are lightning fast as compared to SHA-224, SHA-256, and SHA-1. As the simulation starts in Contiki Cooja, decryption takes less time, which means faster website rendering and a longer battery life. Although the cipher element of TLS may not be the most power-hungry part of the protocol, using fewer CPU duty cycles (as shown in Figure 9) for encryption saves power, especially when working with large files. A 256-bit key and a 32-bit nonce are used by ChaCha20 to create a key stream, which is XORed with the plaintext stream. It is especially well-suited to low-power devices and real-time communications, because it operates three times faster in software than AES. The fundamentals of the ChaCha20 have been studied in order to develop a new key stream generator for key production that takes into consideration the reduction of difficult phases and boosting of security levels. IoT data will be encrypted using the generated keys. We refer to the new method as Super ChaCha Lightweight Stream Cypher, which is detailed in Algorithm 2 and has 10 rounds that are finally condensed into.

Algorithm 2 Super ChaCha Lightweight Stream Cypher.

TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 = {0xCC, 0xA8}

TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 = {0xCC, 0xA9}

TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 =0{0xCC, 0xAA}

TLS_PSK_WITH_CHACHA20_POLY1305_SHA256 = {0xCC, 0xAB}

TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256 = {0xCC, 0xAC}

TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256 = {0xCC, 0xAD}

TLS_RSA_PSK_WITH_CHACHA20_POLY1305_SHA256 = {0xCC, 0xAE}

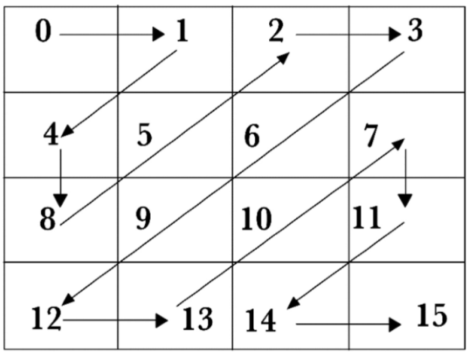


Figure 7. Zig Zag Form

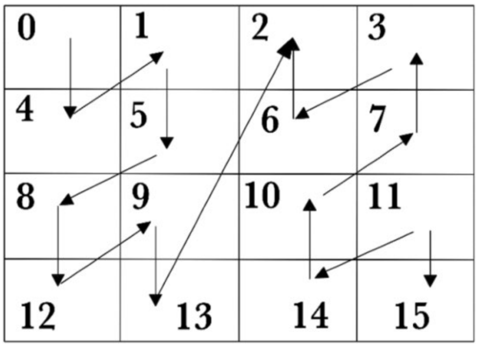


Figure 8. Alternate form

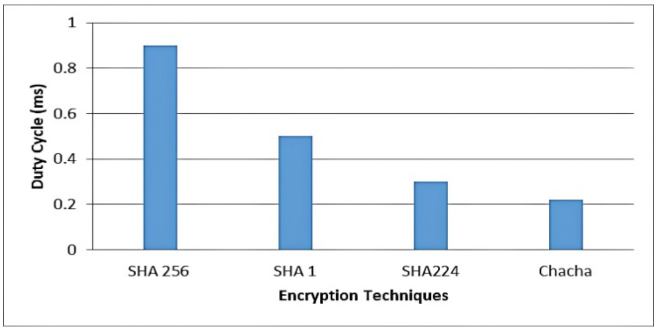


Figure 9. The computation time of encryption

The data collected and tracked by the sensors in the proposed work would contribute to energy saving while providing a high level of communication security. Compared to earlier research, it has created a system with IoT sensors that better maintains smart home equipment. Before doing anything, the user must abide by the device specifications and have direct access to the sensor data in the system we are creating.

6. Conclusions

The technology known as the internet of things has the potential to completely transform a number of aspects of our lives, including entertainment, healthcare, transportation, and our relationships with the government. Along with this wonderful potential, there are many noteworthy problems. As we struggle to create laws, regulations, and governance that shape this progress without strangling innovation, the number of devices and the rate at which they are growing pose threats to our security and liberties. IoT technologies benefit and threaten smart homes. IoT-based smart homes are subject to a number of security threats from inside and outside. A smart home or device breach could compromise a user's privacy, personal information, and safety. Thus, smart houses must be made safer and more livable. Before implementing security, all the relevant underlying issues must be identified. This study provided a secure IoT-based smart home algorithm. Due to the limited computing capability of IoT sensor nodes, an efficient security solution based on effective key generation, which meets all the essential data security criteria while requiring minimal processing time for data encryption, is critical. Smart home solutions should prioritize safety and security. To prevent cyber-attacks, smart homes should have security and privacy features such as locks. This work gives the CoAP protocol credence. A Contiki OS smart home software uses three hash methods to establish credibility. SHA224 is the greatest smart home algorithm for energy, throughput, and time. Chacha cipher suites are much faster than SHA-224, SHA-256, and SHA-1 in terms of duty cycle.

With 5G technology, the planned IoT platform would be used for medical monitoring, emergency responses, agriculture, healthcare, energy management, and industrial automation. IoT data security may improve with authentication and hybrid cryptography. Network security assaults are needed to verify data security solutions. The simulations continue. Thus, IoT device experiments will be needed.

Funding: This research received no external funding.
Data Availability Statement: data will be available on the request
Conflicts of Interest: The authors declare no conflicts of interest.

References

[1] Braghin, C.; Lilli, M.; Riccobene, E. A Model-based approach for Vulnerability Analysis of IoT Security Protocols: The Z-Wave case study. Comput. Secur. 2022, 127, 103037.

[2] Alwahedi, F., Aldhaheri, A., Ferrag, M. A., Battah, A., & Tihanyi, N. (2024). Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. Internet of Things and Cyber-Physical Systems..

[3] Hossain, M., Kayas, G., Hasan, R., Skjellum, A., Noor, S., & Islam, S. R. (2024). A Holistic Analysis of Internet of Things (IoT) Security: Principles, Practices, and New Perspectives. Future Internet, 16(2), 40.

[4] Singamaneni, K. K., Budati, A. K., & Bikku, T. (2024). An Efficient Q-KPABE Framework to Enhance Cloud-Based IoT Security and Privacy. Wireless Personal Communications, 1-29.

[5] Shahidinejad, A., & Abawajy, J. (2024). An all-inclusive taxonomy and critical review of blockchain-assisted authentication and session key generation protocols for IoT. ACM Computing Surveys, 56(7), 1-38.

[6] Aboshosha, B.; Dessouky, M.; Ramadan, R.; El-Sayed, A.A. LCA- Lightweight Cryptographic Algorithm for IoT Constraint Resources. Menoufia J. Electron. Eng. Res. 2019, 28, 374–380. https://doi.org/10.21608/mjeer.2019.67379.

[7] Xu, R., Jin, W., & Kim, D. H. (2022). Knowledge-based edge computing framework based on CoAP and HTTP for enabling heterogeneous connectivity. Personal and Ubiquitous Computing, 1-16.

[8] Stolojescu-Crisan, C.; Crisan, C.; Butunoi, B.P. An IoT-based smart home automation system. Sensors 2021, 21, 3784.

[9] Mahdi, M.S.; Hassan, N.F.; Abdul-Majeed, G.H. An improved chacha algorithm for securing data on IoT devices. SN Appl. Sci. 2021, 3, 1–9. https://doi.org/10.1007/s42452-021-04425-7.

[10] Sarker, A., Kermani, M.M., Azarderakhsh, R. Error Detection Architectures for Ring Polynomial Multiplication and Modular Reduction of Ring-LWE in $\boldsymbol {\frac {\mathbb {Z}/p\mathbb {Z}[x]}{x^{n}+ 1}} $ Benchmarked on ASIC. IEEE Trans. Reliab. 2021, 70, 362–370.

[11] Ahn, J.; Kwon, H.-Y.; Ahn, B.; Park, K.; Kim, T.; Lee, M.-K.; Kim, J.; Chung, J. Toward Quantum Secured Distributed Energy Resources: Adoption of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). Energies 2022, 15, 714. https://doi.org/10.3390/en15030714.

[12] Desnanjaya, I.G.M.N.' Arsana, I.N.A. Home security monitoring system with IoT-based Raspberry Pi. Indones. J. Electr. Eng. Comput. Sci. 2021, 22, 1295.

[13] Bassoli, M.; Bianchi, V.; De Munari, I. A Plug and Play IoT Wi-Fi Smart Home System for Human Monitoring. Electronics 2018, 7, 200. https://doi.org/10.3390/electronics7090200.

[14] Wenbo, Y.; Quanyu, W.; Zhenwei, G. Smart home implementation based on Internet and WiFi technology. In Proceedings of the 2015 34th Chinese Control Conference, Hangzhou, China, 28–30 July 2015; pp. 9072–9077. https://doi.org/10.1109/chicc.2015.7261075.

[15] Sarker, A.; Kermani, M.M.; Azarderakhsh, R. Fault Detection Architectures for Inverted Binary Ring-LWE Construction Benchmarked on FPGA. IEEE Trans. Circuits Syst. II Express Briefs 2020, 68, 1403–1407. https://doi.org/10.1109/tcsii.2020.3025857.

[16] Peng, J.Y.; Zhang, D.; Deng, Y.W.; Li, R.Y.M. A Review on Sustainable Smart Homes and Home Automation in TMall, Baidu and Know the Topic: Big Data Analytics Approach. In Current State of Art in Artificial Intelligence and Ubiquitous Cities; Springer: Singapore, Singapore, 2022; pp. 155–167.

[17] Li, R.Y.M.; Shi, M.; Abankwa, D.A.; Xu, Y.; Richter, A.; Ng, K.T.W.; Song, L. Exploring the Market Requirements for Smart and Traditional Ageing Housing Units: A Mixed Methods Approach. Smart Cities 2022, 5, 1752–1775.

[18] Guin, U.; Singh, A.; Alam, M.; Canedo, J.; Skjellum, A. A secure low-cost edge device authentication scheme for the internet of things. In Proceedings of the 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID), Pune, India, 8–10 January 2018; pp. 85–90.

[19] Pirbhulal, S.; Zhang, H.; Alahi, M.E. A novel secure IoT-based smart home automation system using a wireless sensor network. Sensors 2017, 17, 69.

[20] Kang, W.M.; Moon, S.Y.; Park, J.H. An enhanced security framework for home appliances in smart home. Hum.-Centric Comput. Inf. Sci. 2017, 7, 1–12. https://doi.org/10.1186/s13673-017-0087-4.

[21] Lachner, C.; Dustdar, S. A Performance Evaluation of Data Protection Mechanisms for Resource Constrained IoT Devices. In Proceedings of the2019 IEEE International Conference on Fog Computing (ICFC), Prague, Czech Republic, 24–26 June 2019; pp. 47–52. https://doi.org/10.1109/icfc.2019.00015.

[22] Patil, S.; Joshi, S.; Patil, D. Enhanced Privacy Preservation Using Anonymization in IOT-Enabled Smart Homes. In Smart Intelligent Computing and Applications, Smart Innovation System, and Technologies; Springer: Singapore, Singapore, 2020; https://doi.org/10.1007/978-981-13-9282-5_42.

[23] Dhiman, G.; Oliva, D.; Kaur, A.; Singh, K.K.; Vimal, S.; Sharma, A.; Cengiz, K. BEPO: A novel binary emperor penguin optimizer for automatic feature selection. Knowl.-Based Syst. 2020, 211, 106560. https://doi.org/10.1016/j.knosys.2020.106560.

[24] Kponyo, J.J.; Agyemang, J.O.; Klogo, G.S.; Boateng, J.O. Lightweight and host-based denial of service (DoS) detection and defense mechanism for resource-constrained IoT devices. Internet Things 2020, 12, 100319. https://doi.org/10.1016/j.iot.2020.100319.

[25] Rana, A.K.; Mullana, H.I.S.A.M.; Sharma, S. Enhanced Energy-Efficient Heterogeneous Routing Protocols in Wsns for IOT Application. Int. J. Eng. Adv. Technol. 2019, 9, 4418–4425. https://doi.org/10.35940/ijeat.a1342.109119.

[26] Bonkra, A.; Bhatt, P.K.; Rosak-Szyrocka, J.; Muduli, K.; Pilař, L.; Kaur, A.; Chahal, N.; Rana, A.K. Apple Leave Disease Detection Using Collaborative ML/DL and Artificial Intelligence Methods: Scientometric Analysis. Int. J. Environ. Res. Public Health 2023, 20, 3222. https://doi.org/10.3390/ijerph20043222.

[27] Douiba, M.; Benkirane, S.; Guezzaz, A.; Azrour, M. An improved anomaly detection model for IoT security using decision tree and gradient boosting. J. Supercomput. 2022, 79, 3392–3411. https://doi.org/10.1007/s11227-022-04783-y.

[28] Dhawan, S.; Gupta, R.; Bhuyan, H.K.; Vinayakumar, R.; Pani, S.K.; Rana, A.K. An efficient steganography technique based on S2OA & DESAE model. Multimedia Tools Appl. 2022, 82, 14527–14555. https://doi.org/10.1007/s11042-022-13798-9.

[29] Apostu, S.A.; Vasile, V.; Vasile, R.; Rosak-Szyrocka, J. Do Smart Cities Represent the Key to Urban Resilience? Rethinking Urban Resilience. Int. J. Environ. Res. Public Health 2022, 19, 15410. https://doi.org/10.3390/ijerph192215410.

[30] Fotohi, R., & Aliee, F. S. (2021). Securing communication between things using blockchain technology based on authentication and SHA-256 to improving scalability in large-scale IoT. Computer Networks, 197, 108331.

[31] Rana, S.K.; Rana, S.K.; Nisar, K.; Ibrahim, A.A.A.; Rana, A.K.; Goyal, N.; Chawla, P. Blockchain Technology and Artificial Intelligence Based Decentralized Access Control Model to Enable Secure Interoperability for Healthcare. Sustainability 2022, 14, 9471. https://doi.org/10.3390/su14159471.

[32] Mahdi, M. S., Hassan, N. F., & Abdul-Majeed, G. H. (2021). An improved chacha algorithm for securing data on IoT devices. SN Applied Sciences, 3(4), 429.

[33] Farooqi, N., Gutub, A., & Khozium, M. O. (2019). Smart community challenges: enabling IoT/M2M technology case study. Life Science Journal, 16(7), 11-17.

[34] Nikolov, N. (2020, September). Research of MQTT, CoAP, HTTP and XMPP IoT communication protocols for embedded systems. In 2020 XXIX International Scientific Conference Electronics (ET) (pp. 1-4). IEEE.

[35] Sharad, Kaur, E. N., & Aulakh, I. K. (2020). Evaluation and implementation of cluster head selection in WSN using Contiki/Cooja simulator. Journal of Statistics and Management Systems, 23(2), 407-418.

[36] Mostafa, A., Lee, S. J., & Peker, Y. K. (2020). Physical unclonable function and hashing are all you need to mutually authenticate iot devices. Sensors, 20(16), 4361.

[37] Rao, V., & Prema, K. V. (2019, December). Comparative study of lightweight hashing functions for resource constrained devices of IoT. In 2019 4th International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS) (pp. 1-5). IEEE.

[38] Anastasova, M.; Azarderakhsh, R.; Kermani, M.M.; Beshaj, L. Time-Efficient Finite Field Microarchitecture Design for Curve448 and Ed448 on Cortex-M4. In International Conference on Information Security and Cryptology; Springer: Cham, Switzerland, 2023; pp. 292–314. https://doi.org/10.1007/978-3-031-29371-9_15.

[39] Anastasova, M.; Azarderakhsh, R.; Kermani, M.M. Fast Strategies for the Implementation of SIKE Round 3 on ARM Cortex-M4. IEEE Trans. Circuits Syst. I Regul. Pap. 2021, 68, 4129–4141. https://doi.org/10.1109/tcsi.2021.3096916.

[40] Sanal, P.; Karagoz, E.; Seo, H.; Azarderakhsh, R.; Mozaffari-Kermani, M. Kyber on ARM64: Compact implementations of Kyber on 64-bit ARM Cortex-A processors. In Proceedings of the Security and Privacy in Communication Networks: 17th EAI International Conference, SecureComm 2021, Virtual, 6–9 September 2021; pp. 424–440

[41] Niasar, B.M.; Azarderakhsh, R.; Kermani, M.M. Cryptographic accelerators for digital signature based on Ed25519. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 2021, 29, 1297–1305.

[42] Verma, R. K., Kumar, A., Pattanayak, P., Chauhan, P. S., Bali, V., & Mathur, S. (2023, November). Design of L-Shape Slot Loaded Rectangular Microstrip Patch Antenna for IoT/WLAN/WiMAX Applications. In International Conference on Trends in Computational and Cognitive

Engineering (pp. 487-497). Singapore: Springer Nature Singapore.

[43] Bali, V., Bali, S., Gaur, D., Rani, S., & Kumar, R. (2023). Commercial-off-the shelf vendor selection: A multi-criteria decision-making approach using intuitionistic fuzzy sets and TOPSIS. Operational research in engineering sciences: Theory and applications, 6(2).

[44] Verma, R. K., Bali, V., Kumar, A., Pattanayak, P., & Sabat, D. (2024, April). Design of Compact T-Shape Slot and Notch Loaded Dual Band Microstrip Antenna for 5G/WLAN Application in S and C-Band. In 2024 IEEE 13th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 88-93). IEEE.