International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Comprehensive Review of Hashing Algorithm Optimization for IoT Devices

Teba Mohammed Ghazi Sami [1], Subhi R. M. Zeebaree [2*], Sarkar Hasan Ahmed [3]

Submitted: 16/02/2023 **Revised:** 18/04/2023 **Accepted:** 09/05/2023

Abstract: The Internet of Things (IoT) has grown dramatically in recent years, it is due to its big impact on people's daily life in critical applications like healthcare, smart homes, smart cities, and smart everything. It also attracts industries and researchers to work on this technology. IoT devices are susceptible to be compromised because of their network capacities, very low computing power, limited battery life, and data storage. The biggest obstacle to the adoption of IoT systems has been recognized as the requirement for lightweight and energy-efficient security solutions to secure smart devices and stored data. In this paper we have reviewed fourty five papers that are related to IoT hashing algorithms and its optimizations, and the papers were published from 2018 and 2022. The papers were then filtered and analyzed. After filtration process, fourteen papers were removed from the list, since they were not totally pertinent to the problem and thirty one papers left for analysis. Among these papers. Among of these thirty one papers, eighteen studies (58%) are focusing on Application layer security, more specifically they focused on Authentication in IoT System.

Keywords: *Internet of Things, IoT, IoT Architecture Layers, hash; hashing, SHA, lightweight, optimized; optimization, optimizing*

1. Introduction

The IoT has been able to bridge the gap between actual industrial surroundings and cyberspace of computing systems because to the advances brought about by the Fourth Industrial Revolution. This calls for a networked system that is capable of connecting and engaging with other systems on the network without the need for human-to-human or human-to-computer interaction. This is in contrast to the scenario that is now being played out in physical industrial settings. This calls for a networked system that is capable of connecting and interacting with other systems on the network. This is required in order to fulfil the requirements of the task that is now being worked on, thus it can't be avoided. Additionally, the widespread utilisation of cutting-edge technologies such as artificial intelligence (AI), big data analytics (BDA), machine learning (ML), and other one-of-a-kind tools has made it a great deal simpler to make efficient use of the data that has been obtained from the various sources that are connected to the network. For example, artificial intelligence (AI), big data analytics (BDA), and ML are all examples of technologies that fall under the category of big data analytics. AI, BDA, ML, and other one-of-a-kind technologies are able to learn from historical data and make accurate predictions about the future. This is why this is the case. This is a very crucial point to bear in mind when it comes to making decisions based on the facts [1]. The Internet of Things, sometimes abbreviated as IoT, is the most cutting-edge advancement in internet technology that is presently accessible. It is sometimes referred to as IoT. As a result of this, a wide variety of electronic devices, each of which has its own individual set of qualities, are able to interact with one another and collaborate effectively. On the Internet of Things, there is a digital representation of every conceivable piece of real-world hardware and software. This includes both physical devices and computer programmes. This encompasses both the actual hardware and the software used on computers [2] .

Kevin Ashton is generally acknowledged as the person who is responsible for the first use of the phrase "Internet of Things" in 1999. The Internet of Things (IoT) has seen a rise in adoption rates in recent years, which may be attributed, in part, to the widespread availability of high-performance wireless technologies. Without RFID tags and sensors, the Internet of Things will be impossible to operate properly. A computer programmer has the ability to track the whereabouts of an RFID tag even after it has been permanently attached to a piece of equipment or an item. Radio frequency identification (RFID) tags may be located, read, and identified with the assistance of a device known as an RFID reader. Radio frequency identification is what is meant by the acronym RFID. Because it uses chips on both the transmitting and receiving ends that are on the microscale, radio frequency identification (RFID) technology is able to communicate across very long

1 Computer Science Department, Faculty of Science, University of Zakho, Duhok, Iraq; teba.sami@uoz.edu.krd

2 Energy Eng. Dept., Technical College of Engineering, Duhok Polytechnic University, Duhok, Iraq; subhi.rafeeq@dpu.edu.krd

3 Network Department, Sulaimani Polytechnic University/ Iraq; sarkar.ahmed@spu.edu.iq

Corresponding Email: subhi.rafeeq@dpu.edu.krd

distances [3,4]. According to the information presented on Forbes.com, it is projected that the global market for the Internet of Things would reach a value of $267 billion by the year 2020. The research firm Gartner predicts that in the year 2017, there will be an investment of $273 billion and the networking of 8.4 billion objects. In addition, there will be a total number of connected devices of 8.4 billion. In 2017, customers will be introduced to 8.4 billion brand-new things, which is a 31% increase compared to the previous year's total number of brand-new products launched. The Internet of Things has a wide variety of applications, some of which include cutting-edge medical technology (including intelligent ambulances), energy conservation, smart cities with infrastructure, smart farming and agriculture, vehicle-to-vehicle Internet (IoV), always-connected autonomous vehicles, smart homes, intuitive distribution networks, and smart farming and agriculture. Other applications include the vehicle-to-vehicle Internet (IoV), always-connected smart homes, and intuitive distribution networks. These are but a few of the many possible uses. The Internet of Things is being put to use in a variety of different ways, but these applications are some of the more common ones [5] .

According to a report published online, the number of linked IoT devices will reach 14.4 billion by the end of 2022 [6]. Insecure communication of these devices frequently raises worries about the security of the data they gather and transmit, inviting hackers and risking data security. To address these issues, a higher-level security system is required to prevent unwanted access [7] . Systems that are part of the Internet of Things (IoT) need high levels of connectivity as well as power [8] . This is essential because to the unique qualities of these systems, as well as the vast number of devices that produce copious amounts of data, since both of these factors make it vital for this to take place.The Internet of Things (IoT) is going to need a massive amount of connectivity in addition to a constant supply of energy to power all of the many technologies that will comprise it. Because of the limitations in their processing power, storage capacity, and network connection, these devices are susceptible to a wide variety of different kinds of assaults. As a direct result of this, these assaults are susceptible to being broken into. As a direct result of this, the challenges of privacy and security have been brought to the forefront as the two most essential concerns with internet-connected gadgets. [9] .

The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST), which is an entity that specialises in standardisation and technology. It is composed of three unique sets of cryptographic hash functions, each of which is referred to by its own number: SHA-1, SHA-2, and SHA-3 accordingly. The SHA-1 hashing algorithm is gradually being phased out of use because of the problems that are associated with using it. To the general public for the very first time in the year 2001, the concept that SHA-2 need to be used instead of SHA-1 was given for the very first time. The National Institute of Standards and Technology (NIST) made the announcement in 2015 that the SHA-3 hashing algorithm will be the most recent version of the algorithm to be released. The phrase "secure hashing algorithm 3" is abbreviated as "SHA-3." Despite this, SHA-3 is not yet extensively utilised, and the key reasons for this may be split down into two categories: security concerns and implementation issues. To begin, there has not been discovered a flaw within SHA-2 that is believed to be particularly damaging. This is the current situation as of the time of this writing. Second, while SHA-2 is still frequently used for system security, SHA-3 utilises a fundamentally different hardware architecture. This is despite the fact that SHA-2 is still widely utilised. Despite the fact that SHA-2 is still being used extensively, this is the case. This is the situation even though a sizeable population is now using SHA-2 as a cryptographic hashing algorithm. We will be required to make that step in order to facilitate the transition from SHA-2 to SHA-3, which is critical given the large investment in new hardware infrastructure that would be required for the transition. Due to the fact that this is the situation, the study of SHA-2 and SHA-3 is now being carried out independently while at the same time concurrently. SHA-2 will be used by older systems since it is the most widely used hashing algorithm; however, brand new systems may choose to implement SHA-3 as their hashing algorithm of choice. Systems that are built on earlier foundations will continue to make use of the SHA-2 hashing algorithm. The outstanding long-term collision resistance that it offers makes SHA-2 one of the most trustworthy hash algorithms that can be employed in modern computer settings. This is why it is still one of the most used hash algorithms. A wide variety of different uses are found for the Secure Hash Algorithm 2 (SHA-2) family of hashing algorithms, which includes SHA-224, SHA-256, and SHA-512, amongst others. These applications include a wide range of possible uses, from the mining of cryptocurrencies to the operation of devices that are connected to the Internet of Things (IoT). Because of the considerable gains in speed and efficiency that they deliver, hardware implementations of SHA-2 functions are becoming increasingly prevalent. This is due to the fact that hardware implementations give. In addition to being able to meet performance and cost requirements, SHA-2 hardware has to be flexible enough to accommodate a wide variety of different applications. In addition to the requirements that it must fulfil in terms of performance and cost, this need is a must [10].

2. Internet-of-Things (IoT)

In the year 1990, the world was made aware of the existence of the world's first remotely operated toaster. This toaster was connected to the Internet of Things in its own unique

way. As a demonstration of the innovation, this toaster was used; it also served as a proof-of-concept device. After a further ten years of waiting, the first application of intelligent devices to see widespread use was in the area of radio frequency identification (RFID), which is based on the tracking of commodities. Consumers have a better understanding of the Internet of Things (IoT) thanks, in large part, to the efforts of industry giants such as Cisco, IBM, and Ericsson. These companies are all considered to be leaders in their respective fields. Only two instances of the Internet of Things devices that have become commonplace are thermostats that have the capability to automatically manage the temperature and sensors that are put in factories in order to monitor the operation of equipment. These are only two examples of the Internet of Things devices that have become the standard. It is anticipated that by the year 2023, personal computers will account for fifty percent of all devices that are capable of connecting to the internet, and that connections made between computers would account for fifty percent of all traffic on the internet. This forecast is based on the fact that between now and 2023, it is anticipated that the number of linked devices will quadruple on an annual basis. Each and every minute, the world wide web serves as the entry point for hundreds of brand-new pieces of technology as they establish their very first connection to the internet. There has been a rapid surge in the number of electronic devices that are capable of talking with one another during the last few years. There are already over 31 billion linked devices, and it is anticipated that another 4 billion will be connected by the end of the year. According to the most recent estimates, this figure is expected to keep rising in the near future. It is anticipated that by the year 2025, the number of devices that are connected to the Internet of Things will have increased by a factor of more than three, reaching a total of 75 billion by that time [11]. The Internet of Things is intended to make the process of doing so much more efficient. It establishes a global digital network that any computer on the planet will be able to connect to. These devices are able to communicate with one another and be managed via the use of the internet thanks to their internet connections, the many sensors that they include, and other technologies that they have. Applications that are developed with the help of the Internet of Things can be able to profit from the network strategy. The Internet of Things has a domino effect on almost every other kind of network attack as well [12].

As a result of recent advancements in wireless networking and the declining cost of computing power, the Internet of Things has the potential to one day link practically everything, from a pill to an airliner. This is a possibility because of the Internet of Things. It is conceivable to offer historically thoughtless equipment the capacity to communicate data in real time without the presence of a human operator if the equipment is connected to sensors and those sensors are installed by a professional. The usage of internet access enables these types of devices to acquire this functionality, which may then be used. The Internet of Things helps to foster the development of a culture that is more receptive to novel ideas and adaptable in its method of operation by bridging the divide that exists between the digital and the physical worlds [13].

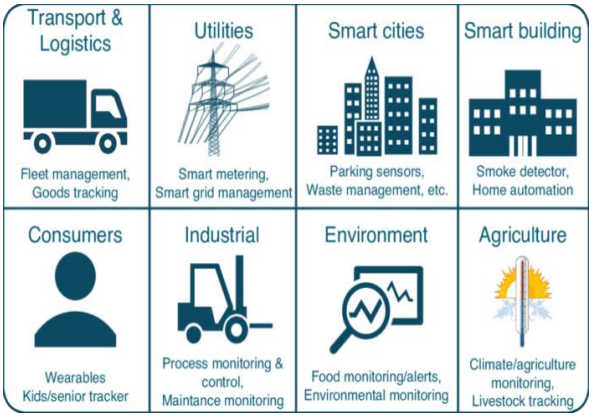


Fig. 1. Internet of Thing (IoT)

3. Methodology

The IoT is one of the fastest-growing technology today. These fast-growing are bringing revolution to the digital world because of the large and various fields in that IoT is covered; the security of these IoT devices is one of the most critical sections in IoT. A lot of research and papers have been done regarding the security of IoT. In our paper, we have used the following keyword for collecting data and searching for related papers which is the following ("IoT" OR "Internet of Things") ("hash" OR "hashing" OR "SHA") ("lightweight" OR "optimized" OR "optimization" OR "optimizing"). We used the IoT keyword to collect general information about the IoT and its approaches. We used the "Hashing" keyword to gather information from research papers about how the data has been hashed and secured. Because we have different device sizes, the performance of these devices is different, and the power of these devices will also change, so we need to search for optimization mechanisms of hashing algorithms depending on the power of the devices. Using those keywords initially, we collected about 45 papers. Then we started filtering and analyzing these papers, and the filtration was done based on the paper's title and abstract. After the filtration, we removed 14 paper because it was not entirely relevant to our topic, after that we have started analyzing these papers based on some criteria, which are the following (content, title, publication year, citation) result of that, we got about 31 papers that are very related and useful to our paper.

4. IoT- Architectural

The Internet of Things does not conform to a standardised design; rather, it is organised in a hierarchical manner and is

separated into communication layers, very similarly to the way that conventional information technology networks are built. This is because the Internet of Things is a collection of interconnected networks that are interconnected via the use of various protocols. As a direct result of the research that has been carried out, a number of different models have been developed, some of which comprise three, four, and even five different degrees of complexity. The production of these particular models has been advanced to the point where they are now available [14].

The components that come together to form the Internet of Things may be broken down into four distinct layers, as shown in Figure 2: the sensor layer, the network layer, the processing layer, and the application layer. Figure 2: There are four separate levels that make up the Internet of Things. Image sensors, gas sensors, and water sensors are just a few examples of the types of sensors that may be included in the foundational layer of the Internet of Things. The second layer is made up of connecting devices that have a protocol installed in them, which gives them the ability to interact with the layer that is positioned above them. It is the responsibility of the layer right above the one that is in charge of receiving data from the lowest layer to process all of the information that has been received. The processing layer is made up of all of the servers and edge computing devices that are in charge of carrying out functions like as decision making and categorization. These devices are responsible for the data that is processed by the system. These activities need to be finished in order to fulfil the processing layer's duties and obligations. The system is in charge of carrying out these obligations as its primary duty. Within the overall architectural architecture of the Internet of Things, the application layer is the most sophisticated and complex component. Users at the end of the chain have access to a variety of programmes that have been hand-picked for them based on the requirements of this tier. These choices were determined by the layer that we are currently looking at. Further down on this page, you'll find an explanation that goes into further detail on each of these levels [15].

4.1. Perception / Sensing Layer

On top of this foundation, the architecture of the Internet of Things (IoT) is developed and implemented. It is in charge of collecting all of the information that was obtained from the many sensors that were placed in various parts of the system. In addition to this, the devices that make up this layer are in charge of transmitting and receiving data to and from the layers that are higher up. These tasks are carried out by the devices that make up this layer. Both of the layers are responsible for fulfilling this duty. Regardless of whether the items are in a static or dynamic state, sensors are able to extract certain sorts of information, some examples of which include the characteristics of the things, the atmosphere of the regions immediately around the objects, and the present status of the objects themselves. Because of this, the Internet of Things (IoT) refers to all of the equipment that is used to collect data as "things," including sensors, people, electrical devices, and mobile phones. This includes all of the equipment that is used to gather data [15]. Sensors in IoT devices can be classified in three broad categories as described below [16] .

4.1.1. Motion Sensors

Measure the devices' orientation as well as their change in motion.

4.1.2. Environmental Sensors

Internet of Things devices are equipped with a broad variety of sensors, including as light sensors, pressure sensors, and others, in order for these devices to be able to detect any changes that may take place in the environment in which they are situated. The incorporation of environmental sensors into Internet of Things devices serves the primary purpose of achieving the objective of enabling these devices to make autonomous decisions in response to changes in their surroundings. This is the most important task that environmental sensors are responsible for.

4.1.3. Position sensors

Position sensors are often included into devices that are connected to the Internet of Things. These sensors' primary responsibility is to pinpoint the precise location of the item. Magnetic sensors and sensors that use the Global Positioning System (GPS) are the two types of location sensors that are utilised in Internet of Things devices more often than any others. This is because magnetic sensors and GPS sensors both provide very accurate position information. Magnetic sensors, which are employed rather often in the function of a digital compass, are utilised in order to assist in precisely orienting displays. This may be accomplished by the utilisation of magnetic sensors.

4.2. Transportation / Network Layer

The information that is collected at the sensing layer has the potential to be communicated with the other nodes in the system by using the network layer as a conduit. This is possible because the network layer acts as a conduit. In order for the many devices that make up the Internet of Things to be able to communicate with one another and exchange information, a wide variety of communication protocols are used by these devices. This category includes a wide variety of communication protocols, some of which are as follows: Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRa; cellular network; GSM; WLAN; IPv6; and a few more examples.

4.3. Middleware / Data Processing Layer

It's possible that this place is where a large portion of the intelligence that controls the devices that are linked to the

Internet of Things is generated. Because of the enormous amount of data that was obtained from the sensors in the layer below it, this layer requires a significant number of processing resources in order for it to function properly. These resources must come from a higher layer. Following its collection by the sensing layer, the data is then sent to the data processing layer, where it is subjected to further processing and analysis. The results of previous studies are also saved in the data processing layer of various Internet of Things devices (such as smartwatches, smart home hubs, and so on) in order to improve the overall quality of the user experience. This was done in order to make the gadget more useful to the user. This is done in order to provide the user with an overall better experience, which should be more favourable. The results of the processing of data may, at the discretion of the network layer, be sent to any and all other devices that are connected at the moment in question.

4.4. Application Layer

Is the IoT architecture's top layer. It offers a variety of services to users, including management devices and the device's display interface.

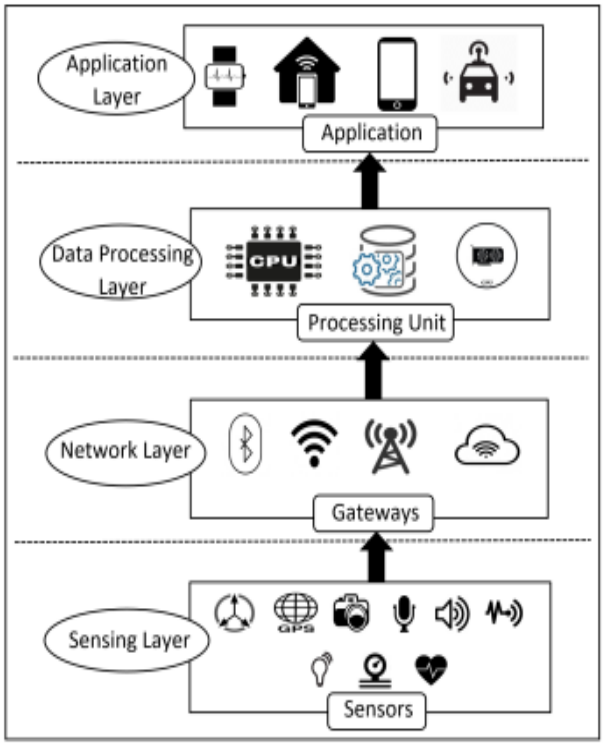


Fig.2. IoT Architecture Layers and Components

This layer is outfitted with a sophisticated decision engine that has the capacity to swiftly adjust to the needs of a wide variety of different business sectors. The healthcare industry, the management of energy resources, and environmental monitoring are just a few examples of these types of businesses. The amount of recently collected data that was used in the training of the intelligent choice system has a direct bearing on the accuracy of the answer result. Since the intelligent decision system was educated, this has been the case ever since. The Internet of Things has the potential to be used in a wide variety of industries, such as intelligent transportation, intelligent housing, personal care, and medical care.

5. IoT Security

As IoT applications grow and adapt, cyber-attacks against those apps are becoming increasingly regular. Securing IoT devices is getting more complex for both manufacturers and customers [17]. The lack of safe devices in the IoT is linked internationally to this action, which is a result of the heavy work of homogeneous sensor nodes in the IoT. It is vulnerable to a variety of flaws that are remembered as one of the most serious issues in the provision of security in additional apps [18]. In the IoT, heterogeneity refers to a wide range of physical resources, including processor computing power and storage capacity, as well as interfaces, frameworks, and rules. The most important worry is the lack of conventional security tools. We envision a future when IoT devices are virtually merged into the landscape and generate vast volumes of data. It is necessary to keep and process data securely in order to make it meaningful and valuable. As a result, in order to develop IoT applications, it is necessary to research IoT security challenges that are distinct from those faced by traditional networks.

These challenges are listed below and depicted in Fig. 3. [11,19,20].

6. Challenges

Fig. 3. IoT security challenges

6.1. Identification

It is necessary for the individual components of an Internet of Things system to be able to recognise and interact with one another for the system as a whole to operate well. They need to have an awareness of the several diverse components that, when put together, comprise the network. In addition to this, in order for entities to interact in the appropriate way, they need to have the ability to discern the difference between friendly and hostile ones. The great majority of items that are connected to the Internet of items will have some kind of connection, whether it is with a specific organisation, place, or corporation. This might take the shape of a direct or indirect relationship. It's possible that this relationship is with any of these items. Consequently, the act of asserting one's right to one's own identity is what is meant when one refers to the "process of identification."

6.2. Confidentiality

As a result of the fact that this information travels via a network's many nodes, it is vital that the flow of data for Internet of Things devices be protected against access by unauthorised third parties. Because of the diverse integration of devices, services, and networks, information that is kept on Internet of Things devices is at risk of having its confidentiality breached by compromised nodes inside the Internet of Things network. It is very necessary to take precautions against the accidental or malicious exposure of sensitive data during both the transmission and storage of the data in question. Device and message access control guarantees that only approved parties, such as servers, clients, devices, administrators, or any other network device, have access to the message. These approved parties might be anybody from a customer to an administrator. They could even be both. When it comes to private information, there should be as little unauthorised interaction with passwords, keys, and other kinds of authentication credentials as is physically possible. This is to prevent sensitive data from being compromised.

6.3. Integrity

Because there are so many possible risks involved with utilising Internet of Things devices, the information that is linked with such devices should not be changed. It is of the highest necessity to carry out a second check in order to guarantee that the data or the message have not been altered in any way while it was being communicated, stored, or processed in any way. This may be done by comparing it to the original version. If data is to keep both its meaning and its value after being saved and processed, then it is very necessary that the data be processed and stored in a secure manner. As a consequence of this, the development of applications for the Internet of Things requires the use of a tool that is capable of providing both integrity and severity.

6.4. Authentication and Authorization

It is essential that the system, along with any potentially sensitive information that may be included inside it, be only accessible to those personnel who have been granted prior authorization to use it. This is essential in order to ensure that the integrity of the internet of things (IoT) is maintained. It is important to verify the identities of any users, sensing devices, and gateway nodes that will be involved before granting access to a protected resource (such as private data, for example). This must be done before access may be granted to the resource. The investigation into whether or not they are who they claim to be is of the highest significance. Because there is such a broad range of IoT-enabled architectures and ecosystems, it is vital to do a second check to validate that the identified user has the required authorization to access the data, resources, or applications that are stored inside the system. This is because there is such a wide variety of IoT-enabled architectures and ecosystems. If the user does not have this authorisation, they will not be able to access the information, resources, or apps.

Access to a resource on the Internet of Things (IoT) may be contingent on factors such as the identity of the device's owner (which may provide additional information on humans who are responsible for particular obligations) or the location (which may determine whether a user is accessing the resource locally or remotely). For instance, the name of the person who owns the device might offer extra information on those who are responsible for certain responsibilities. The combination of these two criteria offers further insight into the kind of people who are required to fulfil particular obligations.

6.5. Privacy

People have the legal right to anticipate that their personal information, starting with the moment it is collected and continuing all the way up until the moment it is deleted, will be handled with the utmost care throughout all stages of the data's lifecycle, beginning with the moment it is gathered and continuing all the way up until the moment it is erased. This is because people have the legal right to expect that their information will be managed with the greatest level of care. Organisations who conduct business in the European Union, for example, are required to comply with the General Data Protection Regulation (GDPR), in addition to other contracts, laws, and regulations. This is because the GDPR entered into effect in the year 2020 in the European Union.

6.6. Availability of Services and Continuity

Availability and continuity in the supply of security services should be assured to avoid any potential operational faults and interruptions. When the system and its services are needed, they must be available. As a result, availability refers to the likelihood that a system (or component) will be operational at a given time. As described by, this encompasses both reliability, i.e., the capacity to uncouple, fix, and modify components without blocking the service

and exceeding preset thresholds, and maintainability, i.e., the ability to achieve specific performance standards in a particular context. Denial-of-service attacks against IoT devices can limit the availability of connected services.

6.7. Resources Constraints

The majority of nodes in an IoT design lack storage space, electricity, and a CPU. They typically communicate over low-bandwidth channels. Threats to IoT systems may result in greater energy usage by overwhelming the network with traffic and depleting IoT devices through duplicate or fraudulent calls.

6.8. Autonomic Control

The main structural distinction between an IoT network and a traditional network is that the former has challenges with management and controllability. As a result, the growth of the IoT has been severely impeded. The IoT connects a vast number of different smart devices. On the one hand, this heterogeneity complicates network and IoT application administration. Rapid proliferation of heterogeneous networks based on IoT may disclose a large number of single-points-of-failure, causing IoT-based services to deteriorate.Objects in an IoT network, on the other hand, should create connections on their own and organize/configure themselves to adapt to the platform they're on. Self-configuring, self-optimizing, self-management, self-healing, and self-protection are some of the approaches and procedures used in this type of control.

6.9. Association

Associating an identity with a particular entity could be dangerous because it could lead to profiling and tracking. As a result, the most important issue is to outlaw such behavior in the IoT and put in place certain protective measures.

6.10. Localization

The next issue is localization, which occurs when computers attempt to determine and log a user's location at a certain point in time and space.Designing approaches for IoT interactions that discourage such behavior is one of the most difficult aspects of IoT security protocols. Profile information of a given individual is frequently used in ecommerce services to forecast interests through linkage with other profiles and such data. A fundamental difficulty is combining corporation interests in profiling and data analysis with user privacy obligations.

The architecture of IoT, several types of attack could target the IoT environment, we focus on the most common and dangers types of them. Table 1 existing threats in IoT systems are examined in four categories based on IoT architecture [11,17,21,22].

Table 2. Existing threads on IoT.

Layers of IoT	**Perception/ Sensing Layer**	**Transportation/ Network Layer**	**Middleware/ Data Processing Layer**	**Application Layer**
Description	RFID Reader, Sensors, Gateway, GPS	2G/3G Communications Network, Internet, Mobile Network, Broad Television Network	Information Processing, Cloud Computing, Data Analytics, Data Storage	Medical Applications, Enterprise Computing, Transportation Applications, Mobile Applications
Threats	Spoofing, Signal/Radio Jamming, Device-tampering/Node-capturing, Path-based DoS Attack (PDoS), Node Outage, Eavesdropping, etc.	Selective Forwarding, Sybil Attack, Sinkhole Attack (Blackhole), Wormhole, Man-in-the-Middle Attack, Hello-flood Attack, Acknowledgement Flooding, etc.	Tampering with Data, DoS Attack, Unauthorized Access, etc.	Sniffer/Loggers, Injection, Session Hijacking, DDoS (Distributed Denial of Service), Social Engineering, etc.
Security Attack	Botnet attacks, Malicious scripts, Virus, Worms, and spyware	RFID spoofing, Routing information attacks	Malicious node injections,	Data breaches, Shared technology vulnerabilities, Cloud computing data security attacks
Solution	Authentication, authorization, cryptography, stenography, img compression, etc.	SSL/TLS, IPSec, PPSK, firewall, IPS, etc.	Authentication, firewall, IPS, access control list, antivirus, selective disclosure, boundary, session inspection, IDS, verification of data, data encryption, etc.	

7. Related Work

The main goal of this paper [2], to stress the need of using cryptographic approaches that have a small footprint in order to protect apps that run on the internet of things. In this article, we take a look at the most promising lightweight cryptography solutions that may be utilised on devices with limited memory, power, and computing capabilities. These solutions can be used to keep data secure while using a minimal amount of processing power and battery. These methods are meant to be implemented along with public key cryptography in order to get the desired results. The reality that many lightweight systems are still in their early stages is obscured by their tremendous expansion in recent years. In addition, the authors provided a summary of and made comparisons between a broad range of lightweight algorithms that had been developed for a number of different hardware platforms.

This work [3], is an effort to present a research that is both comprehensive and up to date of the basic cryptographic building blocks that will be accessible till 2019. This article contains information on 21 distinct lightweight cyphers, some of which include block cyphers, stream cyphers, hash functions, and five distinct flavours of elliptic curve cryptography (ECC), amongst other types of cyphers. In spite of the fact that a number of studies have been conducted on the subject, there has not yet been an exhaustive analysis of the implications that may arise from increasing the size of the LWC pool. This is something that has to be done as soon as possible. An complete examination of LWC cyphers is provided in the most current research that was carried out. This research presents a full view of these cyphers since it takes into account all 54 potential implementations of these cyphers and takes them into consideration. In order to determine which cypher provided the greatest amount of potential advantages, a large variety of criteria, including chip size, energy and power utilisation, the efficiency of the hardware and software, throughput, latency, and figure of merit (FoM), were considered. The results of the study indicate that the Advanced Encryption Standard, often known as AES, is the block cypher that presently provides the maximum degree of security and should be used. When it comes to asymmetric cryptography, the fact that ECC may also be used for authenticating users while simultaneously ensuring non-repudiation makes it an appealing alternative that should be investigated further. There is an ever-growing need for cyphers that are extremely effective, inventive, and as lightweight as is practically feasible. This is due to the fact that the level of complexity of attacks is continually increasing. This method, on the other hand, just outlines the steps that must be performed in order to get authorization; it does not address the issue of regulating the amount of information that is shared in any way.

Cheng et al. in [23], Our approach makes use of a copy of the eight working variables so that they may be loaded from RAM more quickly by using the indirect addressing mode with displacement. This is accomplished by employing a duplicate of the variables. In order to achieve this goal, first a duplicate of the variables must be created, and then the copies must be displaced. In addition, the code for the compression function is hand-optimized in Assembler, and in order to achieve the highest possible level of efficiency, it makes use of both the ldd and std instructions. Within the scope of this body of work, we provide the first highly optimised Assembler implementation of the SHA-512 hashing algorithm for the ATmega family of 8-bit AVR microcontrollers. It was decided to utilise the SHA-512 hashing algorithm since it is the one that is most often selected by users. They were successful in achieving the desirable balance of adequate speed and adequate code preservation by avoiding unrolling the primary loop of the compression algorithm. Because of this, they were able to restrict the total amount of lines of code to a manageable level. They were successful in achieving both of these objectives as a direct result of this factor. In order to carry out the compression function, an 8-bit microcontroller equipped with an AVR ATmega128 has to have somewhat less than 60k clock cycles available. This corresponds to a compression rate of around 467 cycles per byte when expressed in terms of clock cycles. Because of this, the total length of time required to complete the operation is going to grow to about 4.35 times what it was initially expected to take. This increase in speed was made feasible by the use of a one-of-a-kind approach that repeatedly repeats the working variables without the necessity that loop unrolling be carried out in between each iteration of the process. This improvement in speed was made possible by the use of a method that iteratively repeats the working variables. It was decided to do this in order to make the four sigma processes more efficient and cut down on the amount of money that was spent on accessing memory (SRAM). The decision to do this came about as a result of a discussion. The SHA-512 acceleration on AVR and the optimisation strategy that will be addressed in the following paragraph both offer a broad range of possible applications that may be utilised in a wide variety of settings and settings. One of these applications is the optimisation approach, which will be examined in more detail in the following paragraph. It is not difficult to modify it in such a way that it may be used with other architectures that make use of indirect addressing (for example, MSP430 and ARM), and it can be useful for other cryptosystems that need word-by-word rotation of working variables or a state. In light of these results, they developed the hypothesis that low-powered Internet of

Things (IoT) devices will progressively begin to make use of SHA-512 (in addition to cryptosystems that are based on SHA-512, such as EdDSA). This hypothesis was based on the fact that they observed that SHA-512 is used in cryptosystems such as EdDSA.

The authors of [24] Another user offered the possibility of coining an abbreviation for this word, and they recommended token-based lightweight user authentication as a candidate. a protocol for authenticating users and conducting critical negotiations on low-power devices. Users make connections with gateways, which are entrusted with regulating the entire pool of resources that are accessible to the users. Users create connections with gateways. The smart devices themselves are the only item that imposes restrictions on the resources that may be accessed at any given time. In order to facilitate the process of transferring session tokens amongst the many participants that are taking part in the activity, the protocol makes use of symmetric cryptography in conjunction with one-way hash functions. This is done in order to lessen the likelihood that the tokens will be taken without permission. In addition, Perfect Backward Secrecy, which is more often known to as PFS and stands for Perfect Forward Secrecy, is used throughout the process of generating new keys for each session. According to the conclusions of the performance research that was recently made public, it competes very well with other solutions that are currently available on the market for user authentication in situations that include the Internet of Things.

Agrawal et al. [25] , A summary of the CAESAR competition that will take place in 2019 was just presented in an article that was just made available to the public. This research assessed lightweight AE algorithms that were released after the year 2010, which is a noteworthy year because it marks the beginning of a new trend in the field of lightweight cryptography. Additionally, the year 2010 is notable because it indicates the beginning of a new trend in the area of lightweight cryptography. In addition to this, it emphasises the necessity for LWC in circumstances in which there is a limited supply of resources. There were a total of 17 distinct lightweight authenticated systems investigated in this research, nine of which were actually entered into the CAESAR challenge to be analysed. In the course of the study, both the hardware and the software were analysed into very minute detail in order to offer proof on the efficiency with which the lightweight AE techniques functioned.

In [26], Aghili et al. created a one-of-a-kind secure lightweight RFID authentication protocol (SecLAP) by resolving the flaws in the Lightweight RFID Mutual authentication (LRMI) standard in order to solve the problem of authentication in healthcare IoT networks. This was done in order to overcome the issue of authentication in healthcare IoT networks. Because of this, both the medical internet of things' privacy and its general safety are improved, which is a direct result of this. They did research to prove that the SecLAP technique is secure in both directions of communication and is resistant to attacks such as desynchronization, replay, reader/tag impersonation, and tracking. They found that the SecLAP approach is secure in both modes of communication. In addition, they discovered that the mechanism ensured confidentiality in both the sending and receiving sides of the communication. Through the use of BAN-logic, they were successful in ensuring the reliability of SecLAP.

Ahmed et al. [27] Secure hash function combiners that are capable of being implemented in devices that are linked to the Internet of Things have been created as a component of a system to meet the need for increased security. Authentication may now be done out making use of a wide number of distinct elements thanks to this. The development of each hash function starts with the production of a static key, which is then followed by the formation of the idea of a one-time password. Finally, the hash function is created. In order to achieve this objective, these two aspects work in conjunction with one another to complement one another. On the other hand, the approach requires the use of a variety of hash algorithms, each of which may need a large amount of resources. This is especially true in the case of electronic devices that have a limited amount of memory space available to them. In addition to the message authentication code, the simulated authentication process kept track of a variety of other degrees of security. These characteristics included, but were not limited to, resistance to collisions, pseudo-randomness, and one-wayness. Because of this, the authentication system assured that the data was correct and full, as well as that only authorised Internet of Things devices were able to access it. In addition, it restricted access to the data so that only those devices could utilise it. Additionally, it assured that these particular devices were the only ones that could access the data. According to the results of the simulations, CMA performs better than TOTP in terms of the proportion of authentication attempts that are unsuccessful. In addition, the study of CMA indicates a quality of service measurement that is suitable in terms of the calculation time overhead, the throughput, and the packet loss ratio. All of these metrics were measured.

Research was carried out by Dwivedi and colleagues [28] to assess the obstacles that need to be conquered before blockchain technology and wearable sensors can be coupled in a manner that is both efficient and useful. Components of the system include the blockchain network, data storage in the cloud, healthcare providers, smart contracts, and Internet of Things (IoT) wearable

devices that consumers put on for medical reasons. Execution of the algorithms that make up a blockchain takes place on a network architecture that is structured in a hierarchical manner. They provide a method for the protection of networks that are linked to devices that are part of the Internet of Things. This approach calls for the organisation of networks into clusters and the selection of a chief administrator for each cluster. The efficiency of the cluster's other nodes has been improved as a direct result of the efforts that have been put forth by the leader of the cluster. In spite of the fact that this method could resolve issues like as scalability, traffic overhead, and power consumption, the lack of a global consensus mechanism renders the system susceptible to cyberattacks and makes it impossible for it to be sustainable. In addition, because of this vulnerability, the system cannot be maintained indefinitely. The current state of affairs has not altered despite the fact that there is a chance that this strategy may fix these problems.

Sharif et al. [29] For wireless sensor networks (WSNs) that are based on the Internet of Things, it is suggested that an authentication and key agreement method be utilised. It is hoped that this strategy would fix the security issues that existed in the protocols that came before it. The authors of this essay proposed a methodology for the construction of three-factor authentication that can be broken down into a total of four separate processes. The following steps are required to complete these processes: establishing the system, enrolling users and nodes, signing in and authenticating yourself, changing your password, and changing your password again. If you read the post, you will be able to get further knowledge on this strategy. They proved that it was feasible to exploit the protocol in the form of a replay attack and that forward secrecy could not be guaranteed with complete certainty. Additionally, they demonstrated that it was possible to exploit the protocol in the form of a side channel attack. To achieve this goal, it was necessary to demonstrate that it was possible to circumvent the protocol. In addition to this, they provided evidence that there is a method that may be used to avoid the forward secrecy. They demonstrated a technique of key agreement between the user, the gateway, and the sensor, which they said was unbreakable, and they also demonstrated it for the audience. Their approach is safe against common forms of intrusion, including stealing identities, trying to guess passwords, replaying chats, and posing as other users. The formal security analysis that had been performed on this protocol was validated with the assistance of the AVISPA software, and the results of that study were found to be satisfactory. The authors assert that their method is effective and works exceptionally well in settings that are based on WSNs and the internet of things.

This research [30], a novel and efficient two-factor lightweight mutual authentication approach for Internet of Things (IoT) devices that makes use of a programmable Physically Unclonable Function (PUF) as the first factor (cryptographic authentication mechanism). This method was built with the purpose of being used with Internet of Things (IoT) devices in mind from the beginning. While we wait, An entity-based fingerprint is the second component, and its mission is to build a fingerprint that is one-of-a-kind for each entity by aggregating characteristics from several levels of the communication protocol. This component's role is described in more detail below. The generation of an entity-based fingerprint falls within the purview of this component. In addition, the fingerprints of each device are evaluated in both directions, which helps to limit the likelihood of a backdoor login being used. This is done so that any prospective changes may be tracked and kept an eye on. If the fingerprint of an Internet of Things (IoT) device is altered in any manner, then a new round of cryptographic authentication will need to be carried out on the device. This is because the fingerprint is used to verify the identity of the device. This forward-thinking authentication system was designed with the restricted resources, processing capability, and functionality of low-power Internet of Things devices in mind as it was being developed. This was done in order to guarantee that it will function in the correct manner. In order to determine whether or not the procedure that was presented is effective, several current cryptographic authentication methods are used. In addition to this, we provide the findings of a security research as well as a cryptanalysis that demonstrates its resistance to authentication assaults. Both of these studies were conducted by us. Our company was responsible for conducting both of these separate research. The method that has been presented is also modifiable, which means that other features may be added to the second layer in order to increase accuracy even further while also reducing the amount of overhead that is required.

Gupta et al. in [31], Let's have a debate about safe methods of encrypting communications right now since the situation is perfect for it and we can start right now. On this page, many works are dissected, and comparisons are given between the consequences of each of the numerous outcomes created by the various works. After that, they go on to the next step, which consists of generating random numbers using the DLFSR approach and creating hashes with the SPONGE algorithm. This stage is reached after they have completed the previous one. When used in conjunction with a particular LFSR, DLFSR has the potential to provide an exceptionally high degree of unpredictability. SPONGE, on the other hand, has the capacity to increase preimage resistance on greater bit digests. The LFSR methodology is often used in

conjunction with the aforementioned two methodologies, which are described in the previous sentence. As a component of the Dynamic Linear Feedback Shift Register technology, the feedback polynomial goes through a process of dynamic correction. To go a little more, this transition is occurring in the here and now. I hope that helps clarify things.

Gunathilake et al. in [32], The new method of implementing intelligent security applications in low-power data-processing devices that are a component of the Internet of Things (IoT) is referred to as next-generation lightweight cryptography (LWC). This method was developed by the National Institute of Standards and Technology (NIST). Devices that function in accordance with the LoRaWAN specifications may benefit greatly from using this technique for improving their level of security. As a consequence of this, having a discussion about how it operates, the challenges it faces, and the potential applications it will have in the future is very vital. When one examines the findings of the study in light of the research regarding the practicability and efficiency of LWC deployment in 5GN smart cities, one finds that the study yields optimistic results. This is the conclusion that one arrives to when one conducts an analysis of the findings of the study.

Paliwal in [33], voiced his concern about data integrity and confidentiality in IIoT networks. The author stressed that sensitive data acquired by sensor nodes in Wireless Sensor Networks (WSN) should only be available to those who need it. As a result, he offers a hash-based privacy-preserving authentication technique tailored to WSNs. He started by looking at weaknesses in existing systems and determining that they are not suitable for limited contexts. He then went on to design a lightweight hash-based system and compare it to others that were already in use. Paliwal proved his conclusions using formal analysis (Real-or-Random oracle model), simulation, and informal analysis.

Shah and Engineer [34], examine and assess a variety of symmetric and asymmetric lightweight cryptographic algorithms that are simple to employ for hardware and software implementations in IoT devices with limited resources. As a result of the changes in hardware/software and the application, the outcomes of all described algorithms may differ. Any algorithm's results, whether in terms of speed, cycles, or throughput, are unknown. For RFID and IoT applications, only a few algorithms are capable and secure. Several algorithms are resistant to attacks such as the Man-in-the-Center attack, Differential attacks, and Key-IV attacks, among others.

Liu et al. in [35], It has been suggested that the Internet of Things might benefit from a one-of-a-kind PUF-based three-factor anonymous user authentication system. This has been put forth as a possibility. It has been shown, via both formal and informal security analysis using the ROR model, that the proposed protocol is resistant to a broad range of typical assaults, such as those that include physical capture/tempering and tracking respectively. Specifically, the proposed protocol has been proven to be immune to both of these types of attacks. Specifically, it has been shown that the protocol is resistant to certain kinds of assaults. In addition to this, it was found that the existing user authentication procedures for the internet of things (IoT) included a number of holes that enabled for security breaches to occur. These flaws allowed for unauthorised access to be gained by third parties. The protocol that was described, in contrast to the methods that are now being utilised, has the potential to boost the degree of security that is supplied by the Internet of Things. In addition to this, simulations conducted in NS3 demonstrated that the protocol is both applicable and effective in an Internet of Things environment that is representative of the actual world.

For IoT devices, Melki and others [36], Internet of Things (IoT) devices may leverage channel-based parameters and adjustable physical unclonable functions (PUF) in order to provide a new approach of mutual multi-factor authentication that is lightweight and more efficient. Making use of PUF will make it possible to accomplish this goal. This method makes use of simple cryptographic procedures, such as bit-wise exclusive-OR and a one-way hash function. Both of these processes are put to use. A PUF value is a shared secret identity that is produced at random at the beginning of each session. This value is used to authenticate users to a network. PUF values are used in order to block access by unauthorised parties. This value is exchanged between two separate users in a back and forth transaction. Additionally, this protocol takes advantage of the random channel characteristics to give strong resistance against a wide variety of various forms of assaults while simultaneously being relatively simple to put into place. This is accomplished by the use of random channel features. This is achieved by using the capabilities of the random channel in a manner that enables the utilisation of those features. It is crucial because this is the first study of its kind to dynamically authenticate connected devices by employing physical layer security and PUFs. This is the reason why this research is so important. The suggested protocol was tested for its usability as well as its degree of security, and the results showed that it had a low cost for computation as well as communication. Both of these aspects of the protocol were examined.

Wu, Pengfei, et al. in [37], It was suggested that a magnetic resonance-coupled WPT model be used for Internet of Things networks that are powered by UAVs. This technique was successful in resolving the issues that

developed when seeking to optimise energy consumption while also reducing trajectory unpredictability. Because of their compact size, unmanned aerial vehicles (UAVs) often get their power from a battery that is already installed on board. This is common practise. This suggests that there is a limit put on the total amount of power that the unmanned aerial vehicle (UAV) is allowed to use. Therefore, the amount of energy that is used by UAVs has a significant impact on the efficiency with which communication is carried out. This is particularly true in multi-UAV networks, in which the UAVs must collaborate in order to achieve the objective of data-gathering while making the most use of the energy that is available to them. This is especially true in multi-UAV networks, in which the UAVs must cooperate in order to accomplish the aim of data-gathering. When it comes to entirely charging devices that are connected to the Internet of Things, the temperature limitation is no longer an issue that has to be taken into account as a problem that must be solved. The way of supplying energy that has been described is adequate in terms of its adaptability and the extent to which it has the potential to be scaled up.

P-HIP, a lightweight and privacy-preserving authentication technique for HIP-enabled IoT devices, was proposed by Hossain and Hasan [38]. In place of the more common X.509 certificates, the Elliptic Curve Qu-Vanstone (ECQV) encryption mechanism is used in the proposed authentication procedure for the P-HIP. This is due to the increased safety offered by ECQV. P-HIP also lessens the need to exchange certificates, which are often sent across a connection that is prone to data loss. Certificates are exchanged to establish the authenticity of host IDs like public keys and host identification tags. P-HIP minimises the frequency with which these exchanges are required. Certificates are often sent over the network in a significant number of smaller pieces called fragments. Because of this, one of the primary contributors to high computational costs and excessive energy utilisation has been eliminated, which has resulted in both of those problems being mitigated. To exchange keys in P-HIP, however, public-key cryptography is still required, and users must collaborate with a Certificate Authority (CA) that has a solid reputation in order to get ECQV credentials. In addition, users must be able to verify their identities using a trusted third party.

In [39], We came up with a method that has a low amount of overhead and allows remote users to authenticate each other and exchange keys for use in the Internet of Things (IoT). This was accomplished with the help of our innovation. This strategy is going to be used in the not-too-distant future. In order to effectively avoid replay attacks, modification assaults, and man-in-the-middle assaults, the process of authenticating the device used symmetric and asymmetric key encryption, hash codes, and timestamps. These three different kinds of assaults are together referred to as attack vectors. These safety measures were carried out one after the other without interruption. Formal and informal security analyses are used in order to assess the scheme's resistance to attacks such as replay attacks, modification attacks, and man in the middle attacks.

Several researchers used the edge layer to improve the security of IoT systems by addressing critical security requirements like access control, authentication, and privacy protection. The goal of the study in [40], the purpose of this article is to offer a description of the most cutting-edge edge-layer security architecture that is presently available for the Internet of Things. In addition to this, it may be used as a template for the development of innovative approaches to Internet of Things security at the edge of the network. In the first step of this process, an architecture for the Internet of Things that is based on edge computing will be developed. Let's begin by having a look at an Internet of Things design that focuses on the regions that are located on the periphery of the network. Extensive research is now being carried out on security architectural designs, firewalls, intrusion detection systems, authentication and authorisation protocols, and other strategies for keeping information private for Internet of Things devices that are placed on the network's periphery.

The authors [41], Please describe, with reference to the Internet of Things (IoT), how hash-based signature schemes may be classified, created, and identified from one another in comparison to one another. Because this was going to be the primary focus of our work, we made the conscious decision to concentrate in on the challenge of incorporating HBS schemes within the framework of the internet of things. We emphasised how important it is to select appropriate schemes while also taking into consideration the trade-offs that need to be made between the requirements that are specific to the application (such as the signature size and the signing speed) and those that are specific to the platform (such as memory constraints and hardware support for particular hash functions).

Hammi et al. in [42], An authentication system that is built on lightweight elliptic curve encryption has been created. This system was developed primarily for usage with the internet of things (IoT). We were successful in developing a new OTP method by applying the concepts of OTP to a larger variety of settings and scenarios with the assistance of ECC and isogeny. This allowed us to create a unique OTP system. One-time passwords (OTPs) that are based on codes and OTPs that are based on the passage of time are two examples of methods that are not as safe as this one. This technique is the most secure of the three. A protected dialogue that goes in both ways is used to assess whether or not the service connection may be considered

legitimate. It is probable that it will be able to get access to the essential equipment in order for it to carry out its responsibilities as an authorised remote service provider for real-time entities. These responsibilities include providing remote services to various entities. It is possible for it to produce a secure session key that can be used by all of the persons engaged, which would further protect the connection. This would be possible because to the fact that this is possible.

In order to optimise the area-performance tradeoffs of the PHOTON-80/20/16 lightweight hash function, the research presented here offers an iterative design that makes use of a broad selection of FPGA chips manufactured by Altera and Xilinx. FPGAs made by Xilinx are the primary topic of investigation in this study. PHOTON is a cryptographic hash algorithm that was built specifically for use on devices that have limited resources, both in terms of their hardware and their software. PHOTON was developed for use on devices with limited resources in both hardware and software. PHOTON was developed primarily for usage on low-resource devices, both in terms of their hardware and their software, and was built from the ground up for this purpose. Unfortunately, the currently available hardware implementations of the PHOTON hash function are not only very resource-intensive, but they also only give middling performance in terms of frequency and throughput. Given that the PHOTON hash function is one of the most widely used hash algorithms, this presents an issue. It is not impossible to increase the PHOTON design's maximum frequency as well as the throughput; but, doing so would result in the device being physically larger. Due to the fact that this tournament is divided into rounds, every combination and permutation that is even somewhat conceivable is tested concurrently. Because of the way the sponge was designed, in order for it to be able to process a single input message that is comprised of 20 bits, the absorption phase has to be repeated a total of 12 times. After a total of 48 repetitions of the operation for compressing the data, a hash value is produced for the data that has been compressed. The solution that has been suggested delivers improved area-performance trade-offs in comparison to the techniques that are currently being used. This is because the design of the MixColumns module is developed by employing look-up tables rather than the time-consuming computations of the multipliers. This has the effect of reducing the amount of time needed to complete the design. Another option that may be utilised in order to reduce space inside the logic is to use round constants rather than round counters. This is an alternative approach that can be used. It is able to realise its full potential because it makes use of less logical resources to achieve the same level of performance as other systems, which enables it to achieve higher levels of efficiency. The use of the selected FPGA device resulted in a 10.26% improvement in throughput while simultaneously producing a 51.04% rise in operating frequency. An increase in throughput was the driving force behind both of these advancements. In addition, there was an increase in utilisation of logic space that was 7.56 percent greater than it was previously, which contributed to the gain of 60.64 percent. When doing more study, it is necessary to establish whether or not lightweight block cyphers already exist that have an internal architecture that is comparable to the one that is being suggested, or whether or not they do not. In addition to this, it is necessary to carry out the design on actual hardware, improve time analysis, and examine the design space for serialised and pipelined architectures [43].

The authors in [44], Encryption and decryption will become substantially more secure as a result of the implementation of the Elliptic curve ElGamal (EC-ElGamal) technology. In addition, encryption and decryption will become significantly more efficient. In addition to this, they provide a hybrid hashing technique that increases not just the efficiency of the Genetic Algorithm but also the safety that SHA-384 provides. The integration of these two strategies enables the accomplishment of this goal. It is possible that the suggested system of EC-ElGamal-based transaction encryption and enhanced SHA-384-based block hashing might be implemented in order to make LSB more suitable for usage in blockchain-based Internet of Things applications. This would be accomplished by improving the block hashing algorithm. In order to strengthen LSB's defences, this action would be taken. The proposed strategy takes use of a method of encryption that is more advanced than the one that is already in operation, which enables it to achieve large advances in contrast to the system that is now in place. These improvements include a twenty percent reduction in the amount of time required to process transactions, a twenty two percent reduction in the amount of time required to process block validations, an increase of fifty three percent in both the hash rate and the hash quality, and a reduction of seven percent in the amount of storage space that is required.

NABEEL et al. in [45] The Lightweight New Mersenne Number Transform (LNMNT) Hash function is an example of a lightweight cryptographic hashing method that has the potential to be beneficial for Internet of Things applications. There are several characteristics of the suggested LWT hash function that are fully studied in this article. Some examples of these aspects include randomness, ambiguity, diffusion, hash function distribution, and resistance against a broad range of attacks. In order to ensure that the procedure for conducting an evaluation of the randomness can be carried out without any problems, the NIST test suite is used. Comparisons between the LNMNT LWT hash function

and other LWT hash algorithms have been done with regard to the amount of energy that is used, the length of time that is required to carry out the function, the number of cycles that are utilised per byte, and the amount of memory that is utilised. The NMNT is a remarkable diffusion operator that may have incredibly low entropy and can be calculated in a very short amount of time. Additionally, it is capable of being computed. The newly proposed hash function will result in a transformation that has varying lengths, and these lengths will be represented by powers of two. The Cooja Simulator was used in order to carry out research on both the extent of the system's computational complexity and the amount of power that it required to run. Both of these facets were investigated further.

The researchers [46] carried out an in-depth investigation on the various sponge-based lightweight hash products that are now available on the market. In addition to the findings from GLUON, the results of KECCAK, HASH-ONE, QUARK, PHOTON, and SPONGENT were also taken into consideration. In spite of the fact that the writers conducted a comprehensive study, they decided to concentrate their attention on the organisational structures that are the most common in general. There were a total of seven factors that were taken into consideration: security, space needs, digest, throughput, power requirements, and execution cycles. Attention was paid to all of these factors. You may be able to get a comparison of the performance, energy consumption, and safety of a variety of different hash algorithms. Utilising each and every one of the LWT hash algorithms that are now accessible comes with its own unique set of benefits as well as drawbacks. There is no LWT hash algorithm that can handle either the problem of how many resources are needed or the problem of how safe the system has to be. Both of these problems are intractable. As a direct result of this, it will be required to devise a completely novel method for hashing the data associated with LWT.

A lightweight hash-based Blockchain (LightBC) is proposed by Pohrmen et al. in [47] for the IoT based on SPONGENT. It was tested using a Blockchain simulator, and the findings shown that it performed wonderfully for up to 8,000 nodes when compared to a Blockchain that was based on SHA-256. In order to evaluate how well the BlockLite emulation works, we mimicked the behaviour of LightBC. According to the results of the simulation, using SPONGENT results in a significant decrease in the amount of time that is necessary for the manufacture of Blockchain blocks. It is possible that making advantage of these cost reductions will assist in finding solutions to a fair number of the problems that develop throughout the process of introducing Blockchain technology into the Internet of Things.

Through this observational analysis [48], According to proponents of the technology, the fact that blockchains can communicate with one another makes it easier for users to maintain their privacy and safety. It is not necessary to extract it as a consequence of the implementation of the proposed BC; as a result, the produced transactions do not incur any additional processing time as a result of its implementation. As a direct consequence of the proposed BC, it is predicted that the amount of time required to process freshly submitted transfers would not increase by a significant amount. Because the suggested BC does not need any revisions, the implementation of it will not result in any delays in the processing of the created transfers when it is put into effect. It is required to make use of a notion that has been accessible for some time in order to establish a centralised ledger on the level of IoT networks. This is because IoT networks are becoming more complex. Because of this, worries about storage space are addressed, and general security is enhanced as a result of the use of protected hashing. A decentralised blockchain approach is used as the underlying data storage mechanism in the new design, which results in a simplification of the more superior function. This brings the architecture up to date with the most recent and best practises that are currently available. The findings of the simulation reveal that the capacity for data storage first increases by fifty percent, but that after this point, it begins a slow decline that continues until it reaches 256 bytes, at which point it stabilises.

Idriss et al. [49], A lightweight PUF authentication method was shown to exist, as was shown in the demonstration. Even though all that is necessary to finish it is a PUF circuit, a TRNG, and a few bitwise operations, this method is able to successfully finish the challenge-response authentication protocol. This is despite the fact that all that is required to finish it is a PUF circuit. Other lightweight PUF-based protocols do not provide the same level of security as does this protocol, which includes authenticated secret message exchange and mutual authentication as part of its list of security features. Other lightweight PUF-based protocols do not provide the same level of security as does this protocol. As a direct consequence of this, the degree of security provided by other lightweight PUF-based protocols is worse. In addition to this, we also provide a protection that is predicated on the concept of challenge correlations. This defence may be used to guard against assaults that are carried out via MITM. The LPA protocol increases the overall level of security provided by limited Internet of Things devices, which allows a greater range of applications that are suitable for use with such devices. In turn, this enhances the overall degree of security supplied by restricted Internet of Things devices.

The writers in [50], found a number of vulnerabilities in the software that is used to run healthcare IoT devices. LightIoT is a green communications protocol that was created particularly for Internet of Things (IoT)-enabled health informatics. It has a low power consumption and a high level of security. It lays a special emphasis on biological data. LightIoT is a communications protocol that does not negatively impact the natural environment. LightIoT is a three-step process that integrates a mobile gateway, a central server, and low-power wearable devices in order to accelerate the onboarding and authentication operations. LightIoT was developed by IBM. Additionally, the quantity of power that is needed by each individual device is decreased thanks to LightIoT. It is necessary to send two messages to register wearables with a remote server before a secure end-to-end session can be formed for the transfer of data between the entities that are engaging with one another. This is necessary before a session can be made to allow for the exchange of information between the entities. Before constructing a secure connection from end to end, this step has to be completed. Because of the use of lightweight hash functions and XOR operations, LightIoT is in a position to successfully carry out these obligations. As a consequence of this, it is a good solution for the rapid transmission of information that must be supplied on time and cannot afford any delays in its delivery. It is possible to conclude that LightIoT is successful because it has a high degree of resistance to a broad number of attack scenarios, while at the same time requiring relatively little in the way of computational and communication overhead.

In this research [51], As a direct consequence of this, we provide a brand-new method that is very lightweight and that we refer to as "HashXor." This method only requires two lightweight "Hash" operations and three lightweight "Xor" operations in order to protect the identity of IoT devices and the privacy of their users. This approach is considerably more efficient than ECIES in terms of both the length of time it takes to finish the procedure and the amount of computation that it needs. It is also far quicker than a large number of other well-known lightweight solutions that have been presented as viable alternatives for the purpose of protecting user identities in 5G mobile networks. These technological advancements have been offered as potential replacements. For a few of these extra strategies, other ways of approaching the problem have been proposed. Formal and security analyses, both of which were carried out with the assistance of the AVISPA tool, have both validated the scheme and shown that it does not pose any risks when put into practise.

This article [52] security not just of networks in general, but also, and more particularly, the security of healthcare monitoring systems that are built on top of the Internet of Things (IoT) and Cloud Computing. In light of the tight resource constraints that regulate the sharing of health data, we provide a contemporary evaluation of the research field and propose a risk-free method that is based on lightweight cryptography as a workaround. This is done in order to facilitate the exchange of health data. In order to overcome these concerns and ensure the genuineness as well as the integrity of the data, we advised making use of lightweight cryptography and, more specifically, a lightweight hash function that is standardised by NIST. In a similar vein, we suggested that you encrypt any sensitive information that you may have using the symmetric method known as AES-128. This was our recommendation since it is the most secure method currently available. AES-128 is recognised as a lightweight cryptographic method by the National Institute of Standards and Technology (NIST). Because it is both speedy and secure, it is appropriate for use in situations where there is minimal space for data security. Due to the fact that it is both quick and secure, AES-128 is an excellent choice for usage in circumstances in which there is little room for data protection.

The writers in [53], Have a discussion on the benefits and drawbacks of employing each of the several methods that are presently being used to build hashes. There are many different methods. In order to better meet the requirements of the user, a wide variety of various hashing algorithms have been investigated and evaluated objectively. Throughout the whole of this process, particular focus was placed on each of the four distinct hash structures. Blake, JH, Keccak, and SHA are the names that have been given to these structures. The following deductions and conclusions have been reached as a consequence of the findings of a number of separate studies conducted on a broad variety of various facets of the problem. DM contributed to the development of the first one, which was ultimately given the name SHA-2 once it was completed. The chaining variable was made up of eight different words, and the message block included a total of sixteen different words' worth of content. In addition to its two compression operations and its AND operation for bitwise logic, the SHA-2 hashing algorithm also includes a compression operation. Rounding and modular addition are accomplished with the help of this operation, which is also one of the reasons why the method is considered to be very secure. In order to complete the hashing process, SHA-256 only required 32 bits, in contrast to SHA-512, which required 64-bit words to do so. JH's second effort at creating a hash function led in the invention of a compression mechanism that integrated the 256-bit and 512-bit hashing algorithms into a single operation. This allowed JH to create a hash function that was more secure than his previous attempt. It is essential to keep in mind that JH-256 and SHA-256 provide the identical results; however, JH512 is preferable than SHA-512 in terms of

performance. The third architecture, known as Blake, has the capacity to generate 256-bit solutions and offers two levels of compression (respectively, 32-bit words and 64-bit words). Blake's throughput ratio is around fifty percent lower than what it is when compared to SHA-2. The fourth iteration of Keccak's sponge design made use of a fixed permutation, but it was simple enough to be tweaked in such a manner that the overall security strength was surrendered in favour of enhanced efficiency. This was done in order to improve the overall efficiency of the system. Because of this, it was able to produce hash outputs that were either extraordinarily large or extremely little depending on the preferences of the user. The remarkably high level of both the security margin and the efficiency of the hardware implementation should not be underestimated. In addition to that, Keccak now integrates a range of unique chaining modes, all of which are essential components of strong encryption. Keccak's cypher is called Keccak-256. When compared to SHA-2, the throughput that can be reached with Keccak is much higher than what can be achieved with SHA-2.

The authors in [54], created a remote user authentication system based on elliptic curve encryption that is both easy to use and particularly tailored for use with Internet of Things connections. In order to ease the process of authenticating users and transferring keys, the system makes use of symmetric cryptography in conjunction with the cryptographic hash function that is provided by the ECC. Since it only uses cryptographic hash functions and symmetric encryption/decryption, the performance study shows that the solution is both cost-effective and efficient in terms of transmission and processing overhead. This is because it only uses symmetric encryption/decryption and cryptographic hash functions. This is shown by the fact that it only makes use of cryptographic hash algorithms. This is because the only technique used is symmetric encryption and decryption for both the encryption and the decryption processes. The suggested method was subjected to exhaustive rounds of security testing with the assistance of the AVISPA simulation tool, and the results shown that it is capable of withstanding even the most severe assaults on its secrecy.

The authors in [55], provides a variety of recommendations for addressing security issues by using CPS technology, the bulk of which depend on expensive centralised processes or specialised applications of system installations. These guidelines are given due to the fact that CPS technology provides a number of different choices for responding to security risks. Therefore, the development of a reliable method that is capable of overcoming the weaknesses that are built into the CPS technologies that are employed by IoT devices is of the utmost importance. This is a prerequisite that just can not be stressed enough.

The writers in [56], This architecture was intended to safeguard the protocols of the Internet of Things from attacks such as man-in-the-middle attacks, reply attacks, and brute force assaults, among others. In addition to that, the authentication and authorization security architecture for the Internet of Things provided by this architecture is significantly improved. On the IoT device side of the proposed architecture, the enhanced token authentication with identity verification capabilities is coupled with a unique sender verification approach that is based on time stamps. This architecture was conceived with the intention of securing the Internet of Things. As a result of this action being performed, which is intended to ensure that only authentic messages are transmitted to the devices, this step is taken. This combination helps to achieve the aim of removing the requirement that local identity verification mechanisms be implemented in IoT devices, which is one of the purposes of the proposed framework. Another goal of the proposed framework is to simplify the process of implementing IoT devices.

Authors in [57] We have made an effort to propose a seamless authentication framework with privacy-preserving (SAF-PP) protocol in the hopes of resolving the concerns about security and confidentiality that have been raised in relation to intelligent eHealth systems. We did this in the hopes that we would be able to find a solution to these problems. We have done this in the hopes that it would enable us to better safeguard the information that is communicated over these systems. This is the motivation behind why we have done this. They presented an extensive body of research that demonstrated that the SAF-PP is able to preserve critical security features while simultaneously enhancing the system's overall efficiency. This was shown by the fact that it is able to keep the system more efficient overall. This was accomplished while also increasing the overall effectiveness of the system. The results of the performance analysis indicate that the SAF-PP that was suggested is superior in terms of delivering packets to users and extending the lifespan of the network.

This article [58], We have presented a seamless authentication framework with privacy-preserving (SAF-PP) protocol in order to overcome the difficulties regarding privacy and security that have been brought to light in relation to smart eHealth systems. These issues have been brought to light because of the fact that smart eHealth systems have been brought into the spotlight. We came to the conclusion that we needed to take this action in order to fulfil our goal of improving the data's level of security while it was being sent through these networks. They presented a substantial amount of evidence indicating that they believe the SAF-PP is able to maintain important security features while while increasing the system's overall efficacy. During this time, the efficiency

of the system as a whole was improved, which led to better results overall. According to the findings of the performance analysis, the implementation of the recommended SAF-PP would improve the delivery of packets to end users and would also lengthen the lifespan of the network.

Table 2. Analysis of the selected studies.

Source Tittle/ Authors	Year	Proposed (Algorithm / Scheme / Protocol)	Work	IoT Security Challenges	IoT Architecture			
					Sensing	Network	Middleware	Application
Efficient Implementation of the SHA-512 Hash Function for 8-bit AVR Microcontrollers / Cheng et al.	2018	unique compression function optimization strategy based on the duplication of the eight working variables	obtain great speed without unrolling the compression function's main loop, resulting in a minimal code size	Optimization				●
Hash-Based Conditional Privacy Preserving Authentication and Key Exchange Protocol Suitable for Industrial IoT / Paliwal et al.	2019	In an IIOT environment, a lightweight authentication and key at technique for greemenWSNs is needed.	The proposed work's security is demonstrated through the use of the Real-or-Random oracle model, AVISPA, BAN logic, and informal security analysis. solves flaws in previous systems and introduces a new method for exchanging session keys more quickly.	Authentication, Privacy		●		●
A Survey on Lightweight Authenticated Encryption and Challenges for Securing Industrial IoT / Agrawal et al.	2019	9 of the 17 lightweight authenticated methods were submitted to the ongoing CAESAR competition. ACORN, ASCON, JAMBU, and Ketje are among the 9 AE projects.	Because the resources on these IoT devices are limited, traditional AE techniques cannot be used. They need safe and efficient AE methods that can deal with a variety of resource restrictions.	Authenticated, Resource Constraint				●
Lightweight Cryptography: an IoT Perspective / Gupta et al.	2019	the DLFSR-based random number generator and the SPONGE-based hash creation	On bigger bit digests, SPONGE provides superior preimage resistance, whereas DLFSR and a set of LFSR provide a high degree of unpredictability.	Authentication	●			
An Effective Multifactor Authentication Mechanism Based on Combiners of Hash Function over IoT / Ahmed et al.	2019	CMA, TEOTP hash function, TOTP	In terms of authentication failure rate, CMA surpasses TOTP and protects the integrity, validity, and availability of sensed data for legitimate IoT devices.	Authentication, Integrity,				●

Adaptive and Extensible Energy Supply Mechanism for UAVs-aided Wireless Powered IoT / Wu et al.	2019	heuristic algorithm Memetic Algorithm	When IoT devices need to be fully charged, the results showed that the degree constraint is no longer com pulsive. The adaptivity and extensibility of the suggested energy supply method are satisfactory.	Authentication, Performance		●		
Lightweight multi-factor mutual authentication protocol for IoT devices / Melki et al.	2019	For IoT systems, an unique and lightweight mutual multi-factor authentication technique is presented.	Because it has low communication and processing costs, it outperforms previous systems and is secure and robust against various authentication attacks.	Authentication				●
Token-Based Lightweight Authentication to Secure IoT Networks / Dammak et al.	2019	Protocol TBLUA	It has a higher security level and more security features, such as anonymity, Perfect Forward Secrecy, and resistance to well-known attacks.	Authentication		●		
Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications / Gunathilake et al.	2019	covered the necessity of LWC	Overall, the analysis points to promising potential in terms of successful LWC implementation and performance in 5GN smart cities.	Authentication, Integrity, Privacy				●
Optimized Blockchain Model for IoT based Healthcare Applications / Dwivedi et al.	2019	blockchain-based IoT model	Most privacy and security issues are handled while taking into account the resource limits of numerous IoT devices.	Authentication , Privacy				●
Secure and Lightweight Mutual Multi-Factor Authentication for IoT Communication Systems / Noura et al.	2019	novel mutual multi-factor authentication scheme for IoT devices based on configurable PUFs	utilizes the unique features of an IoT device and the communication layers to create a (fingerprint) profile for each IoT device, which is subsequently monitored in both forward and backward directions to decrease the risk of unauthorized authentication.	Authentication, Integrity, rivacy,		●		
SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT / Aghili et al.	2019	authentication protocol called SecLAP	robust against the attacks in LRMI	Authentication, Safety			●	

Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme / Sharif et al.	2019	Three-factor authentication and key agreement protocol for IoT based WSN	Secure against active and passive threats, and suitable for IoT-based WSN scenarios.	Authentication		•		
A Survey of Lightweight Cryptographic Algorithms for IoT-Based Applications / Shah et al.	2019	decide the algorithm appropriate for chose applications in paper	Because the majority of algorithms are hardware dependent, they will perform well. While few algorithms are software-dependent, this does not rule out the possibility of them performing well on hardware. There are no guaranteed outcomes for any algorithm in terms of speed, cycles, or throughput. For RFID and IoT applications, only a few algorithms are capable and secure.	Authentication, Proficiency, Optimization				•
A Survey of Edge Computing Based Designs for IoT Security / Sha et al.	2019	provides a systematic and in-depth examination of existing edge-based IoT solutions.	These solutions address the most critical aspects of IoT security, such as complete security architecture, firewalls, intrusion detection systems, authentication and authorization procedures, and privacy-preserving de signs.	Authentication, Privacy		•		
On the Role of Hash-based Signatures in Quantum-Safe IoT: Current Solutions and Future Directions / Suhail et al.	2020	HBS schemes	Investigate the best HBS for IoT networks in terms of performance - constrained requirements, resource constraints, and design optimization goals.	Authentication, Privacy				•
MAKE-IT—A Lightweight Mutual Authentication and Key Exchange Protocol for Industrial IoT / Choudhary et al.	2020	lightweight remote user mutual authentication and key exchange model for IIoT.	The suggested approach can withstand a variety of common attacks and provides numerous security aspects such as data confidentiality, identity anonymity, integrity, and so on.	Authentication, Confidentiality,		•		
A Lightweight ECC-Based Authentication Scheme for IoT / Hammi et al.	2020	ECC and isogeny are used in a unique approach to OTP generation.	As opposed to asynchronous OTP-type techniques, this novel scheme does not require challenge/response handling.	Efficiency				•

P-HIP: A Lightweight and Privacy-Aware Host Identity Protocol for IoT / Hossain et al.	2020	P-HIP is a privacy-preserving and lightweight authentication mechanism.	To make the HIP suitable, P-HIP used ECQV cryptography to reduce computation overheads for mutual authentication. The computation-intensive cryptographic processes, such as s, signature validation, and asymmetric encryption and decryption, were removed from P-HIP. P-HIP also did away with the need to exchange certifications.	Privacy, Authentication,				●
A Physically Secure, Lightweight Three-Factor and Anonymous User Authentication Protocol for IoT / LIU et al.	2020	a new lightweight three-factor anonymous user authentication protocol based on PUF has been developed.	The suggested protocol is resistant to a number of well-known assaults, including physical capture/tempering and tracking attacks.	Authentication, Efficient		●		●
Lightweight Cryptography: A Solution to Secure IoT / Dhanda et al.	2020	develop lightweight security schemes for IoT.	The most commonly used lightweight cryptographic primitives are AES and ECC.	Efficiency				●
FPGA-Based Lightweight Hardware Architecture of the PHOTON Hash Function for IoT Edge Devices / AL-SHATARI et al.	2020	PHOTON hash function area-performance trade-offs	It's a round-based design, which means that all permutation operations are completed in a single round.	Authenticating	●			●
EC-ElGamal and Genetic Algorithm-Based Enhancement for Lightweight Scalable Blockchain in IoT Domain / GURUPRAKASH et al.	2020	EC-ElGamal	For SHA-384, the usage of EC-ElGamal and a Genetic algorithm-based key improves security and performance.	Privacy, Localization				●
A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography / Sadhukhan et al.	2020	For IoT networks, a three-factor ECC-based lightweight remote user authentication technique is used.	In comparison to past analogous designs, the scheme is quite light. Additionally, the symmetric key and password update phases are supported. As a result, the scheme is acceptable for practical application due to the security performance trade-off and other added functions.	Efficiency		●		

Sponge based Lightweight Cryptographic Hash Functions for IoT Applications / Gupta et al.	2021	comparative analysis of the findings of KECCAK, HASH-ONE, QUARK, PHOTON, SPONGENT and GLUON.	Each hash design has its own accomplishments.	Authentication				•
Security Analysis of LNMNT-LightWeight Crypto Hash Function for IoT / NABEEL et al.	2021	hash function based on the NMNT	The suggested hash functi on generates a variable length transform (powers of two). The New LWT Hash Function desi gn is ideal for a wide rang e of IoT applications due t o these qualities.	Authentication				•
LightBC: A Lightweight Hash-Based Blockchain for the Secured IoT / Pohrmen et al.	2021	A SPONGENT-based lightweight Blockchain was proposed.	The adoption of SPONGENT greatly reduces the block production delay in the Blockchain. As a result, when Blockchain technology is applied for IoT, it has the ability to solve a variety of problems.	Authentication				•
A performance comparison of lightweight cryptographic algorithms suitable for IoT transmissions / Jebrane et al.	2021	In terms of memory, energy usage, and compute complexities, examines the most promising lightweight cryptography solutions for resource-constrained devices.	compared and summarized Various lightweight algorithms are implemented on a variety of hardware and software platforms.	Computation, Complexities.		•		•
HashXor: A lightweight scheme for identity privacy of IoT devices in 5G mobile network / Choudhury et al.	2021	scheme ‘HashXor’ that uses only lightweight ‘Hash’ and ‘Xor’ operation	The technique is substantially quicker than ECIES in terms of computation cost and execution performance. It's also quick when compared to other popular 5G mobile network lightweight techniques. Through security and formal examination, the scheme is determined to be safe and logically valid (using AVISPA tool).	Identity, Privacy		•		

A Lightweight PUF-Based Authentication Protocol Using Secret Pattern Recognition for Constrained IoT Devices / IDRISS et al.	2021	LPA protocol based on secret pattern recognition	Even after the device's secret patterns are exposed, the suggested protocol has a high level of resistance to modeling assaults. Mutual authentication and authenticated secret message exchange are among the security measures available.	Authentication				●
LightIoT: Lightweight and secure communication for energy-efficient IoT in health informatics / Jan et al.	2021	LightIoT	It is extremely resistant to a variety of attack scenarios and has low computational and communication overheads. The validation of mobile wearable devices in an operating setting is a constraint of LightIoT.	Authentication		●		
Hashing based Data Transaction and Optimized Storage for IoT Applications / Parmar et al.	2021	Through this observational analysis, integrated blockchain provides security and privacy benefits.	It uses a common concept to create a centralized ledger at the IoT network level to optimize storage issues and to improve security by employing protected hashing.	Interoperability, Privacy				●
Hash Constructions for CoAP under an IoT Environment / Kumar et al.	2021	A new hashing design based on a sponge structure.	Blake, JH, Keccak, and SHA were the four hash constructions studied by the authors.	Authentication				●
Definition of a lightweight cryptographic solution to secure health data on IoT and cloud / Chhaybi et al.	2021	A recent assessment of IoT and cloud-based healthcare monitoring solutions was conducted.	To ensure integrity and authentication, the use of lightweight cryptography, particularly a lightweight hash function specified by the NIST, was recommended. In the same vein, the AES-128 algorithm is both quick and secure.	Authentication, Integrity		●	●	
Hash-MAC-DSDV: Mutual Authentication for Intelligent IoT-Based Cyber-Physical SystemsAdil M, Jan M, / Farouk A	2022	a lightweight hash media access control destination sequence distance vector (Hash-MAC-DSDV)	ensures D2D authentication by the Hash-MAC-DSDV mutual scheme, where the MAC addresses of individual devices are registered in the first phase and advertised in the network in the second phase.	Authentication, optimization		●		●

User Authentication and Authorization Framework in IoT Protocols User A, Janicke H	2022	an enhanced IoT security framework for authentication and authorization is proposed and implemented	protect the IoT protocols from different types of attacks such as man-in-the-middle attacks, reply attacks, and brute force attacks	Authentication, Efficiency,		•		
Seamless privacy-preservation and authentication framework for IoT-enabled smart eHealth systemsDeebak B, Memon F	2022	resents a seamless authentication framework with privacy-preserving (SAF-PP) protocol to deal with security and privacy issues of smart eHealth intelligence.	proves that the proposed SAF-PP can adhere to significant security properties while improving the system efficiency rate.	Efficiency, Availability		•		
Security-Level Improvement of IoT-Based Systems Using Biometric FeaturesMoradi M, Moradkhani M, Tavakoli M	2022	Improve the level of biometric security compared with traditional password-based methods will be proven in section three using the Markov model	the suggested mechanism enhances the system security by 120.38% on average, which is 106.23, 110.45, and 144.46% of relative improvement compared with IoT sensors, controller layer mechanisms, and application layer mechanisms, respectively.	Authentication, Efficiency	•		•	•

8. Statistical Analysis and Conclusion

During the process of gathering the data, the target papers were papers that were published between 2018-2021. For the analysis of the data, we choose some set of information and key to analyzing the data based on which are the following (publication year, IoT security Challenges, IoT architecture).

Fig. 4 shows the analysis of which IoT Layer has the highest rate of research and papers made, as expected during the fast growth of IoT devices and appearing different companies that provide IoT technologies, researchers are focusing on the application layer, which has the highest research on, this increasing of the IoT devices means increasing usage of the network, so second highest is a network layer because we need optimization for the networks as shown in 2022 the network layer has the main focus from the reviewers and researchers, lastly both middleware and sensor layer which is increasing year by year.

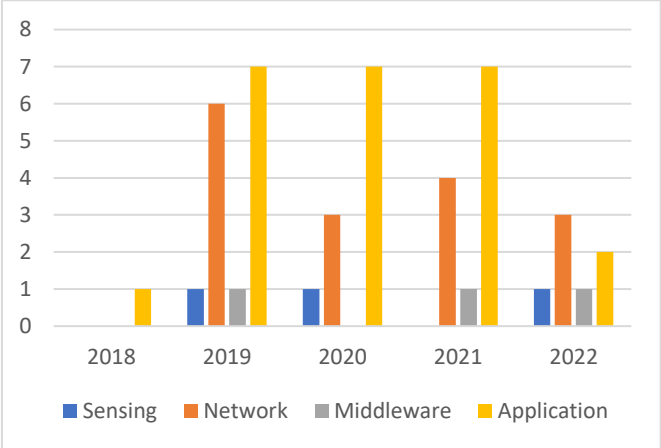


Fig. 4. Bar chart showing the number of papers for each year and each IoT Layer

Fig. 5 shows the analysis of extracting information about which year have the highest research rate. Suddenly the highest rate was in 2019, 41%, and the second was in 2021, 29%. Then in the third, 2020, which is 26%, in the third one 2022 which mostly focused on the network layer, and its percentage was 11%, and the last one is 2018, which is 3%.

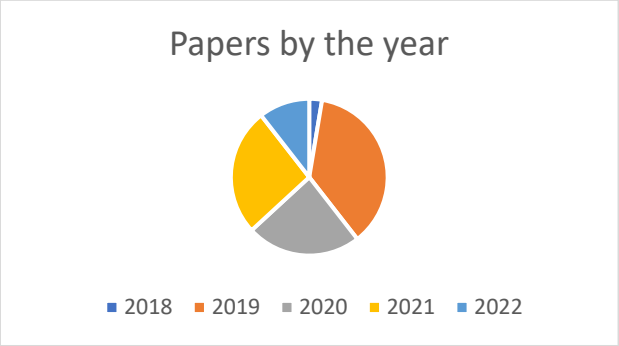


Fig. 5. Pie chart shows the number of studies for each year

Fig. 6 shows The analysis to detect the highest rate of IoT security challenges and its Layer. As expected papers we have filtered, the highest IoT security challenge is authentication and privacy. The highest IoT security challenge is the authentication layer, the application layer. Privacy is also in the application layer; the second highest Layer is the network layer authentication at the top of it, and the second is privacy. The unexpected was that the sensing had a minimum rate among the other layers

Fig. 6. Bar chart shows the number of papers according to various criteria

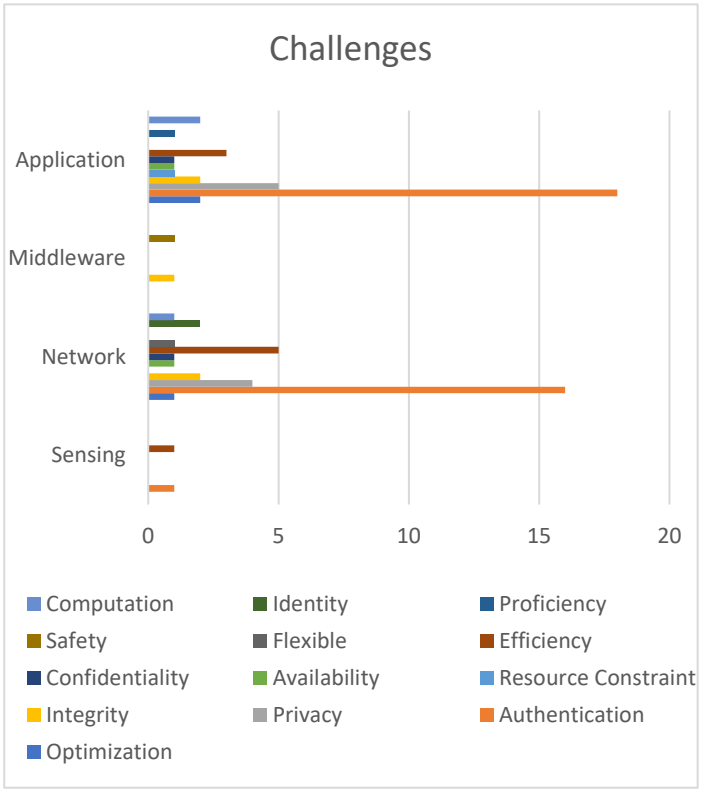


Fig. 7 shows that after checking each IoT security challenge, we have started to detect the IoT security challenges according to our selected years. the result was that in 2019 the highest IoT security challenge is authentication which has the highest rate among other years and the second one is privacy. Hopefully, the analyzed data is highly relative to our title, which security

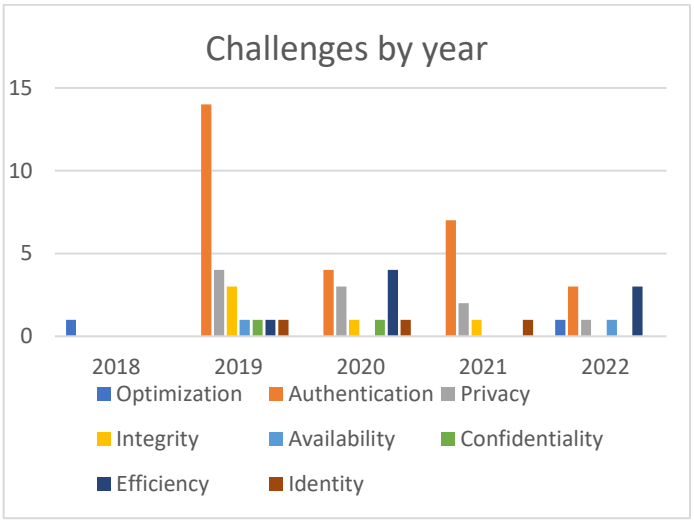
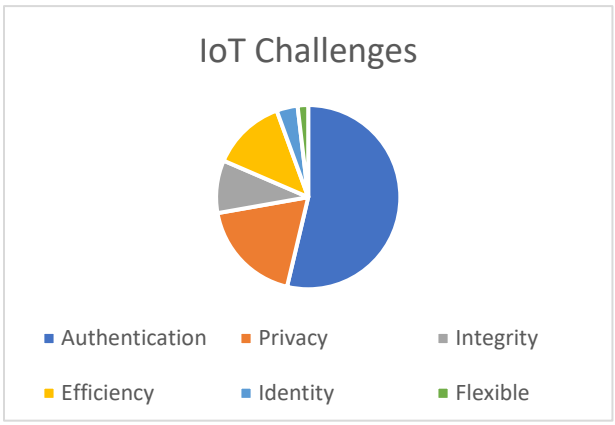


Fig. 7. Bar chart of the number of papers according to challenges and years

Fig. 8 shows an analysis to detect the highest IoT security challenge among all other challenges: authentication in the first place and efficiency in the second. Authentication is the most concerning topic in IoT technology. Many research papers are focus on the authentication and efficiency, privacy of the data that are exchanged on the networks.

Fig. 8. Pie chart of number of studies according to IoT challenges.



References

[1] Kairaldeen, A. R.; Abdullah, N. F.; Abu-Samah, A.; Nordin, R., Data integrity time optimization of a blockchain IoT smart home network using different consensus and hash algorithms. *Wireless Communications and Mobile Computing* **2021,** *2021*, 1-23.

[2] Jebranea, J.; Lazaara, S., A performance comparison of lightweight cryptographic algorithms suitable for IoT transmissions. *Gen. Lett. Math* **2021,** *10* (2), 46-53.

[3] Dhanda, S. S.; Singh, B.; Jindal, P., Lightweight cryptography: a solution to secure IoT. *Wireless Personal Communications* **2020,** *112*, 1947-1980.

[4] Hussien, N.; Ajlan, I.; Firdhous, M. M.; Alrikabi, H., Smart shopping system with RFID technology based on internet of things. **2020**.

[5] Diwan, S. A., Dynamic Lightweight Mechanism for Security and Performance in Internet of Things. *International Journal of Interactive Mobile Technologies* **2022,** *16* (10).

[6] Ma, J.; Sang, Y.; Zhang, Y.; Xu, X.; Feng, B.; Zeng, Y. In *An Adaptive Ensembled Neural Network-Based Approach to IoT Device Identification*, Collaborative Computing: Networking, Applications and Worksharing: 18th EAI International Conference, CollaborateCom 2022, Hangzhou, China, October 15-16, 2022, Proceedings, Part II, Springer: 2023; pp 214-230.

[7] Shantha, R. M. J.; Mahender, K.; Jenifer, A. J. M.; Prasanth, A. In *Security analysis of hybrid one time password generation algorithm for IoT data*, AIP Conference Proceedings, AIP Publishing LLC: 2022; p 030021.

[8] Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M., On blockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems* **2018,** *88*, 173-190.

[9] Alfrhan, A.; Moulahi, T.; Alabdulatif, A., Comparative study on hash functions for lightweight blockchain in Internet of Things (IoT). *Blockchain: Research and Applications* **2021,** *2* (4), 100036.

[10] Denysiuka, D.; , T. S.; and Mariia Kapustiana, Proof of Stake And Proof of Work Approach for Malware Detection Technologies. *CEUR Workshop Proceedings* **2022,** *3156*.

[11] Schiller, E.; Aidoo, A.; Fuhrer, J.; Stahl, J.; Ziörjen, M.; Stiller, B., Landscape of IoT security. *Computer Science Review* **2022,** *44*, 100467.

[12] Alphonse, A. S.; Priya, E. D.; Kowsigan, M., Review of Machine Learning Techniques Used for Intrusion and Malware Detection in WSNs and IoT Devices. *Design and Development of Efficient Energy Systems* **2022**, 57-65.

[13] Haji, S. H.; Ameen, S. Y., Attack and anomaly detection in iot networks using machine learning techniques: A review. *Asian journal of research in computer science* **2021,** *9* (2), 30-46.

[14] Aggarwal, V. K.; Sharma, N.; Kaushik, I.; Bhushan, B. In *Integration of Blockchain and IoT (B-IoT): Architecture, Solutions, & Future Research Direction*, IOP Conference Series: Materials Science and Engineering, IOP Publishing: 2021; p 012103.

[15] Alshahrani, H. M., Coll-iot: A collaborative intruder detection system for internet of things devices. *Electronics* **2021,** *10* (7), 848.

[16] Sikder, A. K.; Petracca, G.; Aksu, H.; Jaeger, T.; Uluagac, A. S., A survey on sensor-based threats and attacks to smart devices and applications. *IEEE Communications Surveys & Tutorials* **2021,** *23* (2), 1125-1159.

[17] Alhammadi, N. A. M.; Zaboon, K. H., A Review of IoT Applications, Attacks and Its Recent Defense Methods. *Journal of Global Scientific Research* **2022,** *7* (3), 2128-2134.

[18] Janani, K.; Ramamoorthy, S. In *Iot security and privacy using deep learning model: a review*, 2021 International conference on intelligent technologies (CONIT), IEEE: 2021; pp 1-6.

[19] Lata, N.; Kumar, R., Security in Internet of Things (IoT): Challenges and Models. *Mathematical Statistician and Engineering Applications* **2022,** *71* (2), 75–81-75–81.

[20] Leloglu, E., A review of security concerns in Internet of Things. *Journal of Computer and Communications* **2016,** *5* (1), 121-136.

[21] Driss, M.; Hasan, D.; Boulila, W.; Ahmad, J., Microservices in IoT security: current solutions, research challenges, and future directions. *Procedia Computer Science* **2021,** *192*, 2385-2395.

[22] Anuradha, M.; Jayasankar, T.; Prakash, N.; Sikkandar, M. Y.; Hemalakshmi, G.; Bharatiraja, C.; Britto, A. S. F., IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. *Microprocessors and Microsystems* **2021,** *80*, 103301.

[23] Cheng, H.; Dinu, D.; Großschädl, J. In *Efficient implementation of the SHA-512 hash function for 8-bit AVR microcontrollers*, Innovative Security Solutions for Information Technology and Communications: 11th International Conference, SecITC 2018, Bucharest, Romania, November 8–9, 2018, Revised Selected Papers 11, Springer: 2019; pp 273-287.

[24] Dammak, M.; Boudia, O. R. M.; Messous, M. A.; Senouci, S. M.; Gransart, C. In *Token-based lightweight authentication to secure IoT networks*, 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE: 2019; pp 1-4.

[25] Agrawal, M.; Zhou, J.; Chang, D., A survey on lightweight authenticated encryption and challenges for securing industrial IoT. *Security and Privacy Trends in the Industrial Internet of Things* **2019**, 71-94.

[26] Aghili, S. F.; Mala, H.; Kaliyar, P.; Conti, M., SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT. *Future Generation Computer Systems* **2019,** *101*, 621-634.

[27] Ahmed, A. A.; Ahmed, W. A., An effective multifactor authentication mechanism based on combiners of hash function over internet of things. *Sensors* **2019,** *19* (17), 3663.

[28] Dwivedi, A. D.; Malina, L.; Dzurenda, P.; Srivastava, G. In *Optimized blockchain model for internet of things based healthcare applications*, 2019 42nd international conference on telecommunications and signal processing (TSP), IEEE: 2019; pp 135-139.

[29] Ostad-Sharif, A.; Arshad, H.; Nikooghadam, M.; Abbasinezhad-Mood, D., Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme. *Future Generation Computer Systems* **2019,** *100*, 882-892.

[30] Noura, H. N.; Melki, R.; Chehab, A. In *Secure and lightweight mutual multi-factor authentication for IoT communication systems*, 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), IEEE: 2019; pp 1-7.

[31] Gupta, D. N.; Kumar, R., Lightweight cryptography: an IoT perspective. *Trivium* **2019,** *80* (1), 2580.

[32] Gunathilake, N. A.; Buchanan, W. J.; Asif, R. In *Next generation lightweight cryptography for smart IoT devices:: implementation, challenges and applications*, 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), IEEE: 2019; pp 707-710.

[33] Paliwal, S., Hash-based conditional privacy preserving authentication and key exchange protocol suitable for industrial internet of things. *IEEE Access* **2019,** *7*, 136073-136093.

[34] Shah, A.; Engineer, M. In *A survey of lightweight cryptographic algorithms for iot-based applications*, Smart Innovations in Communication and Computational Sciences: Proceedings of ICSICCS-2018, Springer: 2019; pp 283-293.

[35] Liu, Z.; Guo, C.; Wang, B., A physically secure, lightweight three-factor and anonymous user authentication protocol for IoT. *IEEE Access* **2020,** *8*, 195914-195928.

[36] Melki, R.; Noura, H. N.; Chehab, A., Lightweight multi-factor mutual authentication protocol for IoT devices. *International Journal of Information Security* **2020,** *19*, 679-694.

[37] Wu, P.; Xiao, F.; Huang, H.; Sha, C.; Yu, S., Adaptive and extensible energy supply mechanism for UAVs-aided wireless-powered Internet of Things. *IEEE Internet of Things Journal* **2020,** *7* (9), 9201-9213.

[38] Hossain, M.; Hasan, R., P-hip: A lightweight and privacy-aware host identity protocol for internet of things. *IEEE Internet of Things Journal* **2020,** *8* (1), 555-571.

[39] Choudhary, K.; Gaba, G. S.; Butun, I.; Kumar, P., Make-it—A lightweight mutual authentication and key exchange protocol for industrial internet of things. *Sensors* **2020,** *20* (18), 5166.

[40] Sha, K.; Yang, T. A.; Wei, W.; Davari, S., A survey of edge computing-based designs for IoT security. *Digital Communications and Networks* **2020,** *6* (2), 195-202.

[41] Suhail, S.; Hussain, R.; Khan, A.; Hong, C. S., On the role of hash-based signatures in quantum-safe internet of things: Current solutions and future directions. *IEEE Internet of Things Journal* **2020,** *8* (1), 1-17.

[42] Hammi, B.; Fayad, A.; Khatoun, R.; Zeadally, S.; Begriche, Y., A lightweight ECC-based authentication scheme for Internet of Things (IoT). *IEEE Systems Journal* **2020,** *14* (3), 3440-3450.

[43] Al-Shatari, M. O. A.; Hussin, F. A.; Abd Aziz, A.; Witjaksono, G.; Tran, X.-T., FPGA-based lightweight hardware architecture of the PHOTON hash function for IoT edge devices. *IEEE Access* **2020,** *8*, 207610-207618.

[44] Guruprakash, J.; Koppu, S., EC-ElGamal and Genetic algorithm-based enhancement for lightweight scalable blockchain in IoT domain. *IEEE Access* **2020,** *8*, 141269-141281.

[45] Nabeel, N.; Habaebi, M. H.; Islam, M. R., Security analysis of LNMNT-lightweight crypto hash function for IoT. *IEEE Access* **2021,** *9*, 165754-165765.

[46] Gupta, D. N.; Kumar, R. In *Sponge based lightweight cryptographic hash functions for IoT applications*, 2021 International Conference on Intelligent Technologies (CONIT), IEEE: 2021; pp 1-5.

[47] Pohrmen, F. H.; Saha, G. In *Lightbc: A lightweight hash-based blockchain for the secured internet of*

things, International Conference on Innovative Computing and Communications: Proceedings of ICICC 2020, Volume 1, Springer: 2021; pp 811-819.

[48] Parmar, M., Hashing based Data Transaction and Optimized Storage for IoT Applications. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* **2021,** *12* (5), 1206-1215.

[49] Idriss, T. A.; Idriss, H. A.; Bayoumi, M. A., A lightweight PUF-based authentication protocol using secret pattern recognition for constrained IoT devices. *IEEE Access* **2021,** *9*, 80546-80558.

[50] Jan, M. A.; Khan, F.; Mastorakis, S.; Adil, M.; Akbar, A.; Stergiou, N., LightIoT: Lightweight and secure communication for energy-efficient IoT in health informatics. *IEEE transactions on green communications and networking* **2021,** *5* (3), 1202-1211.

[51] Choudhury, H., HashXor: A lightweight scheme for identity privacy of IoT devices in 5G mobile network. *Computer Networks* **2021,** *186*, 107753.

[52] Chhaybi, A.; Lazaar, S., Definition of a lightweight cryptographic solution to secure health data on IoT and cloud. *Gen. Lett. Math* **2021,** *10* (2), 54-60.

[53] Kumar, A.; Gupta, D. N.; Kumar, R. In *Hash Constructions for CoAP under an IoT Environment*, 2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), IEEE: 2021; pp 1-7.

[54] Sadhukhan, D.; Ray, S.; Biswas, G.; Khan, M. K.; Dasgupta, M., A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography. *The Journal of Supercomputing* **2021,** *77*, 1114-1151.

[55] Adil, M.; Jan, M. A.; Mastorakis, S.; Song, H.; Jadoon, M. M.; Abbas, S.; Farouk, A., Hash-MAC-DSDV: Mutual Authentication for Intelligent IoT-Based Cyber–Physical Systems. *IEEE Internet of Things Journal* **2021,** *9* (22), 22173-22183.

[56] Mohammad, A.; Al-Refai, H.; Alawneh, A. A., User Authentication and Authorization Framework in IoT Protocols. *Computers* **2022,** *11* (10), 147.

[57] Deebak, B.; Memon, F. H.; Cheng, X.; Dev, K.; Hu, J.; Khowaja, S. A.; Qureshi, N. M. F.; Choi, K. H., Seamless privacy-preservation and authentication framework for IoT-enabled smart eHealth systems. *Sustainable Cities and Society* **2022,** *80*, 103661.

[58] Moradi, M.; Moradkhani, M.; Tavakoli, M. B., Security-level improvement of IoT-based systems using biometric features. *Wireless Communications and Mobile Computing* **2022,** *2022*, 1-15.