Wireless Networks (2024) 30:2987–3026
https://doi.org/10.1007/s11276-024-03714-4

ORIGINAL PAPER

Recent Lightweight cryptography (LWC) based security advances for resource-constrained IoT networks

Shraiyash Pandey[1] · **Bharat Bhushan**[1]

Published online: 25 March 2024

Abstract
In today's world, the Internet of Things (IoT) plays a major role to interconnect all the devices and improve the overall Quality of Life (QoL) for people. The main concern among IoT systems revolve around three pillars namely security, confidentiality, and privacy owing to the sensitive nature of the data being transmitted and processed byIoT devices. Traditional cryptographic approaches address these concerns by ensuring the authenticity and confidentiality of IoT systems. However, the majority of IoT devices are resource-constrained, which implies that they operate under significant resource constraints such as limited computational power, constrained battery life, physical compactness, and restricted memory capacity. To this end, Lightweight cryptography (LWC) offers methods specifically designed to accommodate the limitations of resource-constrained IoT devices. This work establishes the role of light weight cryptography for such resource constrained IoT networks in terms of security perspectives. In this work, we explore the security vulnerabilities of IoT systems and the associated lightweight cryptographic methods highlighting four components namely lightweight block ciphers, lightweight stream ciphers, hash functions, and Elliptic Curve Cryptography. The work further discusses the role of LWC and reviews the recent advancements in different sectors of IoT such as smart city, industries, healthcare, smart grids, and agriculture. Finally, several open research directions are highlighted in order to guide future LWC and IoT researchers.

Keywords Internet of things · Cryptography · Lightweight · Security · Networks

1 Introduction

Internet of Things (IoT) [1] is the term for ordinary objects which are managed over the Internet and are relevant, reachable, trackable, and evident via data-collecting devices. Along with mobile devices, technological advances have expanded the Internet to smart gadgets known as IoT, which are capable of detecting, actuating, computing, storing, and communicating. IoT can be viewed as a pervasive collection of uniquely identified real or virtual entities that transmit large amount of information to be employed for smart decision-making. RFID, wireless, wired, and other forms of connectivity are used to connect IoT devices [2, 3]. The primary goal of IoT is for all physical objects to function as computers linked to the Internet, and to advance the way of life by placing as many smart gadgets as possible around people to execute everyday tasks and duties [4, 5]. Various security challenges have been explored over the years, including perceptions of security to gather data, transmission of data which needs to be trusted and safe, and its implementation security. Given all this, it is impossible to deny that the widespread usage of IoT systems need powerful protection from all conceivable attacks of vulnerability, and hence security is necessary at every possible layer that exposes the IoT system.

Providing security, confidentiality, and privacy in IoT devices present a number of issues for a number of reasons. Firstly, constructing as few devices which are feasible enough to make sure that the security algorithm is cost effective [6–10]. Secondly, the basic sensors are linked together to establish a vast virtual network [11, 12]. Thirdly, because the majority of IoT devices are battery-operated, the security methods' power consumption must be minimal [13, 14]. Finally, the central processing unit (CPU) in IoT devices is

✉ Bharat Bhushan
bharat_bhushan1989@yahoo.com

Shraiyash Pandey
shraiyash.pandey@gmail.com

[1] Department of Computer Science and Engineering, School of Engineering and Technology, Block II, Sharda University, Greater Noida, Uttar Pradesh 201310, India

limited and incapable of running complicated algorithms [15, 16]. To address the challenges of security, confidentiality, and privacy in IoT-based systems, cryptographic approaches are required. Security procedures that make good use of cryptographic technologies while adhering to resource constraints are more suitable [17, 18]. As a result, compared to traditional cryptographic approaches, Lightweight Cryptography (LWC)algorithms are better suited to provide solutions to the issues presented in IoT devices.

LWC is an approach that is being explored and researched to address the challenges and specifications of devices withthe limited computational power and resources [19]. LWC offers methods that are capable of being used in various IoT applications. Their hardware architectures are often used for IoT devices and are appropriate for a variety of applications which concentrate on either minimal-area or high-throughput performance [20]. There have been recent advancements in the improvement of cipher's security, new ciphers resilient to fault attacks, improved performance in ciphers, optimization in ciphers, new ciphers strictly for resource-constrained IoT devices, enhancement in Quantum Noise Stream Ciphers, and extended version of previous ciphers. Due to the reduction in computational complexity, one disadvantage of hardware implementation of lightweight algorithms is the reduction in security when compared to traditional heavier cryptographic methods. This is a hardware restriction in the IoT setting, since the absence of high-level security is entangled with the effectiveness and architectural qualities of the implemented resource-constrained IoT devices [21]. Nonetheless, in spite of the hardware restrictions, such lightweight solutions remain capable of offering adequate safety and meets, to some extent, the specifications for a reliable IoT system.

Despite the evolution of IoT over the previous year, there is still lack of comprehensive studies that focus on security mechanisms and methods to address the security concerns of IoT systems. To the best of our knowledge, this paper is one of the first works that thoroughly covers the different lightweight cryptographic methods to protect the private data in IoT and offer protection from various cyberattacks that take place in the IoT system. The major contribution of this work is a presentation of four different appropriate lightweight cryptographic methods: lightweight block cipher [22], lightweight stream cipher [23], hash functions [24], and Elliptic Curve Cryptography (ECC) [25]; which have all been discussed and various implementations of the methods have been explored in detail to resolve the concerns related to security, confidentiality, and privacy of the IoT systems. A summary of the major contribution of this work is mentioned below.

- This work provides a detailed 4-layerd architecture of IoT that includes the Application layer, Middleware layer, Network layer, and Perception layer. It demonstrates the functionality of each layer, and working of the entire IoT system.
- This work explores the various cyberattacks that occur in different layers of IoT, and enumerate the objective of each attack along with the severity of the attack as well.
- This work presents lightweight block cipher, lightweight stream cipher, hash functions, and ECC as the four lightweight cryptographic methods to protect the data in the IoT systems; and it explores the different implementations of each method, along with a comparison between them.
- This work classifies the lightweight cryptographic ciphers based on three parameters with an IoT related practical implication along with providing specific use cases and advantages of ECC
- This work highlights the significance of LWC in IoT through the representation of diverse applications of LWC in different sectors of IoT such as Smart Cities, Healthcare, IIoT (Industrial Internet of Things), Agriculture, Smart Home Automation, and Smart Energy Grids.
- This work emphasizes the addition of several recent advancements in the academia related to LWC in the diverse sectors of IoT
- This work throws light on the major recent advancements in LWC with respect to improvements in different areas such as security, performance, optimization, resilience to attacks, and compatibility with resource constrained devices and IoT networks and nodes.
- This work presents several future research directions in terms of specific improvements for each lightweight cryptographic method, integration of LWC in IoT systems, and the hardware implementation for LWC methods.

The remainder of the paper is organized as follows. Section 2 describes an overview of IoT which includes its background, layers involved in the architecture, its reference model, and the various attacks that occur in each layer. Section 3 presents different implementations of the four lightweight cryptographic methods along with a comparison between them. Section 4 explores the diverse applications of LWC in different sectors of IoT. Section 5 presents a list of recent advancements in LWC which highlights improvements in different functionalities of ciphers and other schemes. Section 6 mentions the future research directions to direct future LWC and IoT researchers, followed by a conclusion in Sect. 7.

2 IoT

Everyday things that are identifiable, readable, locatable, and addressable through sensors and are modifiable with the help of Internet can be referred to as IoT [26, 27]. Radio

Frequency Identification (RFID), wired, or wireless techniques can be used to easily access IoT devices. IoT devices are not only subjected to high-tech things, but also waste bins, animals, clothing, food items, water, etc. To allow for all physical things to act in a computerized way which is connected to the internet is the core purpose of IoT. Similarly, by generating smart devices to perform daily tasks and change the living style of an individual is the core purpose of IoT. IoT is a domain that adds connectivity to different concepts already in place. From the background of IoT, to its current architecture holds the essential information to evaluate the security measures and concerns of the various sectors in IoT. The IoT Reference Model incorporates the entire structure of the IoT and explains the working of it. Each layer in the IoT has a specific purpose and attackers inevitably attempt to break through the various layers to get into the IoT system and perform malicious activates. The subsections below discuss the emersion of IoT into the real world, along with its architecture that entails the working of each layer and the attacks associated with them.

2.1 Background of IoT

The computer scientist Kevin Ashton [28], originated the term 'Internet of Things' (IoT) back in 1999. However, previously in the 1980s some university students had already discussed the idea of implementing intelligence into physical objects by adding sensors while modifying a vending machine of Coca Cola [29]. Therefore, the concept of Internet of Things was introduced way before Kevin Ashton stamped out the term. To track products via a supply chain, he proposed the idea to put radio frequency identification chips on them. Eventually, as IoT based devices progressively started to come into the market, the publics' interest in IoT technology sky rocketed over the next decade. In addition, business sectors and medicine sectors inclined towards the use of IoT Technology over time. To improve customer experience, optimize supply chains, and manage inventory, businesses started to opt for enterprise IoT, which incorporated of precision agriculture, and smart factories [30]. On the other hand, medicine sectors began to implement the use of IoT connected devices such as smart inhalers, and robotic surgery to significantly improve the healthcare.

2.2 Layers of the IoT architecture

Layers of the IoT architecture can be visualized from bottom to top. At the bottom, the perception layer has the duty to collect all sorts of data from hardware equipment. Above the perception layer, to transmit the collected data from perception layer, network layer is responsible. Network layer relies on wireless network, basic networks, satellites, etc. for transmitting data between IoT devices. Through network grid and cloud computing, the computing powers will be set up in the middleware layer. At the very top and at last, to provide services which can be modified with respect to users' requirements, the application layer is responsible. Overall, four different essential layers make up the IoT architecture [31]: (i) the application layer, (ii) middleware layer, (iii) network layer, and (iv) perception layer. Furthermore, each layer of the IoT architecture is discussed below. The four layers are illustrated in Fig. 1.

2.2.1 Application layer

The IoT architecture's upper tier is the application layer. In order to handle various apps, the middleware layer sends data to this layer. The application component displays the IoT data as a grid, diagram, and operating model. Automation at the application layer can be seen in smart towns, smart homes, and smart vehicles, among other things [32]. In fact, a major building block of the IoT is smart object and IoT is referred as a collection of smart objects which are all interconnected via a network. IoT consists of both software and hardware modules. Such modules can have wired or wireless based connectivity. To sense physical movements, sensors in the smart objects capture that movements and collect it [33]. Since the data is captured and collected by the sensors, it can be shared among various devices and allow them to communicate with each other. However, to process the collected information, smart objects are not extremely rich in resource and computational abilities. Therefore, the information is sent to external platforms for computing and processing.

2.2.2 Middleware layer

The vendor-specific services for different IoT node details are operated by the middleware layer, which connects the application tier and network tier. According to the third—party vendor and node requirements, this connection makes it easier to process, pre-process, and store IoT node details [34]. Both the middleware and application tiers make use of resource-intensive hardware that can protect IoT networks with conventional cryptography. Cloud computing plays a major role in the Middleware layer. It is leverage for tasks such as data computation and storage. The benefit of integrating smart devices in IoT is directed towards the improvement in different fields such as energy, health, defense, waste management, etc. [35]. To configure computing resources, on-demand access is provided by a large-scale distributed platform which is known as cloud computing. Through default access mechanism, cloud computing offers the users to do computations on data [36]. Since cloud computing provides storage and computation for smart devices in IoT, it plays a vital role in systems of IoT. The data processed

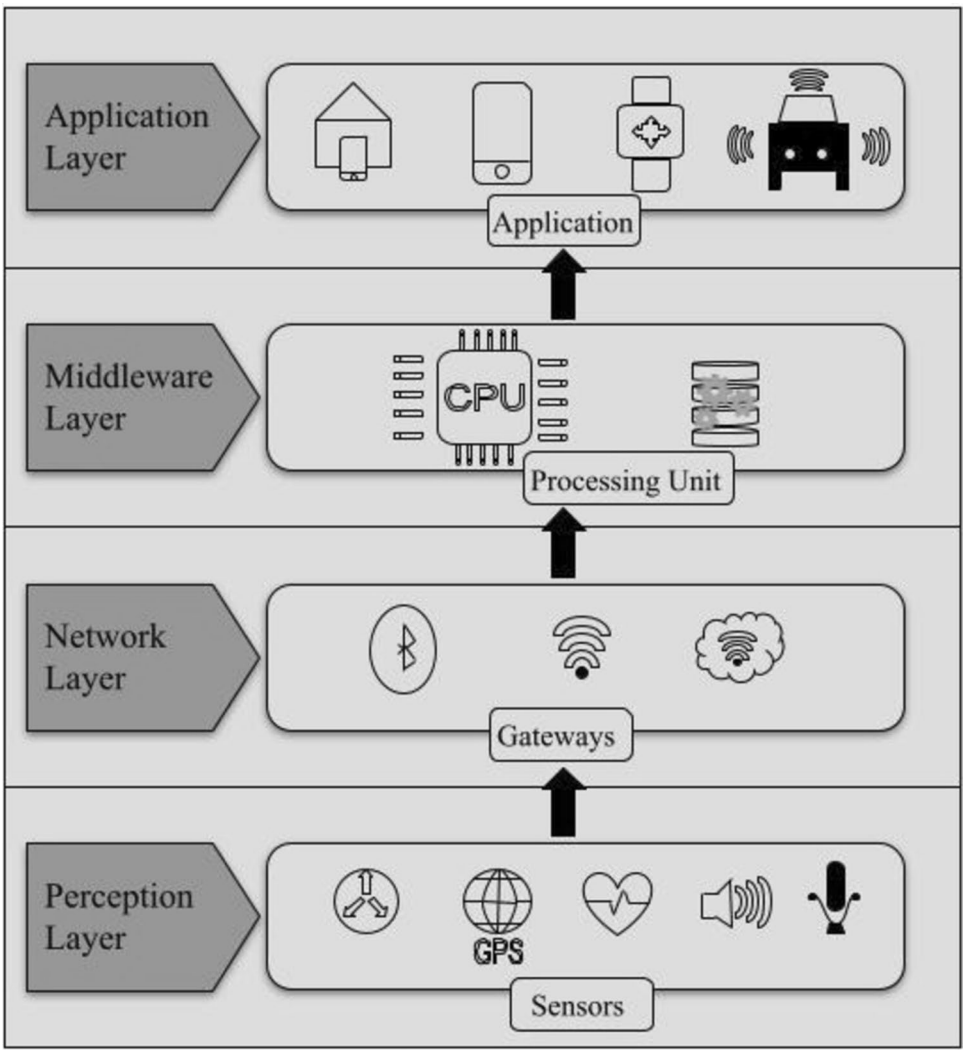

Fig. 1 Layered IoT architecture

by systems in IoT has significantly increased due to the higher number of smart devices on the network [37]. Cloud computing provides scalability since computation and storage of data are limited for smart devices. Apart from scalability, cloud computing also offers elasticity and convenience. Though, there's also a few downsides such as physical distance. For end devices to be offered cloud services, the physical distance is an issue that forms a bottleneck. Precise user location, land local network conditions are also among the few downsides of cloud computing [38].

2.2.3 Network layer

In the IoT architecture, data is processed, routed, and transmitted safely via the Network layer, also known as the Transit layer. For data transfer, this layer makes use of a variety of protocols, including Bluetooth, Infrared, Zigbee, and 6LowPan [39–41]. The network layer relies on the middleware layer for additional processing and activity. Since cloud computing is the core task in the middleware layer, following it fog computing, which takes place in the network layer. It sets cloud services and computational tools at the network's edge to reduce latency issues. Between the edge and cloud computing, fog computing itself forms a layer that includes various devices such as switches, controllers, etc. Such devices can be placed at different locations, either dynamic or stationary. To gain higher computational power, the nodes in the devices are interconnected to centers of cloud data. Server load, bandwidth of the network, and speed are factors that affect the processing of data [42, 43]. Due to low-wireless bandwidth, there are delays in smartphone devices. With computing and storage abilities, a fog computing node is an easier and suitable solution when resource-constrained devices have to be offloaded as compared to the cloud. Since the resource-constrained devices lack the storage and computation abilities, the fog computing provides such features for utilization to the devices which reduces network transmission as well as provide higher system performance.

However, edge computing in the perception layer provides higher performance statistics even after fog computing adds performance in various applications [44]. To resolve issues related to reliability, power consumption, trust and privacy, edge computing performs the computational tasks at the edge nodes which results into utilization of energy consumption.

2.2.4 Perception layer

Information collection and transmission from the actual world are both essential functions of IoT devices. As a result, the perception layer is equipped with a variety of data collection, processing, and transmission tools, including pressure and temperature monitors, Bluetooth, Zigbee, and others. Two components make up the perception layer: the perception node (sensors, actuators, etc.) and the perception network, which connects to the IoT architecture's higher layer [45]. Information is gathered and controlled by perception nodes, such as motors and sensors. However, the perception network sends the data gathered to the portal. Zigbee, GPS, RFID, and Long-Range Wide Area Network (LoRaWAN) technology are all utilized by the perception layer [46]. By providing computational and storage features at the perception layer, issues related to latency and mobility are addressed. Smart device's mobility is supported by the edge devices. Multiaccess edge computing is another term used for edge computing since it is quite similar to fog computing. Data being passed between fog nodes and smart devices is controlled by the smartphones that are the edge nodes. Between a computing platform and smartwatch, an edge device such as smartphone performs as an edge. A network is formed of multiple edges, where such edge devices can communicate with each other and be interconnected. Communication on the network can be bottlenecked through the edge network. However as compared to cloud computing, it offers lower processing power. To provide higher efficiency and faster response time, the data processing is done at the edges as compared to the cloud since data has to be sent to cloud first and then processed [47]. When data is processed close to the smart devices before it is sent to the cloud, it reduces the usage of internet bandwidth. Between the edge and fog layers, the classification of devices can be done easily in terms of computational power with the use of edge-fog cloud architecture [48].

Table 1 displays the IoT layers along with a detailed breakdown of each layer's purpose and elements.

2.3 IoT reference model

The scope for any IoT design is set by the sub-models in the IoT Reference Model. The IoT Reference Model consists of 5 sub-models that provide certain functionalities for various scenarios [49, 50]. An illustration of the IoT Reference Model in terms of its sub-models is presented in Fig. 2. Among these sub-models, the Domain Model is one of the key models and the foundation that provides a description of relevant concepts in IoT. The IoT Domain Model is compulsory for all actions of the IoT ARM, whereas other sub-models such as IoT Security, and Privacy Model, IoT Communication Model are not that important. The IoT Information Model is developed based on the IoT Domain Model. Independent of various technologies, IoT Domain model is developed in a proper way to provide great abstraction. On a conceptual level, the IoT Information Model defines the structure of information that is related to IoT of an IoT system. The IoT Information Model holds the information related to the aspects of IoT Domain Model. Functionalities found in the foundation of IoT Domain Model's key concepts are identified by the IoT Functional Model. Information model provides the information to the functional model that is appropriately handled by its functional components. Following the various connections observed in the IoT Domain model, a number of Functionality Groups (FG) are built on one another. Such groups offer a method for interacting with the instances of different aspects. In heterogeneous environments, communication becomes a difficult task, which is the case in an IoT system. Therefore, the IoT Communication model provides methods for handling the communication. To handle the security, privacy, and trust issues within the IoT system, the IoT Trust, Security & Privacy Model were introduced to provide relevant methods, its interdependencies and relationships [51].

Table 1 Element and purpose of each layer in IoT architecture

Layer	Elements	Purpose
Application layer [32, 33]	Touch panel, consoles, third-party application, websites	Flowcharts, business model, machine learning
Middleware layer [34–38]	Third-party application which is vendor-specific	Real-time action, processing, machine learning
Network layer [39–44]	Firmware, gateways, nodes	Secure and process routing, transmit and process data
Perception layer [45–48]	Sensors, and actuators	Action, monitor, identification, transfer data

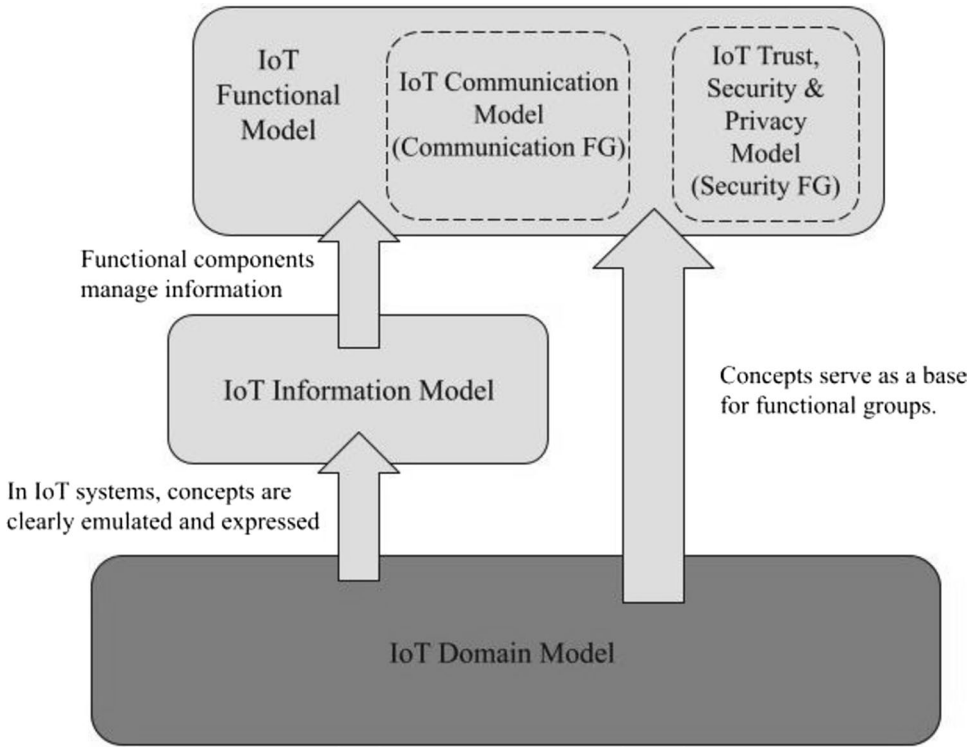

Fig. 2 IoT reference model

2.3.1 IoT domain model

The explanation of the various aspects that relate to a particular interest area is provided by the IoT Domain Model. It distinguishes between what does and does not fluctuate significantly to provide great level of detail within the IoT Domain Model. The significance of providing this general understanding is crucial not only for scientific disclosure but also for internal communication within the project. Due to the IoT Model's resultant of general comprehension, the solutions are evaluated and analyzed for architectural issues and problems that arise in the project. IoT Domain Model is the most important model within the IoT Reference model due to its properties. It withholds primary abstractions along with its duties and relationships [52].

2.3.2 IoT information model

All the various aspects of the Domain Model which are presented in the digital world are modeled by the Information Model [53]. It also models the connections among the various aspects. It offers an infrastructure for data being used by systems. The IoT Information model is also known as meta-model. The infrastructure that it offers includes all the concepts of the system which is related with the retrieval, representation, processing, and collection of data.

2.3.3 IoT functional model

To help comprehend, the primary Functionality Groups (FG) and its relations among other ones is the goal of Functional model. The Functionality Groups consist of Functional Components (FC) which are identified and analyzed in terms of relation with other components by Functional Decomposition (FD) [54]. The Functional Model works as a framework that describes similar output of the primary functionalities. It entails three different aspects: abstract, functionality groups, and functional views. Firstly, the abstract describes the Functional model as a concept rather than implementation through a certain technology. Secondly, functionality groups itself are not enough, instead the relations between one another are required as well. Lastly, to provide the functions at runtime of the system and its overall description is the job of the functional view. To address the privacy and security challenges of IoT devices at the cloud computing layers, edge, fog, and smart objects layer, the conceptual architecture is built with the help of IoT security and communication model [55]. The IoT communication and IoT security models are discussed below.

2.3.4 IoT communication model

Smart objects and the cloud devices define the IoT communication model. To bridge communication protocols, the IoT gateway is used for instances such as Ethernet, Wi-Fi, Z-Wave, NFC, ZigBee, and RFID [50]. In the IoT

communication model, IoT gateway bridges constrained and unconstrained networks. Furthermore, IoT gateway also contributes in the translation of different protocols, such as constrained application protocol, and transformation of informational data among constrained networks of unconstrained networks and IoT devices. The unconstrained network includes high-speed bandwidth and high resource devices. On the other hand, constrained network consists of less resource and low bandwidth IoT devices. IoT devices that are rich in resource and have high-speed bandwidth come under the unconstrained networks, and devices that have relatively fewer resources and a lower communication bandwidth come under the constrained network. For instance, an IoT device that provides a communication bandwidth of less than 1 Mb/s is associated to a constrained network, but ones that provide much higher bandwidth are associated to an unconstrained network [56].

2.3.5 IoT security model

IoT Security model describes the security methods and regulations which the security of IoT devices and information shared between them is based upon. The IoT security model consists of 3 layers [47]: (i) service security layer, (ii) communication security layer, (iii) application security layer. Cryptographic schemes, risk assessment, intrusion detection systems (IDSs), and blockchain-based solutions are all different security techniques introduced to detect cyber security attacks and provide security in IoT. CISCO proposed a model that consists of 7 different layers: physical devices and controllers, connectivity, edge (fog) computing, data accumulation, data abstraction, application, and collaboration and processes [57]. The CISCO 7-layer model was adapted to implement lightweight cryptographic solutions in the IoT systems for security purposes. Earlier, a 4-layer reference model was used, that consisted of cloud computing, fog computing, edge computing, and smart objects. Each and every layer of the 4-layer reference model corresponds to layers in the CISCO model, whose intrinsic capabilities are served by different devices operating on these layers. Each device is associated with a layer, that fits accordingly by the constrained resources to support the different tasks in different layers. The security mechanism depends on the hardware specifications of such devices.

2.4 Classification of IoT devices

Due to the computational power and capability, low memory, and internal storage, the IoT connected devices are displayed in the layers of the architecture within restrained proficiency. The IoT ecosystem uses a variety of service structures, protocols, and network designs to handle the billions of IoT devices that communicate with one another. Class 2, Class 1, and Class 0 are the three categories that IoT devices can be divided into [58]. The devices are differentiated in terms of required Random Access Memory (RAM) and Read-Only Memory (ROM) to operate.

2.4.1 Class 0

IoT devices that are restricted to the resources such as computational capability, memory, and power fall under the Class 0 category of IoT devices. Such devices are available at the perception layer of the IoT architecture, therefore communicates and sense data through protocols for lightweight communication [59]. Low-end nodes are present in the low-end IoT devices, fall under Class 0. Such node's security is the main concern as they more inclined to be vulnerable for threats. Mostly the devices under this category are sensors and actuators such as temperature sensors, light sensors, motion sensors, proximity sensors, humidity sensors, actuators, magnetic sensors, etc.

2.4.2 Class 1

In comparison to low-end nodes, Class 1 IoT devices contain a higher number of resources. These devices, rest over low-end IoT devices in order to enhance the capabilities of class 0 node devices, basically simple microcontrollers [60, 61]. To secure data, such devices can implement data encryption technology. Few examples of such devices that are associated to Class 1 are different types of gateways and hubs such as industrial gateways, cellular gateways, smart home hubs, etc.

2.4.3 Class 2

Devices with a mass number of resources in terms of flash memory, CPU, and RAM are considered to be in the Class 2 IoT devices. A great example for a Class 2 IoT device is Single-board computer such as LINUX and UNIX that implement traditional operating systems [62]. Security is not the main concern for such devices due to having a higher number of resources compared to other category IoT devices. Devices that full under the Class 2 category are different servers such as cloud servers, IoT platform servers, cloud storage servers, application servers, edge cloud servers, data analytics servers etc.

Table 2 presents the hardware-based comparison of various classes of IoT devices.

2.5 Security attacks in different layers

This subsection lists the various different security attacks involved in each layer. However, since network layer and perception layer are more prone and vulnerable to attacks

from intruders, they are discussed in more detail compared to the application layer and middleware layer.

2.5.1 Application layer security attacks

Buffer overflow attacks [63, 64] overwrite memory off-limits and out of bounds so that a buffer overflow occurs in the system. Cross-site scripting attacks [65] include injecting malicious code to perform malicious activities on the web pages. SQL injection attacks [66] manipulate database through given input which is malicious in behavior. Phishing attacks [67] use deceptive tactics to steal private data from the users.

2.5.2 Middleware layer security attacks

Malware and Ransom [68] attacks include the use of malicious software that compromises the system or data in the database. Sleep deprivation attacks [69] include disrupting system or human performance through sleep deprivation.

2.5.3 Network layer security attacks

Denial-of-Service (DoS) attacks [70] focus on overwhelming the system to render it inaccessible for authorized users to enter into the system. Distributed-Denial-of-Service (DDoS) attacks [70] coordinate DoS attack from different sources enabling higher impact on the system to become overwhelmed and inaccessible. Therefore, the DDoS increases the chances of no functionality from the system due to the DoS attacks being sent from multiple sources. Man-in-the-middle attacks [71], also known as the eavesdropping attack, that includes eavesdropping of data between two parties and manipulating the data for malicious activities. Sinkhole attacks [72] divert the network traffic to unauthorized users. Traffic analysis attacks [73] includes monitoring and analyzing network traffic to extract information between parties.

2.5.4 Perception layer security attacks

Jamming attacks [74] disrupt the wireless communication through the interference signals between two parties. Physical capture or damage attacks [74] includes physical damage being done to Io T devices that result in either non-functional IoT device or unrepairable state of the IoT device. Battery draining attacks [75] drain as much of the power source as possible from IoT devices to shut down the device on its own. Device cloning attacks [76]involves creating unauthorized copies of IoT devices to use for malicious actives. These are only a few cyberattacks mentioned above to highlight the attacks in each layer. Table 3 presents the summary of various at tacks launched in different IoT layers.

Table 2 Categories of IoT devices

Category	RAM	Flash	Description	IoT Devices
Class 0 [59]	Less than 1 KB	Less than 100 KB	Communicate and sense data through protocols for light-weight communication	• Temperature sensors • Light sensors • Motion sensors • Proximity sensors • Humidity sensors • Accelerometers • Pressure sensors • Gas sensors • Magnetic sensors • Actuators
Class 1 [60, 61]	About 10 KB	About 100 KB	Rest over low-end IoT devices in order to enhance the capabilities of class 0 node devices	• Smart home hubs • Industrial gateways • Edge computing devices • Cellular gateways • Data concentrators • Protocol converters
Class 2 [62]	About 50 KB	About 250 KB	Devices with a mass number of resources in terms of flash memory, CPU, and RAM	• Cloud servers • IoT platform servers • Data storage servers • Application servers • Edge cloud servers • Data analytics servers

3 6Need for securing the IoT system

There are primarily three reasons that summarize the importance of security within IoT. Firstly, uncontrolled IoT systems not only imperil user's privacy, but can also result into massive damage physically when interconnected devices are used negatively. Secondly, producers are at large risk because they can lose sensitive and important information when intruders gain access to database via the IoT system that withholds confidential information. Lastly, the effect of an attack extends outside a network or single device due to the IoT systems being largely interconnected. Therefore, protecting customer privacy, vital infrastructure and database, and websites from large-scale cyberattacks requires the security of linked IoT devices. About 70% of technologies in IoT include some security issues, stated in a study that was guided by Hewlett-Packard [77, 78]. Even though security in IoT systems is a fundamental aspect, many vendors introduce products into the market with minimal emphasis on its security [79]. Such vulnerability within it can result into various issues regarding integrity, confidentiality, and privacy. Therefore, the security in IoT systems is not highly prioritized, even though it should be. This is due to requirements of the consumers that contradict with providing high level security in IoT systems. For example, battery-efficiency, restriction to size for compatibility, physical appearance, user-friendly, etc. and to be able to provide all these features in a restricted time and low budget. Of course, some features vary between one IoT device to another, but majority of the devices focus on these consumer requirements that leads to developing a device with low security measurements. Each layer within the IoT Architecture requires some security features. A list of requirements within each layer of the IoT Architecture is shown in Fig. 3.

4 Lightweight cryptographic methods for IoT

Lightweight cryptography, a protocol or cryptographic algorithm, is created to be implemented in constrained environments such as health-care devices, sensors, RFID tags, and contactless cards. ISO/IEC 29192 is a standardization document that contains and discusses the properties of lightweight cryptography [80, 81]. Lightweight properties are explained in terms of target platforms in ISO/IEC 29192. The implementations are broken into two parts -software and hardware. A smaller program in terms of line of code and a smaller RAM size are preferred for software implementations in lightweight applications. To evaluate the lightweight properties, the energy consumption and chip size are crucial for hardware implementation [82]. Regarding implementation characteristics, the lightweight methods offer sufficient security and outperform traditional cryptographic ones, which are currently implemented in Internet security protocols.

There are primarily four types of lightweight cryptographic methods accessible for use. The four methods are Lightweight Block Cipher (LWBC), Lightweight Stream Cipher (LWSC), Hash Functions, and Elliptic Curve Cryptography (ECC) as shown in Fig. 4 [83]. Structure of each method, block and key size, and number of rounds are the

Table 3 Summary of attacks in various IoT Layers

Layer	Attack	Severity of attack	Objective of attack
Application layer	Buffer overflow [63, 64]	H	Overwriting memory beyond allocated bounds
	Cross site scripting [65]	N	Injecting malicious code into web pages
	SQL Injection [66]	H	Manipulating database queries through malicious input
	Phishing [67]	N	Deceptive tactics to steal personal information
Middleware layer	Malware and Ransom [68]	H	Malicious software compromising systems or data
	Sleep deprivation [69]	N	Disrupting system or human performance through sleep deprivation
Network layer	DoS [70]	H	Overwhelming a system to render it inaccessible
	DDoS [70]	H	Simultaneous, coordinated DoS attacks from multiple sources
	Man-in-the-middle [71]	H	Manipulating communication between parties
	Sinkhole [72]	N	Diverting network traffic to unauthorized destination
	Traffic analysis [73]	N	Monitoring and analyzing network traffic to extract information
Perception layer	Jamming [74]	N	Disrupting wireless communication through interference signals
	Physical capture or damage [74]	H	Physically compromising or damaging IoT devices
	Battery draining [75]	N	Draining the power source of IoT devices
	Device cloning [76]	H	Creating unauthorized copies of IoT devices

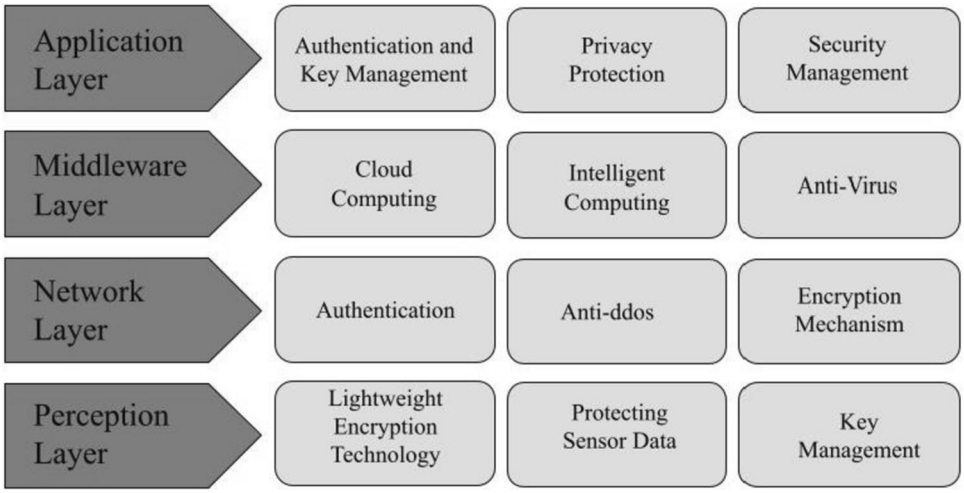

Fig. 3 Security requirements in each layer of the IoT architecture

factors that the four methods can be analyzed by. LWBC, LWSC and Hash functions are classified as symmetric lightweight cryptography, but ECC is classified as asymmetric lightweight cryptography. ECC can provide non-repudiation, and authentication due to its asymmetric cipher functionalities [84].

Ultra-lightweight, lightweight, and low-cost are three classifications of cryptographic algorithms [85]. Software and hardware implementation along with the capabilities of the device are three parameters that classify each cryptographic algorithm. Read-Only memory (ROM) and Random-Access memory (RAM) needs for the implementation of the cipher is specified by the software implementation, the first parameter. The second parameter, device capability, refers to the restriction of resources in the device or whether the device is resource-constrained or not. Resource-constrained devices are constrained in terms of resources; therefore, they lack in the rich resource naturistic. Lastly, hardware implementation offers the information related to Gate Equivalence (GE) or chip area that is necessary for algorithm's implementation. All three parameters help in the classification of cryptographic algorithms. To decide the requirements of a security mechanism for an IoT system, the IoT architecture is a very crucial factor in that decision [86]. Since IoT

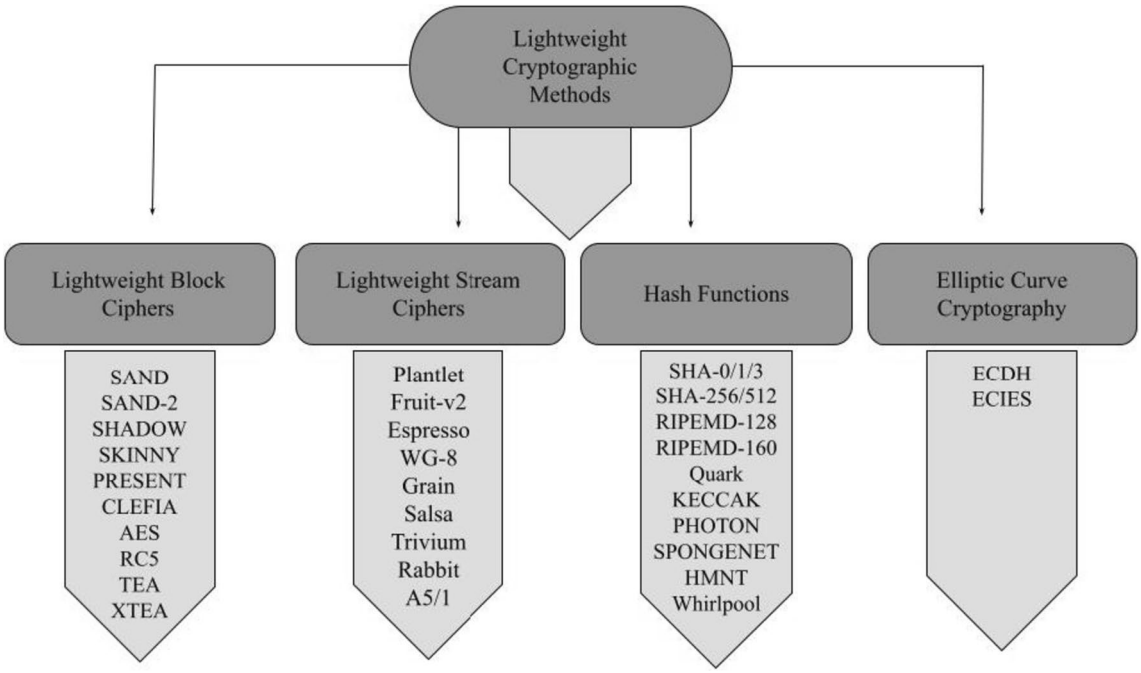

Fig. 4 Lightweight cryptographic methods for IoT

system is built off of the IoT architecture, each layer in the IoT architecture has its own security requirements. Lightweight secure routing protocols, lightweight cryptographic algorithms, lightweight antimalware solutions, etc. can be implemented in IoT systems for security purposes [87].

ECC is mainly used as a method at the application layer, physical, and network layer [88]. In IPv6, both Digital Encryption Standard (DES), and Advanced Encryption Standard (AES) could be utilized. Due to the requirement of higher resources in traditional cryptographic techniques, the devices at the physical layer in IoT use lightweight cryptographic techniques which relatively don't require utilization of a lot more resources. Lightweight cryptographic techniques don't require devices to have higher resources, therefore they are suited for the devices in IoT. Table 4 presents the three parameters in its classification of cryptographic algorithms.

4.1 Lightweight block cipher

Symmetric ciphers that process a complete block at once are known as block ciphers. Feistel network (FN) and Substitution-permutation network (SPN) are two primary types of structures that lightweight block ciphers are based on [105]. Round function is used on half of the state for Feistel structures. Since the same code is used for encryption and decryption process in Feistel structures, it results into low memory usage. On the other hand, SPN doesn't require a key schedule, therefore it foresees attacks. SPN is more compatible due to its requirement of fewer rounds of execution. Thus, it works better in resource constrained devices. The main purpose of lightweight cipher is to overcome difficulties related to security, memory footprint and power consumption. Compared to 64-bits and 128-bits block size in traditional algorithms, the block size must be of 32–64 bits for the algorithm to be considered a lightweight algorithm [106]. Rivest developed a symmetric block cipher that was extremely fast as of the time, known as RC5 [107]. The cipher provided variable key length along with variable word size. RC5 is appropriate for the two parameters mentioned previously for lightweight algorithms, software and hardware implementation. Another lightweight algorithm introduced in 1994 was Tiny Encryption Algorithm (TEA) [108]. Rather than focusing on software and hardware implementation, the TEA is more focused on being suitable for wireless communication.

Overall, TEA was great and secure since it provided provide non-linearity with the implementation of ADD and XOR operations alternatively, however, the issues came down to its key size of 126 bits instead of 128 bits, and possibility of related-key attacks. While the disparity in key size may not appear significant, its impact on cryptographic strength is substantial. The notable distinction is in the considerably greater number of possible key combinations offered by the 128-bit key compared to its 126-bit counterpart. Later on, in 1996, to surmount the issues faced in TEA, XTEA was introduced. XTEA overcame the issues in TEA by introducing key material and modifying the schedule of the key [109]. And then came in 1998, one of the popular block ciphers still used in IoT systems today, AES [110]. AES was designed by Daemen and Rijmen. AES goes under 10 rounds for key sizes of 128 bits, 12 rounds for 192 bits, and 14 rounds for 256 bits. A list of various lightweight block ciphers along with their attributes is presented in Table 5.

4.2 Lightweight stream cipher

Stream cipher is next on the list of lightweight cryptographic methods. At the time of encryption and decryption, 'r' bits are present in stream cipher. The main differentiating attributes among various ciphers are the key size, chip area, IV, and throughput. List of famous lightweight ciphers during the first generation of lightweight cryptography included Trivium, A5/1, Grain and Rabbit [125–128]. Trivium [125] is a block cipher-inspired stream cipher. A5/1 [126] was used for Global System for Mobile Communication (GSM). Rabbit was one of the stream ciphers introduced at an early stage of lightweight cryptography development [127]. Grain [128] is a two-register stream cipher with a non-linear output function. Grain uses an 80-bit key size to work optimally for energy usage, restricted memory, and gate count. However, the most crucial stream ciphers in the second generation of linear cryptography are Trivium and Grain. Popular stream ciphers during the second generation of lightweight cryptography are Lizard, WG-8, Espresso, Fruit and Plantnet. Lizzard is one of the latest stream ciphers that works on IV of 64 bits, and key size of 120 bits to provide minimal cost implementation [129]. WG-8 consumes low energy and is immune to attacks compared to different lightweight stream ciphers. Built for 5G applications and based on the Galois Non-Linear feedback Shift Register (NLFSR) structure, Espresso is used among many applications [130]. Based on Sprout cipher, Fruit cipher was introduced with improved security by designers compared to the sprout cipher [131]. Comparison among various lightweight stream ciphers is presented in Table 6.

4.3 Hash functions

Another method is hash functions that generate a fixed-length string or 'message digest' from a message of some length. There are various purposes of hash functions. Firstly, hash functions can be used to assure the data integrity within the system by determining whether any format of data has been modified or tampered with. Secondly, digital signatures

Table 4 Cryptographic algorithms classification

Classification	ROM/RAM	Device capability	GE	Ciphers	Description	IoT-based example
Lightweight cryptographic algorithms [88]	32 KB ROM 8 KB RAM	Rest below	Up to 3000 Gates	SOSEMA-NUK [91]	Software-oriented stream cipher designed for efficient implementation on various platforms	Remote sensor nodes transmit environmental data with minimal battery usage, aligning with SOSEMANUK's lightweight design
				CLEFIA [92]	Block cipher designed for efficient hardware and software implementations	Smart meters encrypt energy consumption of the data transmission efficiently, keeping meter functionality due to CLEFIA's optimized design
				DEXL [93]	Lightweight stream cipher with high performance and low hardware resource requirements	Wearable health monitors encrypt biometric data transmission efficiently, ensuring real-time monitoring capabilities with minimal energy usage

Table 4 (continued)

Classification	ROM/RAM	Device capability	GE	Ciphers	Description	IoT-based example
Low-cost cryptographic algorithms [89]	4 KB ROM 8 KB RAM	ATmega 128	Up to 2000 Gates	Lizard [94]	Extremely lightweight and efficient hash-based message authentication code (HMAC) algorithm	Smart home devices authenticate and verify data integrity during communication with a central hub, ensuring secure home automation with minimal resource consumption
				Trivium [95]	Stream cipher with minimal hardware requirements and high performance	Wireless sensor nodes encrypt soil moisture data transmission, ensuring data confidentiality and integrity in agricultural IoT networks with minimal resource usage
				TWINE [96]	Block cipher optimized for both hardware and software implementations	Smart locks encrypt access control messages, ensuring secure communication with minimal impact on device performance due to TWINE's lightweight design
				SIMON [97]	Lightweight block cipher optimized for hardware and software implementations	Industrial sensors encrypt equipment performance data transmission efficiently, ensuring data security without compromising device performance, leveraging SIMON's optimized design
				MIBS [98]	Stream cipher designed for low-power, low-latency applications	Low-power IoT devices in smart city networks securely transmit environmental data, conserving energy usage due to MIBS's lightweight implementation
				PRESENT [99]	Block cipher designed for low-resource devices and applications	IoT devices in smart grid networks transmit power consumption data securely, maintaining system efficiency with PRESENT's lightweight encryption

Table 4 (continued)

Classification	ROM/RAM	Device capability	GE	Ciphers	Description	IoT-based example
Ultra-lightweight cryptographic algorithms [90]	4 KB ROM 256 B RAM	8051 microco-ntroller,ATiny 45	Up to 1000 Gates	Sprout [100]	Lightweight and compact cryptographic algorithm suitable for IoT devices	Healthcare devices transmit health data securely, preserving battery life and ensuring data privacy with Sprout's lightweight encryption
				KATAN [101]	Lightweight block cipher with extremely small memory footprint	IoT devices in smart transportation systems encrypt vehicle telemetry data, ensuring secure communication with minimal energy consumption due to KATAN's lightweight design
				QTL [102]	Stream cipher with minimal computational overhead and low memory requirements	IoT devices in smart building networks securely transmit occupancy data, ensuring data privacy with minimal computational overhead using QTL's lightweight encryption
				HUMMI-GBIRD [103]	Lightweight block cipher with minimal memory requirements and low computational overhead	Environmental sensors in climate monitoring IoT networks encrypt data transmission efficiently, ensuring data security without resource strain with HUMMINGBIRD's lightweight encryption
				Piccolo [104]	Lightweight block cipher designed for constrained environments	IoT devices in smart retail environments transmit inventory data securely, preserving data confidentiality with Piccolo's lightweight encryption without impacting device performance

Table 5 Design characteristics of various block ciphers

Block cipher	Structure	Device	Key size (bit)	Block size (bit)	Rounds	Output (Mbps)
SAND [111]	FN	Virtex-5	64/128	64/128	48/54	1465.2/1550.4
SAND-2 [112]	FN	Virtex-5	128	–	47	1705.4
SHADOW [113]	Generalized FN	Virtex-5	64/128	32/64	16/32	226.81
SKINNY [114]	SPN	Virtex-7	64/ 128	64 /96	32/36	49,150/71,680
PRESENT [115]	SPN	Kintex-7	80/128	64	31	1319.22/1529.80
CLEFIA [116, 117]	FN	Artix-7	128/192/256	39/128/128	2488	990/818/696
AES-128 [110, 118]	SPN	Virtex-5	128	128	10	4342/3485
AES-256 [119]	SPN	Virtex-7	256	128	14	278
RC5 [120, 121]	FN	Xilinx Vertex-2	0–2040	32/64/128	0–255	533
TEA [122, 123]	FN	Spartan-7	128	–	64	19.52
XTEA [124]	FN	Spartan-7	128	64	64	312

Table 6 Design characteristics of various stream ciphers

Stream cipher	Key size	IV	Chip area	Type	Output (Mbps)
Plantlet [132]	80	90	928	LFSR + NLFSR + Counter	–
Fruit-v2 [131]	64/80	64	990	LFSR + NLFSR	0.100
Espresso [130]	128	96	1500	Galois structure NLFSR	–
WG-8 [133]	80	80	1786/3942	4 Trivium like SHR	500/6710
Grain-128a [134]	128	96	1857/4617	LFSR + NLFSR	925.9/14479.6
Salsa-20/r [135]	128/256	128	12,126	ARX	990
Trivium [128]	80	80	2580/4921	3SHR	327.9/22299.6
Grain [127]	80, 128	64/96	1294/3239	LFSR, NLFSR	724.6/9876.5
Rabbit [126]	128	64	3800, 4100	Chaotic Table + arithmetic	0.080
A5/1 [125]	64	22	923	LFSR	0.050

are used to achieve non-repudiation and authenticity of a property, and to optimize the digital signature schemes, the message digest is signed rather than generating the signature for a whole message and signing it using a signature generation algorithm. Thirdly, hash functions may be implemented at the time of login for authentication of users by generating a message digest for a password and then compare it to the message digest of authorized password that is stored in the database to approve authentication and provide user the access to the system. Lastly, to generate both a series of sessions keys and pseudo random number, the hash functions can be used as one-way functions.

The size of the logic and number of state bits determines the footprint of a hash function. Inspired by Grain, a stream cipher, and KATAN, a block cipher, similar modified and improved version of a hash called Quark was presented in 2010 [136]. There are three different versions of Quark: s-Quark, U-Quark, and d-Quark. This hash family includes one of the most important hash functions in the industry. Yalcin and Kavun [137] introduced Keccak. With the 160-bit message digest, Keccak was a game changer. However, the only down side was due to its larger chip area compared to traditional standard for being lightweight. On the contrary, the lightest lightweight family of hash functions is PHOTON [138]. It requires the smallest chip area compared to any other. For internal permutation and domain extension, the creators have implemented sponge functions. To achieve a compact design, the SPONGENT [139] uses one of the simplest round functions.

Secure Hash Algorithm (SHA), Message Digest (MD), and RIPEMD (RACE Integrity Primitives Evaluation Message Digest) are one of the popular families of hash functions used in modern cryptography [142–148]. SHA is a family of hash functions that includes variants such as SHA-1, SHA-256, and SHA-3. Though, the initial version of SHA was SHA-0, and it is not considered a secure hash function anymore due to its vulnerabilities [142]. However, the other variants of SHA are widely implemented which offer different output sizes and adequate security levels [143, 144]. RIPEMD is another family of hash functions, though it may not be as popular compared to SHA and MD, but is known for its resistance against certain types of cryptographic attacks and its ability to generate shorter hash outputs. It has two variants, RIPEMD-128 and RIPEMD-160, where the 128 and 160 are the size of the message digest generated by the hash functions in bits [145, 146]. The MD family of

hash functions includes variants such as MD2, MD4, and MD5 are known for their simplicity and efficiency. MD2 was the first hash function in the MD family which generated a message digest of 128-bits. However, it could only operate on a 128-bit message block, whereas future variants such as MD4, and MD5 are able to operate on 512-bit message blocks [147, 148]. Table 7 represents various essential lightweight hash functions with respect to their message digest size, message block size, and possibility of collision.

4.4 Elliptic curve cryptography

In 1985, Neal and Miller Koblitz introduced the concept of ECC [149]. ECC and RSA are two of the most important and widely used asymmetric ciphers that provide security in IoT. Like RSA, ECC is also a public-key cryptosystem, however ECC provides the same security strength or level even with a smaller key size. Asymmetric ciphers such as ECC and RSA are not preferred for only two reasons: the consumption of higher memory and a larger key size. Since ECC has a higher computational complexity of the algorithm, it results into a higher execution time on 8-bit microcontrollers compared to algorithms like AES [150]. The concept of ECC is dependent on elliptic curves. The concept of ECC is implemented among other concepts like key exchange mechanism and encryption scheme, for example, the Elliptic Curve Diffie-Hellman (ECDH) Key Exchanging Mechanism, and Elliptic Curve Integrated Encryption Scheme (ECIES), respectively [151, 152].

ECC has several attributes including robust and efficient that offers several advantages in every layer of the IoT. Firstly, ECC offers advanced security measures and provides enhanced protection compared to traditional encryption [153]. ECC's effectiveness in preventing potential attacks contribute to its role in enhanced mobile Internet security. Secondly, elliptic curve cryptography proves advantageous for mobile Internet security. With a relatively compact key size of 256 bits, ECC requires less storage space compared to other encryption methods [154]. As mobile devices increasingly dominate online interactions, ECC's streamlined approach enhances user experiences and strengthens security measures for mobile Internet activities [155]. Lastly, Elliptic Curve Cryptography demonstrates superior properties. Despite employing shorter key lengths, ECC delivers robust security comparable to longer key lengths in traditional encryption algorithms. For example, a 256-bit ECC key offers similar security strength to a 3072-bit RSA key, which exceeds the standard RSA key length of 2048 bits [156]. Further, additional advantages in relation to each layer of IoT along with several specific use cases are presented in Table 8 below.

To implement cryptographic schemes, a group structure is provided by elliptic curves defined over a finite-field. The point at infinity, point O, is included in the set of rational points on the elliptic curve which are the elements of the group. Elliptic curves are defined by some mathematical functions. A general Elliptic curve is described below:

$$E(G) : y^2 = x^3 + ax + b \tag{1}$$

Here, a and b belong to G.

The graph of the general function is symmetric to the X-axis. And if a line were to be drawn on the coordinate, the elliptic curve will have a maximum of 3 intersections with the line. Figure 5 provides an overall understanding of the elliptic curve by illustrating the three-intersection points P,

Table 7 Comparison of various hashing algorithms

Hashing algorithm	Message digest (bit)	Message block (bit)	Collision
Quark [136]	128–224	256	Yes
KECCAK [137]	160	224–512	Yes
PHOTON [138]	80–256	128	Very unlikely
SPONGENET [139]	88–256	128	Very unlikely
HMNT [140]	128/256/512	824	Yes
Whirlpool [141]	512	512	No
SHA-0 [142]	160	512	Yes
SHA-1 [142]	160	512	Very unlikely
SHA-256/224 [143]	256/224	512	No
SHA-512/384 [143]	512/384	1024	No
SHA-3 [144]	224/256/384/512	1600	No
RIPEMD-128 [145]	128	512	No
RIPEMD-160 [146]	160	512	No
MD2 [147]	128	128	Yes
MD4 [148]	128	512	Yes
MD5 [148]	128	512	Very unlikely

Table 8 Advantages and use cases of ECC

Layer	Advantages	Use cases
Application layer	ECC traditionally offers compact key sizesthat to provides more secure data exchange in the application layer [156]	ECC-based ciphers provide a secure communication between IoT devices and applications along with authentication of IoT devices and users
Middleware layer	In the middleware layer, ECC helps with computational overhead and compatibility with constrained devices. [154]	The data exchange between middleware components is secured through ECC The storage and retrieval of sensitive data between devices is handled by ECC
Network layer	ECC uses bandwidth-efficient encryption and robust security against attacks to offer enhanced protection in the network layer [158]	At the network layer, ECC provides a secure communication over wireless and wired networks in IoT environments that ensures the confidentiality and integrity of data transmitted between IoT devices, gateways, and backend servers
Perception layer	ECC offers small memory footprint and fast key generation suitable for resource-constrained sensor nodes at the perception layer of IoT systems. [157]	In the perception layer, ECC helps with the authentication and authorization of sensor nodes within IoT networks It also enables secure collection and transmission of sensor data to higher layers of the IoT architecture

Q, and R on the coordinate between the line A and general elliptic curve B.

The RSA algorithm's security relies on the computational difficulty of the discrete logarithm problem. On the other hand, the elliptic curve discrete logarithm problem (ECDLP) is used in ECC, which replaces the multiplicative groups with different groups while maintaining the computational difficulty. Addition and doubling operations replace multiplication and squaring in these groups, allowing for faster execution. Moreover, selecting appropriate curve models can result in efficient implementation of scalar multiplications. The NIST and Safe curves website [159] provide the specifications and models of such curves. Table 9 depicts the process of encryption and decryption in ECC.

4.4.1 ECDH

For the encryption of bulk data, symmetric key cryptography is a better option since the dependency of security is on its key agreement protocol and it provides voice packets. Deciding factor for the leaking of keys shared between two users is the security level of the key agreement protocol. However, the weak key in Diffie Hellman key agreement mechanism is an issue. Therefore, an improved key exchanging mechanism is required. ECDH on the other hand, is also a key agreement protocol which provides generation of a secret key shared between two parties [160]. In ECDH, public key, domain value, and elliptic curve are exchanged between both parties. Through the help of the information exchanged between both parties, a shared secret value is computed. And, even if a third party tries to calculate the secret value from gaining the public information, it will be unsuccessful until and unless the third party has the private data value. The diagram for ECDH key exchanging mechanism is shown in Fig. 6.

4.4.2 ECIES

Rogaway and Bellare presented ECIES in 1997, which is also known as DHIES [128]. It resulted from improvements in the ElGamal encryption protocol. It entails a security system that consists of calculations of MAC Code hash and algorithms based on symmetric-key cryptography. It is an integrated encryption system. The functions for ECIES are discussed below [131]. Firstly, Key Agreement (KA) is performed, which is a function for the key generation process done by both sender and recipient of a shared secret key. Secondly, Key Derivation Function (KDF) is executed, where a set of keys are produced from the chosen parameters and keying material. Thirdly, Encryption (ENC), which is the cryptographic algorithm based on symmetric key cryptography and utilizes only one key. Fourthly, Message Authentication Code (MAC), which is the data used to message authentication. Lastly, Hash (HASH), also known as the

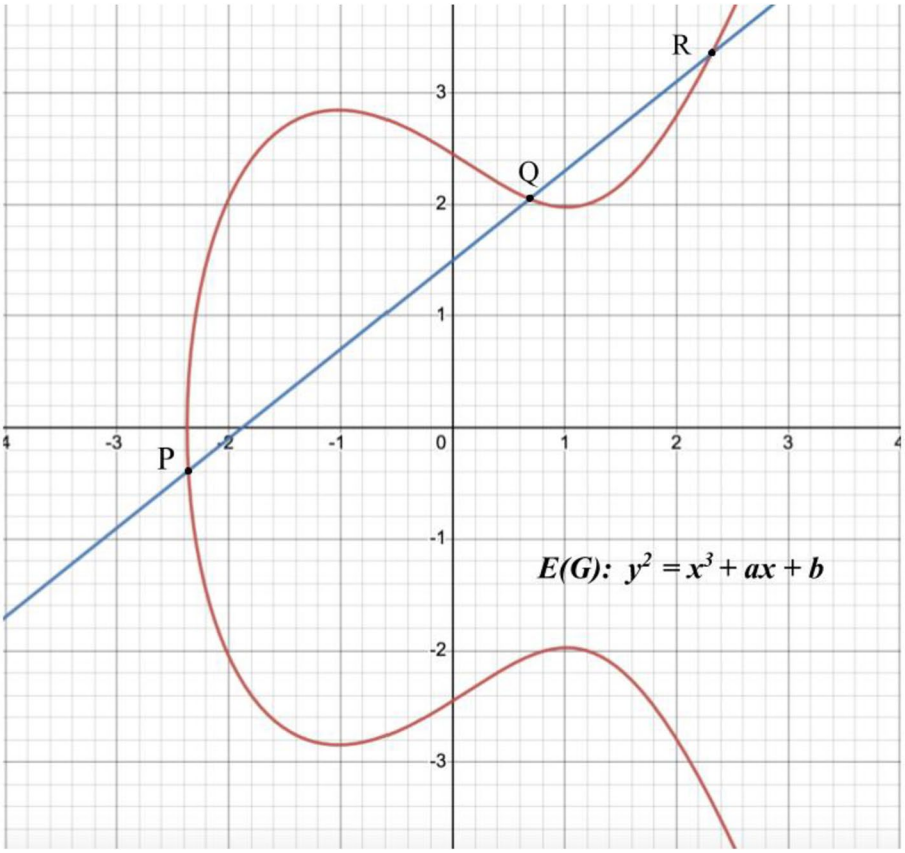

Fig. 5 Elliptic curve on coordinate geometry

digest function. The ECIES encryption-decryption process between User A (sender) and User B (receiver) is depicted in Figs. 7 and 8 respectively.

5 Role of LWC in IoT

LWC handles the unique security demands of the various IoT applications. It considers the dynamic features of IoT devices, including their compact form size, limited memory, and restricted power supply. LWC algorithms are designed to provide appropriate security while reducing computational cost. LWC also improves the power consumption and the lifespan of IoT devices. Conserving power is an important concern for IoT devices, which frequently use restricted sources of power or depend on renewable energy techniques. LWC algorithms are intended to be computationally light, with the goal of reducing the computational overhead necessary for cryptographic operations. This guarantees that IoT devices can employ encryption, digital signatures, secure key exchange, and other cryptographic services required for securing sensitive data and assuring the integrity of IoT connections in an efficient manner.

Another essential feature of LWC in IoT is that it allows for real-time and low-latency operations. Many IoT applications need rapid analysis of information and short reaction times. LWC methods are intended to offer quick encryption and decryption, permitting real-time protected communication and data processing [161]. LWC enables IoT devices to satisfy the strict time requirements of many IoT applications, such as manufacturing automation, energy management systems, and healthcare tracking, by minimizing computational complexity and reducing the delay induced by cryptographic processes [162]. And, LWC also encourages compatibility and uniformity within the IoT ecosystem. The centralization of lightweight cryptographic methods promotes interoperability across various IoT devices and systems. This enables easy integration, secure communication, and data sharing among diverse IoT components, independent of implementation. Overall, LWC plays a major role in various sectors of IoT such as Smart cities, IIoT, Healthcare, Smart Home Automation, Agriculture, and Smart Energy grids. The major role played by LWC in the different sectors of IoT is discussed in the subsections below [163–196].

5.1 LWC in smart cities

It is critical to protect the enormous group of linked devices and networks in smart cities, assuring data and services

Table 9 Encryption decryption in ECC

The Global Public elements are

i. $E_q(a,b)$ – Elliptic curve with parameters a, b, and q, where q is a prime number or integer of the form 2

ii. G– Point on the elliptic curve whose value is large order of n (i)

User A Key Generation

i. Select Private Key $\boldsymbol{n_A}$, where $\boldsymbol{n_A}$<$\boldsymbol{n}$

ii. Calculate Public Key $\boldsymbol{P_A}$, $\boldsymbol{P_A = n_A\, X\, G}$

User B Key Generation

i. Select Private Key $\boldsymbol{n_B}$ where $\boldsymbol{n_B}$<$\boldsymbol{n}$

ii. Calculate Public Key $\mathbf{P_B}$, $\boldsymbol{P_B = n_B\, X\, G}$ (ii)

Calculation of Secret Key by User A

$$\boldsymbol{k = n_A X\, P_B}$$

Calculation of Secret Key by User B

$$\boldsymbol{k = n_B X\, P_A}$$

Algorithm: ECC Encryption

Input: 1. **M**← Message

2. **G**← (i)

3. $\boldsymbol{P_B}$← (ii)

Output: Cipher point "$\boldsymbol{c_m}$"

1. **Start**
2. $\boldsymbol{int\ k}$←random integer
3. $\boldsymbol{P_m}$←$Encodedpointfor Monellipticcurve$ (iii)
4. $\boldsymbol{c_m = \{kG, P_m + kP_B\}}$
5. ***End***

Algorithm: ECC Decryption

Input: 1. $\boldsymbol{n_B}$← Private Key of User B

2. **G** ← (i)

3. $\boldsymbol{P_B}$← (ii)

4. $\boldsymbol{P_m}$←(iii)

Output: **M** ←Original Message

1. **Start**
2. $\boldsymbol{kG * n_B}$
3. $\boldsymbol{P_m + kP_B - (kG * n_B)}$
4. $\boldsymbol{P_m + kP_B - (kG * n_B)}$ (iv)
5. Substitute (ii) for $\boldsymbol{G * n_B}$in (iv)
6. $\boldsymbol{P_m}$ ~~$\boldsymbol{+ kP_B - (kP_B)}$~~
7. $\boldsymbol{P_m}$
8. **Simplify** $\boldsymbol{P_m}$
9. Result ← M
10. **End**

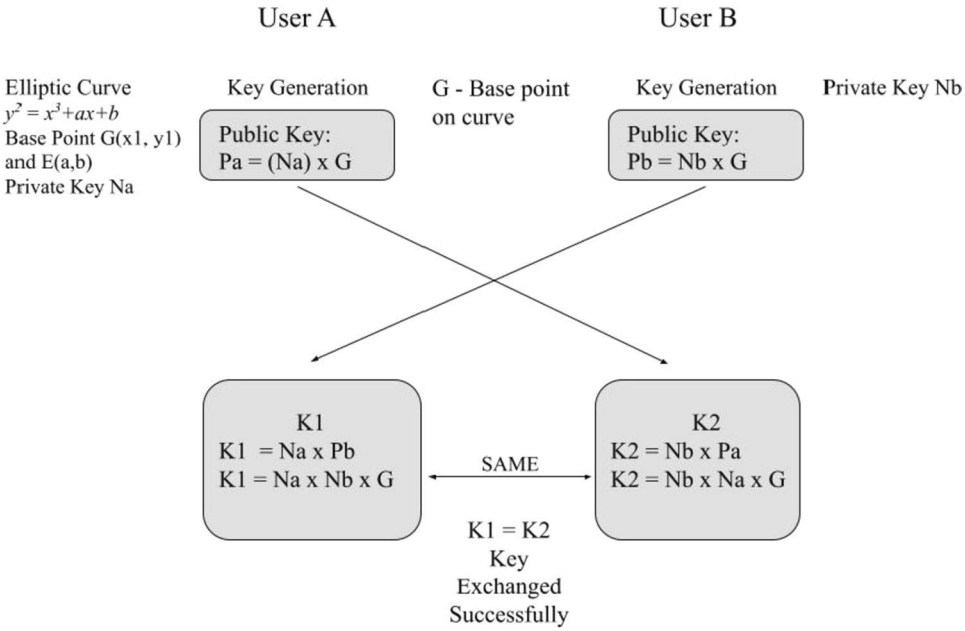

Fig. 6 ECDH key exchanging mechanism

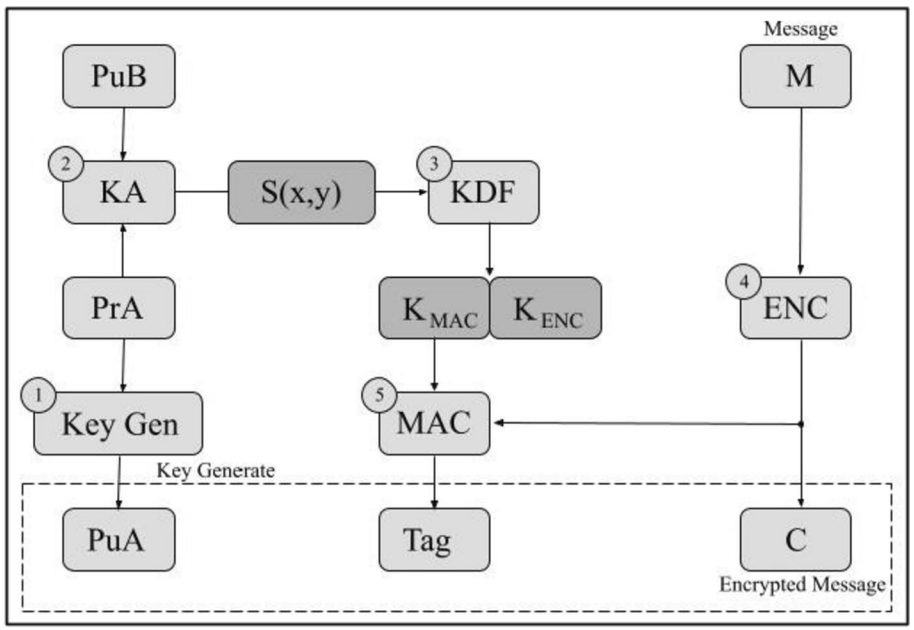

Fig. 7 Encryption in ECIES

safety, reliability, and accessibility. LWC algorithms provide a safe connection among smart city components such as public facilities and amenities, transportation systems, sensors, and smart grids preventing unauthorized use and data breaches [134]. Vital facilities and amenities such as smart lighting, traffic control, security systems, garbage disposal, and ecological monitoring benefit from LWC [164]. It enables safe data interchange among local administration, suppliers, and people while preserving personal information and maintaining privacy. It is a major task to protect smart city systems from various cyber threats and maintain the urban infrastructure security. LWC algorithms help in identifying and mitigating possible cyber threats on smart city systems, preventing interruptions to maintain the security of the urban infrastructure [165]. Such algorithms are essential for the security of applications and services based on IoT.

Pandey et al. [166] delves into the complexities surrounding data protection in smart cities and examines lightweight cryptographic algorithms as potential solutions. Yu etal. [165] introduced a secure and lightweight authentication protocol, SLAP-IoD, leveraging a physical unclonable function (PUF) for Internet of Devices (IoD) applications

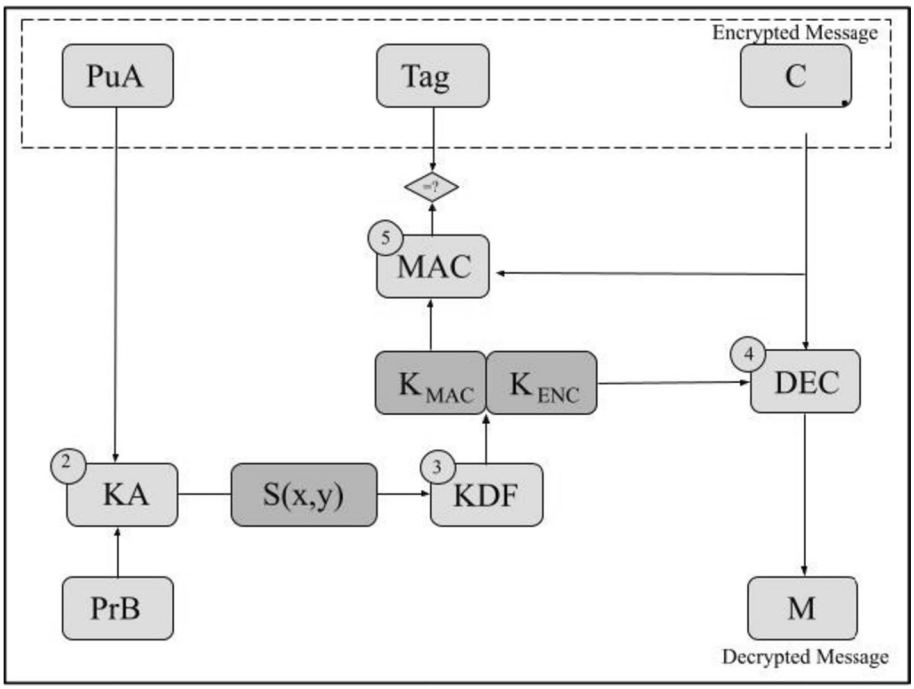

Fig. 8 Decryption in ECIES

in smart city environments. Bajwa et al. [167] utilizes Blockchain technology and the Iterative Filtering (IF) Algorithm to address data privacy concerns and mitigate collusion attacks. Othman et al. [168] proposed a physically secure privacy-preserving message authentication protocol incorporating Physical Unclonable Function (PUF) and Secret Sharing mechanisms.

5.2 LWC in IIoT

LWC plays an important part in protecting the information transmission inside industrial systems, as well as protecting important components and assuring continuous operation. To prevent any data breaches and unlawful access, LWC provides various cryptographic methods that have strong encryption to preserve sensitive data being exchanged between industrial gadgets, controllers, and corporate systems. LWC provides reliable authentication of devices along with access control, and prohibit unauthorized devices or organizations from gaining access to vital systems [169]. It also offers the detection and prevention of breaches inside commercial networks, assuring data integrity and the dependability of automation systems in industries [170].

Kharghani et al. [171] presents a new non-inclusive ROM and MTP function CLS scheme based on pairing. Gupta el al. [172] developed a forward privacy based searchable lightweight public-key encryption. Karati et al. [170] used the concept of lattice cryptography to propose key exchange protocol based on novel identify that offers several security attributes in the IoT. Chen et al. [173] incorporated hash functions, physically unclonable function, and lightweight cryptographic functions to develop a new authentication scheme.

5.3 LWC in healthcare

In the Healthcare sector, the electronic medical records (EMR) must be kept private and secure. Integrity of data must be secured and valuable data must be safeguarded from unauthorized use or disclosure. LWC facilitates encrypted interaction between medical equipment, sensors on clothing, EMR systems, and healthcare professionals, maintaining data integrity and avoiding manipulation [174]. LWC methods provide a secure connection between patients during video consultations and secure transmission of information between the two, ensuring the privacy of private health data [175].

John et al. [176] developed a Real-Time Distant Healthcare Monitoring IoT System (RTDHMIS) to safeguard patient data that utilizes a lightweight block cipher BEST-1 (Better Encryption Security Technique-1) for encryption purposes. Maram et al. [177] highlights the challenges associated with securing private healthcare data transmitted through IoT networks and offering a solution that integrates deep learning algorithms with straightforward encryption techniques. Patwari et al. [178] presents a Lightweight Cryptography (LWC) technique tailored for healthcare Wearable IoT device data protection. Padmashree et al. [179] proposed a framework that allows patients to directly supply

the encryption key to healthcare providers as part of routine access procedures.

5.4 LWC in smart home automation

To ensure anonymity and security of private details and user actions, LWC methods provide end-to-end encryption for data transmitted between smart home appliances [180]. The methods offer safe identification and access control techniques to prevent unauthorized people from taking control of or manipulating with smart home devices. Communication must be encrypted between devices, ports of entry, and cloud-based services. LWC encrypts the communication which prevents any data breaches and guarantees smart home network integrity [181]. It provides smart device secure over-the-air (OTA) upgrades, guaranteeing that software modifications and updates are validated and sent securely to avoid unapproved changes [182].

Nimmy et al. [180] proposed a smart home application protocol that implements a lightweight remote user authentication and offers privacy. An et al. [183] developed a scheme for online/offline sign cryption that is certificateless. Verma et al. [184] highlights the secure automation offered by a smart automation system using ESP32-CAM and ESP32 modules.

5.5 LWC in agriculture

It is essential to safeguard the interaction and transmission of data in IoT applications for agricultural to preserve private data linked to crop management, meteorological conditions, and irrigation systems [185]. The algorithms protect the integrity and security of data exchanged between agricultural monitoring devices, automated machinery, and farm administration systems, which prevents unauthorized access or manipulation [186]. Similar to the role of LWC in IoT, it offers detection of possible hazards to crop health, which allows for quick action and optimization of resource allocation for increased yield and sustainability [187]. It enables a secure connection between agricultural IoT equipment and cloud-based analytics systems, allowing farmers to make data-driven choices while protecting the confidentiality and safety of their agricultural data.

Prvulović et al. [188] develops a layered wireless sensor networks architecture that is energy efficient and used to estimate several lightweight cryptographic. Itoo et al. [189] introduces an agreement framework that is efficient and preserves privacy within smart agriculture monitoring systems. Saini et al. [190] presents a system for key negotiation using hash function and elliptic curve cryptography that offers support to smart agricultural monitoring systems.

5.6 LWC in smart energy grids

Unlawful access, manipulation, and cyber threats are issues in data sharing and smart energy grid communication which can be resolved by LWC. It provides secure communication between smart meters, energy management systems, and utility companies, assuring accurate metering and billing data while preventing any sort of manipulation on data which is unauthorized [191]. LWC algorithms offer detection and mitigation of cyber assaults on crucial energy infrastructure, preventing interruptions or unapproved control [192]. It maintains the smart grid's stability and resilience by securing the communication between renewable energy sources, grid monitoring devices, and energy distribution networks [193].

You et al. [194] presents a scheme for mutual authentication which is lightweight in nature for Smartt Energy Grids. Wang et al. [195] proposed a blockchain based technology called BlockSLAP that lowers the process of interaction to two steps and decentralizes the authority of registration. Jyoti et al. [196] analyzed the problems in the existing schemes and suggested an Anonymous Lightweight Key Agreement Framework (ALKAF) for the SG network. Table 10 highlights the several major advancements within the diverse sectors of IoT below.

6 Recent advancements

The fast rise of the IoT in recent years has resulted in the demand for the development of lightweight cryptographic algorithms to protect the enormous collection of interconnected devices [197]. Such lightweight cryptographic algorithms offer to deliver effective and resilient security solutions while taking into account of resource limitations on IoT devices. As a result, tremendous progress has been achieved in numerous areas of lightweight cryptography. This section discusses the recent advancements in lightweight cryptography methods for IoT, focusing on certain areas that have seen significant improvement. Such certain areas of recent advancementsincludeimprovement in the security of ciphers, new ciphers resilient to fault attacks, ciphers with improved performance, more optimized ciphers, ciphers for resource-constrained IoT devices, enhancements in noise stream ciphers, and extended versions of previous cipherswhich are discussed in the subsections below and presented in Table 10 [187–197].

6.1 Improvement in the security of ciphers

Improving cipher security is critical for protecting private information in a modern interrelated and data-driven society. The growth of technologies such as IoT and cloud

Table 10 Major advancements in the diverse sectors of IoT

IoT sector	Reference	Major contribution
Smart City	Pandey et al. [166]	Delves into the complexities surrounding data protection in smart cities and examines lightweight cryptographic algorithms as potential solutions
	Yu et al. [165]	Introduced a secure and lightweight authentication protocol, SLAP-IoD, leveraging a physical unclonable function (PUF) for Internet of Devices (IoD) applications in smart city environments
	Bajwa et al. [167]	Utilizes Blockchain technology and the Iterative Filtering (IF) Algorithm to address data privacy concerns and mitigate collusion attacks
	Othman et al. [168]	Proposed a physically secure privacy-preserving message authentication protocol incorporating Physical Unclonable Function (PUF) and Secret Sharing mechanisms
IIoT	Kharghani et al. [171]	Presents a new non-inclusive ROM and MTP function CLS scheme based on pairing
	Gupta el al. [172]	Developed a forward privacy based searchable lightweight public-key encryption
	Karati et al. [170]	Used the concept of lattice cryptography to propose key exchange protocol based on novel identify that offers several security attributes in the IIoT
	Chen et al. [173]	Incorporated hash functions, physically unclonable function, and lightweight cryptographic functions to develop a new authentication scheme
Healthcare	John et al. [176]	Developed a Real-Time Distant Healthcare Monitoring IoT System (RTDHMIS) to safeguard patient data that utilizes a lightweight block cipher BEST-1 (Better Encryption Security Technique-1) for encryption purposes
	Maram et al. [177]	Highlights the challenges associated with securing private healthcare data transmitted through IoT networks and offering a solution that integrates deep learning algorithms with straightforward encryption techniques
	Patwari et al. [178]	Presented a Lightweight Cryptography (LWC) technique tailored for healthcare Wearable IoT device data protection
	Padmashree et al. [179]	Proposed a framework that allows patients to directly supply the encryption key to healthcare providers as part of routine access procedures
Smart Home Automation	Nimmy et al. [180]	Proposed a smart home application protocol that implements a lightweight remote user authentication and offers privacy
	An et al. [183]	Developed a scheme for online/offline signcryption that is certificateless
	Verma et al. [184]	Highlights the secure automation offered by a smart automation system using ESP32-CAM and ESP32 modules
Agriculture	Prvulović et al. [188]	Developed a layered wireless sensor networks architecture that is energy efficient and used to estimate several lightweight cryptographic
	Itoo et al. [189]	Introduced an agreement framework that is efficient and preserves privacy within smart agriculture monitoring systems
	Saini et al. [190]	Presented a system for key negotiation using hash function and elliptic curve cryptography that offers support to smart agricultural monitoring systems
Smart Energy Grids	You et al. [194]	Presented a scheme for mutual authentication which is lightweight in nature for Smartt Energy Grids
	Wang et al. [195]	Proposed a blockchain based technology called BlockSLAP that lowers the process of interaction to two steps and decentralizes the authority of registration
	Jyoti et al. [196]	Analyzed the problems in the existing schemes and suggested an Anonymous Lightweight Key Agreement Framework (ALKAF) for the SG network

computing, and greater amounts data transfer has called for the development of secure and efficient encryption methods. This section looks at important breakthroughs in cipher security advancements. Researchers have developed unique algorithms, methods, and encryption approaches to improve cypher security and handle different data protection concerns. In one of the latest works, Liu et al. [198] presented uBlock, a lightweight cipher algorithm for devices in IoT that improved the performance of encryption and decryption using sequential circuits. An improvement of two-fold can be seen in performance if better hardware and nanotechnology is implemented.

Kundu et al. [199] introduced a user independent multivariate group signature scheme that focused on providing anonymity of the user, no connection between users, and traceability using a protocol of 5-pass identification. Panchami et al. [200] presented Feather S-Box of 4-bit that enabled confusion in lightweight ciphers. Feather S-Box provides improved security in terms of balanced, nonlinearity, linear and differential cryptanalysis resistant, and

algebraic attack resistant. Thabit et al. [201] presented a new cryptographic algorithm that is lightweight in nature to provide security for cloud computing applications. The algorithm has improved encryption due to its higher complexity influenced by substitution permutation method and Feistel network structure. Devi et al. [202] presented an approach for malware detection and prevention using deep learning to provide security for transmission of data in IoT devices.

6.2 Ciphers resilient to fault attacks

The susceptibility of cryptographic algorithms to fault attacks creates substantial danger to sensitive data security. These attacks take use of cipher's vulnerability to purposeful or accidental faults introduced during execution, with the goal of compromising their integrity and threatening the confidentiality of the private data. Recognizing the importance of the situation, researchers have created viable solutions to improve ciphers resilience to fault attacks. This section explores into the most recent advances in the subject of fault attack-resistant ciphers, highlighting the novel ideas and techniques. Dofe et al. [203] proposed to prevent fault attacks in SIMON cipher by implementing a new microarchitecture that integrates different masking methods and operand permutation techniques. Roy et al. [204] presented SAFARI, a framework that outputs a C code which is fault attack protected for block ciphers based on the security requirements provided and its specifications of the cipher. The framework compounds various implementations of fault attack resistance in block ciphers automatically.

Potes-Ordez et al. [205] highlighted the need to protect trivium stream cipher from fault injection attacks and introduced various fault detection schemes to resolve the issue. Song et al. [206] presented a new variant of PIPO block cipher for a secure communication that is fast with optimized techniques implemented with ARM/NEON processor. Cnudde et al. [207] presented a new implementation of the block cipher, PRESENT, that provides security against not only fault attacks but also side-channel attacks. Liu et al. [208] proposed a countermeasure towards fault attacks based on a method that quantitively analyzes the protection of SPN structure block ciphers. Wang et al. [209] proposed the use of existing Benes network to resist fault attacks in cryptoprocessors with high performance.

6.3 High performance ciphers

It is critical to achieve faster performance in cryptographic algorithms in order to satisfy the rising needs of contemporary computer systems. This section examines important advances in enhancing the performance of cryptographic algorithms, with the goal of increasing efficiency and throughput. Researchers have developed novel methodologies and architectures for optimizing different ciphers, achieving major improvements in performance. Xu et al. [210] presented the use of pipelined design scheme in ZUC-256 to implement a high-throughput hardware for the cryptographic algorithm. To significantly shorten the algorithm's critical path and increase the operating frequency, the pipelined design scheme is implemented.

Pandey et al. [211] proposed an architecture for PRESENT cipher based on 8-bit data path to process key of 128-bits and plaintext of 64-bits that included 48 clock cycles. The architecture is integrated with a system-on-chip (SoC) environment to provide high performance and power efficiency in the cipher. Gupta et al. [212] presented such an architecture for RC4 Stream cipher that combined loop unrolling and hardware pipeline which per clock cycle generated 2 RC4 keystream bytes. The architecture was the fastest known for RC4 as of the time. Amdouni et al. [213] developed a robust block cipher hardware architecture that provided high performance to encrypt and decrypt images. It was developed using DNA sequence coding and various chaotic maps. Kumar et al. [214] proposed to improve security in the PRINCE block cipher with an optimized hardware implementation. The proposed architecture in the block cipher not only improved security but also maximized resource efficiency.

6.4 Optimized ciphers

The optimization of ciphers is critical in maintaining safe and efficient communication in the field of data security. Experts have focused their efforts on creating more optimized ciphers. These advancements strive to improve several elements of the design of the cipher, such as area optimization, resource usage, performance enhancement, and vulnerability mitigation. Researchers have made great progress in developing ciphers that give enhanced efficiency while preserving solid security measures by introducing new methods, structures, and techniques. In a recent scholarly work, Manoj et al. [215] proposed an architecture on S box circuit for SMS4 cipher to optimally utilize Field Programmable Gate Array (FPGA). Area optimization was the resultant in the reveal of simulation results. Ashaq et al. [216] presented the use of Substitution Box in the architecture that acquired a hardware design for area efficiency in the PRESENT block cipher to improve resource consumption. Tang et al. [217] proposed WBMatrix, that is a matrix library used to optimize the implementation of White-Box block cipher. The matrix library produces pairwise invertible matrices along with reducing multiplication steps. Kim et al. [218] optimized the S-Layer's performance with the help of masking technique and scheduling of registers in PIPO Block cipher on RISC-V Processors and 32-bit ARM to achieve significant

improvement in performance. Chen et al. [111] highlighted the issue of slow diffusion for the first plaintext when all keys are 0 and proposed SAND-2, a new architecture that provided high-diffusion to address the issue.

6.5 Ciphers for resource constrained devices

As IoT expands, resource-constrained devices play an increasingly important role in providing secure connection. However, due to these devices' limited processing power, memory capacity, and communication resources, creating safe cryptographic methods poses unique challenges. This section highlights the recent advancements in ciphers that are especially designed to handle the restrictions of resource-constrained devices. A variety of solutions have evolved, ranging from decreasing computing complexity using Fast Hartley Transform (FHT)-based approaches to establishing lightweight authentication systems and quantum-resistant encryption. In one of the recent academic works, Nakhate et al. [219] proposed the reduction of complexity during scalar multiplication with the help of Fast Hartley Transform (FHT) based on Elliptic Curve Cryptography. They et al. [220] developed a prototype of Cryptography Process Offloading Proxy (CPOP) and justified feasibility of the prototype with its results to provide security services for resource constrained IoT devices.

Li et al. [221] proposed to combine certificateless cryptography (CLC) and ECC to result a lightweight authentication scheme that offers a secure session key for resource constrained devices in IoT. The scheme offers low communication and computation costs with mutual authentication. Ding et al. [222] proposed a signcryption and elliptic curve based anonymous authentication protocol that provides adequate security strength along with reduction in computational and communication cost for devices in IoT. The reduction of computation and communication costs in the protocol results into a suitable protocol for resource constrained devices. Farha et al. [223] proposed an authentication scheme based on SRAM-PUF which guarantees the authenticity of end devices and offers small capacity of memory and low computational overhead for resource constrained devices in IoT. Xu et al. [224] introduced Ring-ExpLWE, an encryption scheme that is quantum-resistant and provides high performance and reduces lightweight hardware implementation for resource constrained IoT devices. Shahbazi et al. [225] presented an implementation of AES based on FGPA called Nano-AES for resource constrained IoT devices that results efficiency in area and still provides high security. Periasamy et al. [226] presented the utilization of an 8-bit manipulation principle (E3LCM) in a lightweight cryptography method to provide improved energy efficiency for resource constrained devices in IoT.

6.6 Ciphers developed for IoT network and nodes

It has become more critical to ensure the information within IoT networks and nodes of the IoT networks due to the fast expansion of IoT. This subsection discusses cipher developed particularly for IoT networks and nodes such as SLIM, Shadow, modified MD5 and HSA5/1. Such advancements enhance the performance, efficiency, and security within the IoT environmental challenges. Healthcare-focused and secured data collection systems have been discussed in this subsection that address the data privacy and integrity concerns. Such solutions being developed highlight the current efforts to develop ciphers that secure the confidentiality and integrity of data in the IoT networks and nodes. In a recent scholarly work, Asare et al. [227] proposed the combination of MD5 and Feistel cipher for a cryptographic scheme to provide higher security for data in the IoT node. Chatterjee et al. [228] presented a modified version of PRESENT cipher that modified the technique to update Key Register and included a new layer in between the P-layer and Substitution-box with reduction of encryption round.

Muzaffar et al. [229] proposed to combine HSA5/1 symmetric block cipher with high-speed and an Edge-Coded Signaling (ECS) protocol to generate a secured transceiver design for a multilayer, lightweight, and high-speed cipher implemented in IoT communication for Single-channel. Tao et al. [230] presented SecureData, which is a secured data collection healthcare system for IoT with primary goal to resolve issues related to data collusion, data breach, and data integrity in IoT nodes of Healthcare. Guo et al. [112] presented a lightweight block cipher called Shadow for IoT nodes to enhance the speed of diffusion in ARX ciphers that operate on ARX operations and are implemented with generalized Feistel structures. Aboushosha et al. [231] presented a lightweight block cipher called SLIM which is highly immune against most cryptanalysis attacks and provides high performance along with attributes such as area efficiency, and energy-sufficiency.

6.7 Enhancement in quantum stream ciphers

This section discusses the improvements in quantum stream ciphers, concentrating on strategies for improving performance and security. Researchers have developed novel approaches for improving encryption and decryption operations, allowing for higher phase levels and optimized modulation algorithms. Variants of current quantum stream cyphers, such as Y-00 and PSK quantum noise randomized cypher (QNRC), that provide increased performance and effective deciphering capabilities, are among these innovations. In addition, to construct extremely safe optical communication systems, the combination of intensity modulation signals, quadrature amplitude modulation

(QAM), and quantum key distribution (QKD) technologies has been researched. In one of the recent academic works,

Tanizawa et al. [232] proposed a variant for the Y-00 quantum stream cipher that implements a coarse-to-fine modulations which enables 2^{17} phase levels during encryption. Li et al. [233] presented a PSK quantum noise randomized cipher (QNRC) that implemented a new method for decryption which has the capability of providing great performance in successfully deciphering the QNRC signal. Futami et al. [234] presented the intensity modulation signals and operation principle in data encryption and decryption for the Y-00 quantum noise randomized stream cipher. The analytical solution of implementing a transmission system of 1000 km results in the deduction of high-secrecy for the whole transmission system. Lei et al. [235] presented a quantum noise stream cipher (QNSC) with 16 quadrate amplitude modulation (QAM) to provide an improved coherent transmission without intermediate amplifiers over 300 km fiber. Nakazawa et al. [236] proposed a combination of the technology with quantum key distribution (QKD) and the technology with QNSC or QAM for an optical communication system that is highly secured. Yang et al. [237] proposed to combine the attributes of Discrete-Fourier-transform spread orthogonal frequency division multiplexing (DFTs-OFDM) into the Quantum Noise Stream Cipher to achieve better performance in security and improved transmission.

6.8 Extended version of ciphers

Cryptographic advancements are always striving to improve the security and performance of current ciphers. This section focuses on the extended versions of prior ciphers, which were created to overcome shortcomings and improve different features of these cryptographic methods. Researchers have improved well-known cyphers like RECTANGLE, Type-1 Generalized Feistel Networks (GFNs), and Light-Weight Syncryption Protocol (LiSP) through proposed modifications that try to solve obstacles and increase their efficacy. In one of the latest works, Zakaria et al. [238] proposed an extension of the RECTANGLE algorithm to improve the diffusion and confusion attributes and overall enhance the security within the existing RECTANGLE algorithm using 3D cipher. Cheng et al. [22] proposed an extended version of the Type-1 Generalized Feistel Networks (Type-1 GFNs) called extended Type-1 Generalized Feistel Networks (Type-1 EGFNs) and implemented Type-1 EGFNS into a lightweight block cipher to provide improved performance and security. Kim et al. [239] designed an extended version of Light-Weight Syncryption Protocol (LiSP), called LiSP-XK. The extended version focused on the issues found previously in LiSP regarding resource constrained environments. LiSP-XK was designed and customized to become more suitable for resource constrained environments in IIoT. Table 11 presents the summary of various cryptographic advances discussed in the above subsections.

7 Future research directions

Various concerns requiring active research attention related to the hardware implementation, integration, security, privacy, and resilience of lightweight cryptographic methods in the IoT environment are discussed in the subsections below.

7.1 Hardware implementation for LWC methods

For IoT devices, energy consumption is a critical constraint and since hardware-based cryptography solutions are not be optimized for energy consumption, it becomes very difficult to implement such solutions. New methods including low-power designs, and energy efficient ciphers are a viable solution to the massive energy consumption problem. Such hardware designs should be optimized for resource-constrained devices in IoT. However, the methods should reduce power consumption as well as ensuring sufficient security levels, otherwise it becomes easier for intruders to execute malicious attacks on these devices.

7.2 Integration of LWC methods in IoT systems

Various challenges related to efficiency, security, and key management occur in the integration and interoperability of lightweight block ciphers, lightweight stream ciphers, Elliptic Curve Cryptographic methods, and hash functions. Seamless integration and synergies among different lightweight cryptographic methods can solve such challenges and provide efficient key management and effective security. Developing key management schemes, optimized protocols capitalize on the power of each method as well as fulfilling the IoT network's specific requirements can offer effective interoperability solutions.

7.3 Improvement in LWBC

Developing basic key schedules, reducing the size of the block, key size reduction without security compromise, and simpler rounds are different improvements in lightweight block ciphers. Reducing the size of the block can offer optimization in the encryption and decryption for resource constrained IoT devices. Basic key schedules can reduce the overhead and enhance the efficiency for IoT environments with resource constraints. A reduced key size will accommodate the IoT device's limited storage and computation capabilities. Simpler rounds reduce computational power needed

Table 11 Major advancements in cryptographic algorithms

References	Major contribution	Cipher/scheme	Results	Limitations
Panchami et al. [200]	Feather S-Box of 4-bit that enabled confusion in lightweight ciphers	Feather S-Box	A 23 and 19% improvement in terms of less Area Delay-Product and Power-Delay Product compared to PRESENT cipher	SKINNY cipher provides higher immunity linear and differential cryptanalysis
Devi et al. [202]	Approach for malware detection and prevention using deep learning to provide security for transmission of data	N/A	Found precision of 92%, accuracy of 95% and error value of 5%	N/A
Kumar et al. [214]	Improvement in PRINCE block cipher's security with an optimized hardware implementation	PRINCE	13.057% performance improvement, and 8.109% efficiency improvement in Virtex-6-FF784 implementation, and a 113% performance and 113.734% efficiency improvement in Virtex-4-FF668 FGPA	The proposed architecture evaluates only gray-scale images, which is not a representation of all IoT devices applications
Chen et al. [111]	SAND-2, a new architecture that provided high-diffusion to address the issue 0 in the previous version, SAND	SAND-2	The throughput achieved in SAND-2 is 10% higher, and full diffusion speed is 63.7% higher in comparison to SAND	N/A
Li et al. [221]	Combined certificateless cryptography (CLC) and ECC to result a lightweight authentication scheme that offers a secure session key for resource constrained devices	CLC & ECC	The effectiveness of the authentication scheme along with the feasibility of it is confirmed via the results	System's security is not scalable due to higher computational costs of real-time key update strategy compared to existing fixed cycle key update strategies
Liu et al. [198]	uBlock, a lightweight cipher algorithm for devices in IoT that improved the performance of encryption and decryption	uBlock	Throughput can achieve 1 Gb/s level with technology of 90 nm for encryption and decryption	Increase in FPGA resources
Xu et al. [210]	Pipelined design scheme in ZUC-256 to implement a high-throughput hardware	ZUC-256	FPGA implementation is increased by 1.06 times, while the area efficiency of ASIC implementation is increased by 1.61 time	Requires a significant amount of resource for hardware implementation
Amdouni et al. [213]	A robust block cipher hardware architecture that provided high performance to encrypt and decrypt images	N/A	Achieves a high-performance throughput of 24,576,153 Mbps	N/A
Ashaq et al. [216]	Substitution Box in the architecture that acquired a hardware design for area efficiency in the PRESENT block cipher	PRESENT	An improvement of 13.67% is obtained in resource consumption	N/A
Tang et al. [217]	WBMatrix, that is a matrix library used to optimize the implementation of White-Box block cipher	White-Box	Improvement in the construction of table and faster encryption	The encryption and table construction phases are improved only on ARMv8 and Intel × 86 platforms
Kim et al. [218]	Optimized the S-Layer's performance with the help of masking technique and scheduling of registers in PIPO Block cipher on RISC-V Processors and 32-bit ARM	PIPO	When 4 different plaintext was encrypted, the performance was improved by 370% and 229% in ARM Cortex-M4 and RISC-V platforms, respectively	Performance can be improved with the implementation of on-the-fly key scheduling technique
Ding et al. [222]	A signcryption and elliptic curve based anonymous authentication protocol that provides adequate security strength	N/A	Effective reduction in the requirement of resources is verified in the protocol via results	N/A

Table 11 (continued)

References	Major contribution	Cipher/scheme	Results	Limitations
Xu et al. [224]	Ring-ExpLWE, an encryption scheme that is quantum-resistant and provides high performance and reduces lightweight hardware implementation	Ring-ExpLWE	35.6 ms is required for encryption and 17.8 ms is required for decryption with implemented software based on Cortex-M3 microprocessor	The Area×Time (AT) of our high-performance and lightweight hardware implementations is reduced by 49.2% and 49.5%, respectively,
Cheng et al. [22]	Extended version of the Type-1 GFNs called extended Type-1 EGFNs and implemented Type-1 EGFNS into a lightweight block cipher	Type-1 EGFNs	The cipher outperforms other existing lightweight ciphers in terms of processing speed, resource utilization, and power consumption	N/A
Kundu et al. [199]	User independent multivariate group signature scheme that focused on providing anonymity of the user, no connection between users, and traceability	Multivariate group signature scheme	N/A	N/A
Thabit et al. [201]	New lightweight cryptographic algorithm that is lightweight in nature to provide security for cloud computing applications	NLCA	Improvement in terms of execution time of the cipher and security forces in comparison to widely used cryptographic systems	Provides faster processing time at the cost of a smaller key size of 128-bit compared to 256-bit key size of DES algorithm
Potestad-Ordóñez et al. [205]	Presented various fault detection schemes to protect trivium stream cipher from fault injection attacks	N/A	Counter measures provide 79% higher fault coverage and 99.9% is reached from one of the counter measures	There is approximately 33% area overhead in the trivium stream cipher countermeasure
Song et al. [206]	A new variant of PIPO block cipher for a secure communication that is fast with optimized techniques	PIPO	301% improvement in performance is seen compared to HIGHT, and 463% compared to revise CHAM	N/A
Farha et al. [223]	An authentication scheme based on SRAM-PUF which guarantees the authenticity of end devices and offers small capacity of memory	SRAM-PUF	Effective authentication with a low memory capacity and computational overhead is obtained via results	Difficult to ensure consistent performance since the algorithm cannot predict which SRAM cells are more likely to become unstable under different conditions
Periasamy et al. [226]	Utilized an 8-bit manipulation principle (E3LCM) in a lightweight cryptography method	E3LCM	Results provide the proposed method consumes only 0.9 Kbytes of RAM and 202mW of power	N/A
Muzaffar et al. [229]	Combined HSA5/1 symmetric block cipher with high-speed and an Edge-Coded Signaling (ECS) protocol	HSA5/1	Only clock cycle is required for encryption and decryption of 148-bit key at 25 MHz of clock frequency that consumes power of 27 μW	The generation of all keystreams must occur within a single clock cycle, as using more than one cycle would result in a lower data rate transmission
Guo et al. [112]	A lightweight block cipher called Shadow for IoT nodes to enhance the speed of diffusion in ARX ciphers	Shadow	N/A	Round based architecture is implemented to prioritize higher throughput over lower resource consumption
Li et al. [233]	A PSK quantum noise randomized cipher (QNRC) that implemented a new method for decryption	QNRC	The QNRC signal is successfully deciphered with the proposed decryption technique that provides improved performance	The method is only tested under a 50 km transmission system which is relatively small length
Lei et al. [235]	A quantum noise stream cipher (QNSC) with 16 quadrate amplitude modulation (QAM	QNSC	The system has the capacity to transmit data at a rate of 10.2 Tbit/s·km	Results only show the performance of the QNSC with a single polarization and single wavelength

Table 11 (continued)

References	Major contribution	Cipher/scheme	Results	Limitations
Kim et al. [239]	Extended version of LiSP, called LiSP-XK which focused on the issues found previously in LiSP regarding resource constrained environments	LiSP-XK	Compared to other signcryption methods, LiSP-XK demonstrates an overall efficiency improvement of 35%	The authentication scheme is not particularly preferred for extreme security due to its lesser complexity
Chatterjee et al. [179]	PRESENT cipher with modified technique to update Key Register and included a new layer in between the P-layer and Substitution-box	PRESENT	The number of rounds is reduced from 31 to 25 for the encryption process in the PRESENT cipher	Number of rounds are reduced; therefore, security is compromised for greater efficiency
Roy et al. [204]	SAFARI, a framework that outputs a C code which is fault attack protected for block ciphers	SAFARI	N/A	Safari is not compatible with ciphers such as Blowfish and Twofish
Nakhate et al. [219]	Reduced complexity during scalar multiplication with the help of Fast Hartley Transform (FHT)	N/A	Improvement of 4%-8% in encryption and decryption time has been observed using FHT in ECC over FFT based ECC	Proposed work doesn't provide precision of calculation due to the lack of a multiprecision library
Shahbazi et al. [225]	Implementation of AES based on FGPA called Nano-AES for resource constrained IoT devices	AES	Compared to previous works similar to this, there is an improvement from 35 to 2.4% using application specified integrated circuit (ASIC)	The proposed design is not suitable for IoT devices that are particularly large in size and acquire significant resource consumption
Asare et al. [227]	Combined MD5 and Feistel cipher for a cryptographic scheme to provide higher security	MD5	Fast and improved encryption of data between the sink mode and IoT edge devices is obtained through the results	Since MD5 is considered a weak hashing algorithm and Feistel cipher implements symmetric cryptography the security can be improved with stronger algorithms
Aboushosha et al. [231]	A lightweight block cipher called SLIM which is highly immune against most cryptanalysis attacks and provides high performance	SLIM	The results display high immunity towards strong differential and linear cryptanalysis attacks	Implementation of symmetric cryptography, and Feistel network structure is not suitable for devices which require extreme security
Futami et al. [234]	Presented the intensity modulation signals and operation principle in data encryption and decryption for the Y-00 quantum noise randomized stream cipher	QNRSC	Demonstrates 1,000-km transmission system secrecy experimentally, using the analytical solution to achieve a 1.5-Gb/s data rate	Cipher relies heavily on the physical layer characteristics, therefore if physical layer is compromised, it will reuslt in failure of entire system
Zakaria et al. [238]	Extension of the RECTANGLE algorithm to improve the diffusion and confusion attributes and overall enhance the security	RECTANGLE	Algorithm achieves a competitive performance, with an execution speed of 0.9516 ms and a throughput of 67.26 bit/ms, compared to existing algorithms	N/A
Liu et al. [208]	Countermeasure towards fault attacks based on a method that quantitively analyzes the protection of SPN structure block ciphers	N/A	Within 10 microseconds, 2000 fault injections are enough to finish the assessment under the analyzed fault models	The quantitively evaluation method is not extendable or compatible with ciphers that implement symmetric Feistel network
Tao et al. [230]	SecureData, which is a secured data collection healthcare system for IoT with primary goal to resolve data security issues	SecureData	When SecureData is applied in IoT-based healthcare, the results display efficient security from various risks	N/A

Table 11 (continued)

References	Major contribution	Cipher/scheme	Results	Limitations
Yang et al. [237]	Combined the attributes of DFTs-OFDM into the Quantum Noise Stream Cipher to achieve faster transmission	QNSC	Results demonstrate transmission of PSK/QNSC and QAM/QNSC signals based on DFTs-OFDM at a rate of 10-Gbit/s over a 200-km fiber link span	The cipher has not been put under other potential sources of noise that could affect the system's performance
Pandey et al. [211]	An architecture for PRESENT cipher based on 8-bit datapath to process key of 128-bits and plaintext of 64-bits that included 48 clock cycles	PRESENT	The fluctuating usage of power is 36.57 mW, the amount of energy usage is 57.95 nJ, and the energy/bit is 0.91 nJ/bit	Xilinx Virtex-5 FPGA and SCL 180 nm technology is outdated in today's date, therefore, optimization is not as sufficient for all technologies
Manoj et al. [215]	An architecture on S box circuit for SMS4 cipher to optimally utilize Field Programmable Gate Array (FPGA)	SMS4	N/A	N/A
Tanizawa et al. [232]	Variant for the Y-00 quantum stream cipher that implements a coarse-to-fine modulations	Y-00 QNSC	2^{17} phase levels are enabled with the help of coarse-to-fine modulations	N/A
Cnudde et al. [207]	New implementation of the block cipher, PRESENT, that provides security against not only fault attacks	PRESENT	N/A	A magnitude of 8.75 rise in area is needed when transitioning from a first-order SCA resistant TI to a first-order SCA resistant PC-II implementation
Wang et al. [209]	Used existing Benes network to resist fault attacks in crypto-processors	N/A	Enhances fault resistance by more than four orders of magnitude above the exposed instance	The network module is ineffective in the FPGA case compared to direct cross wires case since only one algorithm is employed
Nakazawa et al. [236]	Combined the technology with quantum key distribution (QKD) and the technology with QNSC or QAM	QKD and QNSC	An elevated spectral efficiency of 10.3 bits/s/Hz was achieved by executing a single-channel transmission of 70-Gbit/s, utilizing 128 QAM over a distance of 100 km	N/A
Dofe et al. [203]	Integrated different masking methods and operand permutation techniques in a new microarchitecture to prevent fault attacks in SIMON cipher	SIMON	Outperforms the existing fault-detection methods in multiple fault attack conditions	Requires 5% more overhead than most hardware-efficient fault detection methods
Gupta et al. [212]	An architecture for RC4 Stream cipher that combined loop unrolling and hardware pipeline	RC4	The rate of data transfer is 10, 21.92, and 30.72 Gbps	Performance cannot be improved further due to heavy increase in area

for the execution of encryption and decryption operations in the resource constrained IoT devices.

7.4 Improvement in LWSC

Improvements in stream ciphers can be observed by reducing key length, reducing chip area, offering minimal internal state, and reducing the setup cycles of the key. A smaller key length can conserve computational and memory resources; however, reduction should be only to an extent to make sure the stream cipher provides acceptable level of security. On the other hand, a smaller chip area offers better utilization of hardware resources, which is effective for resource-constrained IoT devices. Minimal internal state and fewer number of setup cycles will minimize computational overhead, and optimize performance.

7.5 Improvement in hash functions

Various hash functions can be improved if developers reduce the message size, and/or reduce the message digest/output size. Those are primarily the two parameters that determine the security and overall efficiency of hash functions. A smaller message size will reduce the network overhead, enhance the efficiency of computations, and optimize the memory usage. Whereas due to the smaller hash digest, a smaller output size will offer faster computations, however the extent to reduction should be kept in mind since smaller message digest has higher chances of collision that can lead to compromise of integrity.

7.6 Improvement in ECC

Improvement in the execution speed of ECC operations, and reduction in energy consumption and memory requirement can offer improvements in the various implementations of ECC. More specifically, improvement in the execution speed facilitates quicker cryptographic computations resulting in real-time communications and efficiently processing of data. By reducing both the energy consumption and the memory requirements, it becomes more feasible to implement ECC in resource constrained IoT devices and help improve the battery life of IoT devices.

8 Conclusion

IoT has become a critical component in today's interconnected world, enhancing the quality of life for individuals. However, despite undergoing significant evolution, a persistent issue remains in the form of a dearth of security mechanisms that effectively leverage limited resources while providing sufficiently robust protection to IoT systems. Security, confidentiality, and privacy are vital concerns within IoT systems due to the sensitivity of the data involved. Traditional cryptographic approaches are helpful in addressing these concerns, ensuring the protection and integrity of IoT systems. However, the resource limitations of most IoT devices, including computational power, battery life, size, and memory, pose challenges to the traditional approaches. To resolve these challenges, lightweight cryptography offers methods designed to accommodate these constraints, providing effective security solutions for resource-constrained IoT devices. This work presents lightweight block ciphers, lightweight stream ciphers, hash functions, and ECC as cryptographic methods suitable for securing IoT systems. The study has also examined various attacks that pose threats to IoT security and explored different ciphers or implementations for each method. Furthermore, the role of LWC in different sectors of IoT has been explored, as well as highlighting recent advancements in different areas. Future research directions are focused primarily on the improvements in each method of LWC along with the implementation and integration of the methods. This preliminary study aims to lay the groundwork for future research endeavors in the field of lightweight cryptography methods specifically tailored for IoT systems.

References

1. Fei, H. (2016). *Security and privacy in internet of things (IoTs): Models, algorithms, and implementations*. CRC Press. ISBN 9781498723183.
2. Fan, K., Luo, Q., Zhang, K., & Yang, Y. (2020). Cloud-based lightweight secure RFID mutual authentication protocol in IoT. *Information Sciences, 527*, 329–340. https://doi.org/10.1016/j.ins.2019.08.006
3. Chi, T., & Chen, M. (2017). A frequency hopping method for spatial RFID/WiFi/Bluetooth scheduling in agricultural IoT. *Wireless Networks, 25*(2), 805–817. https://doi.org/10.1007/s11276-017-1593-z
4. Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., & Alkhzaimi, H. A. (2023). Cryptography algorithms for enhancing IoT security. *Internet of Things, 22*, 100759. https://doi.org/10.1016/j.iot.2023.100759. ISSN 2542-6605.
5. Chellappan, V., & Sivalingam, K. M. (2016). Chapter 10—Security and privacy in the Internet of Things. In R. Buyya & A. V. Dastjerdi (Eds.), *Internet of things* (pp. 183–200). Morgan Kaufmann. ISBN 9780128053959. https://doi.org/10.1016/B978-0-12-805395-9.00010-1
6. Hameed, A., & Alomary, A. (2019). Security issues in IoT: A survey. In *2019 International conference on innovation and intelligence for informatics, computing, and technologies (3ICT)*. IEEE. https://doi.org/10.1109/3ICT.2019.8910320
7. Noor, M. B. M., & Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer Networks, 148*, 283–294. https://doi.org/10.1016/j.comnet.2018.11.025,Elsevier
8. Chew, K. M., Tan, S. C. W., Loh, G. C. W., Bundan, N., & Yiiong, S. P. (2020). IoT soil moisture monitoring and irrigation system development. In *ICSCA 2020: Proceedings of the 2020*

9th international conference on software and computer applications (pp. 247–252). ACM Digital Library.
9. Zeadallya, S., Das, A. K., & Sklavos, N. (2019). Cryptographic technologies and protocol standards for Internet of Things. *Internet Things*. https://doi.org/10.1016/j.iot.2019.100075,Elsevier
10. Philip, M. A., & Vaithiyanathan. (2017). A survey on lightweight ciphers for IoT devices. In *Presented at the international conference on technological advancements in power and energy (TAP energy)*.
11. Ahmed, S. F., Islam, M. R., Nath, T. D., Ferdosi, B. J., & Hasan, A. T. (2020). G-TBSA: A generalized lightweight security algorithm for IoT. In *2019 4th international conference on electrical information and communication technology (EICT)*. IEEE. https://doi.org/10.1109/EICT48899.2019.9068848
12. Lepekhin, A., Borremans, A., Ilin, I., & Jantunen, S. (2019). A systematic mapping study on internet of things challenges. In *IEEE/ACM 1st international workshop on software engineering research and practices for the internet of things (SERP4IoT)*. IEEE Digital Library. https://doi.org/10.1109/SERP4IoT.2019.00009
13. Yugha, R., & Chithra, S. (2020). A survey on technologies and security protocols: Reference for future generation IoT. *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2020.102763
14. Rao, V., & Prema, K.V. (2019). Comparative study of lightweight hashing functions for resource constrained devices of IoT. In *4th international conference on computational systems and information technology for sustainable solution (CSITSS)*. IEEE. https://doi.org/10.1109/CSITSS47250.2019.9031038
15. Jiang, X., Lora, M., & Chattopadhyay, S. (2020). An experimental analysis of securityvulnerabilities in industrial IoT devices. *ACM Transactions on Internet Technology*. https://doi.org/10.1145/3379542,ACMDigitalLibrary
16. Alabaa, F. A., Othmana, M., Hashema, I. A. T., & Alotaibi, F. (2017). Internet of Thingssecurity: A survey. *Journal of Network and Computer Applications, 88*, 10–28. https://doi.org/10.1016/j.jnca.2017.04.002,Elsevier
17. Jawhar, S., Miller, J., & Bitar, Z. (2024). AI-based cybersecurity policies and procedures. In *2024 IEEE 3rd international conference on AI in cybersecurity (ICAIC), Houston* (pp. 1–5). https://doi.org/10.1109/ICAIC60265.2024.10433845
18. Rajhi, M. (2021). Security procedures for user-centric ultra-dense 5G networks. In *2021 IEEE international IOT, electronics and mechatronics conference (IEMTRONICS), Toronto* (pp. 1–5). https://doi.org/10.1109/IEMTRONICS52119.2021.9422599
19. Tsantikidou, K., & Sklavos, N. (2022). Hardware limitations of lightweight cryptographic designs for IoT in healthcare. *Cryptography, 6*(3), 45. https://doi.org/10.3390/cryptography6030045
20. Fotovvat, A., Rahman, G. M. E., Vedaei, S. S., & Wahid, K. A. (2021). Comparative performance analysis of lightweight cryptography algorithms for IoT sensor nodes. *IEEE Internet of Things Journal, 8*(10), 8279–8290. https://doi.org/10.1109/JIOT.2020.3044526
21. Singh, S., Sharma, P. K., Moon, S. Y., et al. (2017). Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-017-0494-4
22. Cheng, J., Guo, S., & He, J. (2022). An extended type-1 generalized feistel networks: Lightweight block cipher for IoT. *IEEE Internet of Things Journal, 9*(13), 11408–11421. https://doi.org/10.1109/JIOT.2021.3126317
23. Bokhari, M. U., & Afzal, S. (2023). Performance of software and hardware oriented lightweight stream cipher in constraint environment: A review. In *2023 10th international conference on computing for sustainable global development (INDIACom)*, New Delhi (pp. 1667–1672).
24. Khan, S., Lee, W.-K., Karmakar, A., Mera, J. M. B., Majeed, A., & Hwang, S. O. (2023). Area–time efficient implementation of nist lightweight hash functions targeting IoT applications. *IEEE Internet of Things Journal, 10*(9), 8083–8095. https://doi.org/10.1109/JIOT.2022.3229516
25. Yeh, L.-Y., Chen, P.-J., Pai, C.-C., & Liu, T.-T. (2020). an energy-efficient dual-field elliptic curve cryptography processor for internet of things applications. *IEEE Transactions on Circuits and Systems II: Express Briefs, 67*(9), 1614–1618. https://doi.org/10.1109/TCSII.2020.3012448
26. Ahmed, S. F., et al. (2024). Toward a secure 5G-enabled internet of things: A survey on requirements, privacy, security, challenges, and opportunities. *IEEE Access, 12*, 13125–13145. https://doi.org/10.1109/ACCESS.2024.3352508
27. Tong, F., Chen, C., & Pan, J. (2024). A novel detection and localization scheme for wormhole attack in internet of things. *IEEE Internet of Things Journal, 11*(4), 7141–7152. https://doi.org/10.1109/JIOT.2023.3315757
28. Kramp, T., van Kranenburg, R., & Lange, S. (2013). Introduction to the internet of things. In *Enabling things to talk*. Springer. https://doi.org/10.1007/978-3-642-40403-0_1
29. Teicher, J. (2023). The little-known story of the first IOT device. *IBM Blog*. Retrieved June 12, 2023, from https://www.ibm.com/blog/little-known-story-first-iot-device/
30. Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: A review. *J Big Data, 6*, 111. https://doi.org/10.1186/s40537-019-0268-2
31. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal, 4*(5), 1250–1258. https://doi.org/10.1109/JIOT.2017.2694844,IEEE
32. Syed, A. S., Sierra-Sosa, D., Kumar, A., & Elmaghraby, A. (2021). IoT in smart cities: a survey of technologies, practices and challenges. *Smart Cities, 4*(2), 429–475. https://doi.org/10.3390/smartcities4020024
33. Yadav, A., & Prasad, L. B. (2019) IOT devices for control applications: A review. In *2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India* (pp. 473–479). https://doi.org/10.1109/ICECA.2019.8821895
34. Varadharajan, V., Tupakula, U., & Karmakar, K. (2018). Study of security attacks against IoT infrastructures. Technical Report TR1: ISIF ASIA FundedProject.
35. Fetahu, L., Maraj, A., & Havolli, A. (2022). Internet of things (IoT) benefits, future perspective, and implementation challenges. In *2022 45th Jubilee international convention on information, communication and electronic technology (MIPRO), Opatija, Croatia* (pp. 399–404). https://doi.org/10.23919/MIPRO55190.2022.9803487
36. Cruz-Piris, L., Rivera, D., Marsa-Maestre, I., & Velasco, J. (2018). Access control mechanism for IoT environments based on modelling communication procedures as resources. *Sensors, 18*(3), 917. https://doi.org/10.3390/s18030917
37. Buil-Gil, D., Kemp, S., Kuenzel, S., Coventry, L., Zakhary, S., Tilley, D., & Nicholson, J. (2023). The digital harms of smart home devices: A systematic literature review. *Computers in Human Behavior, 145*, 107770. https://doi.org/10.1016/j.chb.2023.107770. ISSN 0747-5632.
38. Abdalla, P. A., & Varol, A. (2019). Advantages to disadvantages of cloud computing for small-sized business. In *2019 7th international symposium on digital forensics and security (ISDFS), Barcelos* (pp. 1–6). https://doi.org/10.1109/ISDFS.2019.8757549

39. Ghosh, R. K. (2017). Low power communication protocols: ZigBee, 6LoWPAN and ZigBee IP. In *Wireless networking and mobile data management*. Springer. https://doi.org/10.1007/978-981-10-3941-6_6
40. Sharma, R., Pandey, N., & Khatri, S. K. (2017). Analysis of IoT security at network layer. In *2017 6th international conference on reliability, infocom technologies and optimization (trends and future directions) (ICRITO), Noida* (pp. 585–590). https://doi.org/10.1109/ICRITO.2017.8342495
41. Ansar, S. A., Arya, S., Aggrawal, S., Saxena, S., Kushwaha, A., & Pathak, P. C. (2023). Security in IoT layers: Emerging challenges with countermeasures. In P. K. Shukla, K. P. Singh, A. K. Tripathi, & A. Engelbrecht (Eds.), *Computer vision and robotics. Algorithms for intelligent systems.* Springer. https://doi.org/10.1007/978-981-19-7892-0_44
42. Atlam, H., Walters, R., & Wills, G. (2018). Fog computing and the internet of things: A review. *Big Data and Cognitive Computing, 2*(2), 10. https://doi.org/10.3390/bdcc2020010
43. Lombardi, M., Pascale, F., & Santaniello, D. (2021). Internet of things: A general overview between architectures, protocols and applications. *Information, 12*(2), 87. https://doi.org/10.3390/info12020087
44. Hamdan, S., Ayyash, M., & Almajali, S. (2020). Edge-computing architectures for internet of things applications: A survey. *Sensors, 20*(22), 6441. https://doi.org/10.3390/s20226441
45. Adat, V., & Gupta, B. B. (2018). Security in internet of things: Issues, challenges, taxonomy, and architecture. *Telecommunication Systems, 67*(3), 423–441. https://doi.org/10.1007/s11235-017-0345-9
46. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security andprivacy issues in internet-of-things. *IEEE Internet of Things Journal, 4*(5), 1250–1258. https://doi.org/10.1109/JIOT.2017.2694844,IEEE
47. Prakash, V., Singh, A. V., & Khatri, S. K. (2019). A new model of light weight hybrid cryptography for internet of things. In *2019 3rd international conference on electronics, communication and aerospace technology (ICECA)*. IEEE. https://doi.org/10.1109/ICECA.2019.8821924
48. Manifavas, C., Hatzivasilis, G., Fysarakis, K., & Papaefstathiou, Y. (2015). A survey of lightweight stream ciphers for embedded systems. *Security Communications and Network, 9*, 1226–1246. https://doi.org/10.1002/sec.1399
49. Joachim, W. W. (2022). Internet-of-things architecture IoT a project deliverable D1.2-initial architectural reference model for IoT. Retrieved July 26, 2022, from https://cocoa.ethz.ch/downloads/2014/01/1360_D1%202_Initial_architectural_reference_model_for_IoT.pdf
50. Bauer, M. et al. (2013). IoT reference model. In *Enabling things to talk*. Springer. https://doi.org/10.1007/978-3-642-40403-0_7
51. Alghofaili, Y., & Rassam, M. A. (2022). A trust management model for IoT devices and services based on the multi-criteria decision-making approach and deep long short-term memory technique. *Sensors (Basel), 22*(2), 634. https://doi.org/10.3390/s22020634.PMID:35062594;PMCID:PMC8777818
52. Haller, S., Serbanati, A., Bauer, M., & Carrez, F. (2013). A domain model for the internet of things. In *Proc. IEEE int. conf. green comput. commun. IEEE internet things IEEE cyber, phys. social comput., Beijing* (pp. 411–417). https://doi.org/10.1109/GreenCom-iThings-CPSCom.2013.87
53. Mao, Y.-Q., & Shen, S.-B. (2014). Information model and capability analysis of the internet of things. *Ruan Jian Xue Bao/Journal of Software, 25*, 1685–1695. https://doi.org/10.13328/j.cnki.jos.004664
54. Soubra, H., &Abran, A. (2017). Functional size measurement for the internet of things (IoT): An example using COSMIC and the Arduino open-source platform. https://doi.org/10.1145/3143434.3143452
55. Kulkarni, S., & Kulkarni, S. (2017). Communication models in internet of things: A survey. *IJSTE—International Journal of Science Technology & Engineering, 3*(11), 87–91.
56. (2014). The internet of things reference model [Online]. http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf
57. Moganedi, S., &Mtsweni, J. (2017). Beyond the convenience of the internet of things: Security and privacy concerns. https://doi.org/10.23919/ISTAFRICA.2017.8102372
58. Gupta, K. (2022). Machine learning-based device type classification for IoT device re- and continuous authentication. https://digitalcommons.unl.edu/computerscidiss/221/ (Accessed 03 Mar 2023)
59. Jain, V. K., Mazumdar, A. P., Faruki, P., & Govil, M. C. (2022). Congestion control in Internet of Things: Classification, challenges, and future directions. *Sustainable Computing: Informatics and Systems, 35*, 100678. https://doi.org/10.1016/j.suscom.2022.100678. ISSN 2210-5379.
60. Ammar, M., Daniels, W., Crispo, B., & Hughes, D. (2018). SPEED: Secure provable erasure for class-1 IoT devices, 111–118. https://doi.org/10.1145/3176258.3176337
61. King, J., & Awad, A. I. (2016). A distributed security mechanism for resource-constrained IoT devices. *Informatica, 40*, 133–143.
62. Anuradha, M. P. & Rani, K. L. F. C. (2022). Chapter Fourteen—Blockchain technology for IoT edge devices and data security. In P. Raj, K. Saini, & C. Surianarayanan (Eds.), *Advances in computers* (Vol. 127, pp 379–412). Elsevier. ISSN 0065-2458, ISBN 9780128245064. https://doi.org/10.1016/bs.adcom.2022.02.011
63. Kurose, J., & Ross, K. (2006). Chapter 8—Layer 7: The application layer. In: M. Gregg (Ed.), *Hack the stack, syngress* (pp. 285–352). ISBN 9781597491099. https://doi.org/10.1016/B978-159749109-9/50012-5
64. Jat, S., & Patel, P. (2017). Wireless sensor networks protocol: A review. *International Journal of Engineering Development and Research (IJEDR)*, *5*(1), 23–26. ISSN:2321-9939. :http://www.ijedr.org/papers/IJEDR1701005.pdf
65. Sharma, C., Jain, S. C., & Sharma, A. K. (2016). Explorative study of SQL injection attacks and mechanisms to secure web application database—A review. *International Journal of Advanced Computer Science and Applications*. https://doi.org/10.14569/IJACSA.2016.070312
66. Fotiou, N., Marias, G. F., & Polyzos, G. C. (2012). Fighting phishing the information-centric way. In *2012 5th international conference on new technologies, mobility and security (NTMS), Istanbul, Turkey* (pp. 1–5). https://doi.org/10.1109/NTMS.2012.6208747
67. Homayoun, S., Dehghantanha, A., Ahmadzadeh, M., Hashemi, S., Khayami, R., Choo, K. K. R., & Newton, D. E. (2019). DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer. *Future Generation Computer Systems, 90*, 94–104. https://doi.org/10.1016/j.future.2018.07.045. ISSN 0167-739X.
68. Bhattasali, T., Chaki, R., & Sanyal, S. (2023). Sleep deprivation attack detection in wireless sensor network. Retrieved June 11, 2023, from https://doi.org/10.48550/arXiv.1203.0231
69. Obaid, H. S., & Abeed, E. H. (2020). DoS and DDoS attacks at OSI layers. 1–9. 10.5281/zenodo.3610833
70. Chordiya, A. R., Majumder, S., & Javaid, A. Y. (2018). Man-in-the-middle (MITM) attack based hijacking of HTTP traffic using open-source tools. In *2018 IEEE international conference on electro/information technology (EIT), Rochester* (pp. 0438–0443). https://doi.org/10.1109/EIT.2018.8500144

71. Ghugar, U., Pradhan, J., Bhoi, S., & Sahoo, R. (2019). LB-IDS: Securing wireless sensor network using protocol layer trust-based intrusion detection system. *Journal of Computer Networks and Communications, 2019*, 1–13. https://doi.org/10.1155/2019/2054298
72. Chen, C., Asoni, D. E., Perrig, A., Barrera, D., Danezis, G., Troncoso, C. (2018). TARANET: Traffic-analysis resistant anonymity at the network layer. In *2018 IEEE European symposium on security and privacy (EuroS&P), London* (pp. 137–152). https://doi.org/10.1109/EuroSP.2018.00018
73. Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019). Perception layer security in internet of things. *Future Generation Computer Systems, 100*, 144–164. https://doi.org/10.1016/j.future.2019.04.038. ISSN 0167-739X.
74. Nguyen, V.-L., Lin, P.-C., & Hwang, R.-H. (2019). Energy depletion attacks in low power wireless networks. *IEEE Access, 7*, 51915–51932. https://doi.org/10.1109/ACCESS.2019.2911424
75. Affia, A. O., Finch, H., Jung, W., Samori, I. A., Potter, L., & Palmer, X.-L. (2023). IoT health devices: Exploring security risks in the connected landscape. *IoT, 4*(2), 150–182. https://doi.org/10.3390/iot4020009
76. Rekha, S., Thirupathi, L., Renikunta, S., & Gangula, R. (2023). Study of security issues and solutions in Internet of Things (IoT). *Materials Today: Proceedings, 80*(3), 3554–3559. https://doi.org/10.1016/j.matpr.2021.07.295. ISSN 2214-7853.
77. Aldowah, H., Rehman, S., & Umar, I. (2019). Security in internet of things: Issues. *Challenges, and Solutions.* https://doi.org/10.1007/978-3-319-99007-1_38
78. Kolias, C., Stavrou, A., & Voas, J. (2015). Securely making "things" right. *Computer, 48*(9), 84–88. https://doi.org/10.1109/MC.2015.258
79. McKay, K., Bassham, L., Turan, M. S., & Mouha, N. (2017). *Report on lightweight cryptography (Nistir8114)*. Gaithersburg: NIST.
80. Information technology, Security techniques, Lightweight cryptography, Part 2; Block ciphers (ISO/IEC 29192-2). Retrieved February 21, 2014, from https://www.iso.org/standard/56552.html
81. Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. A. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. *IEEE Access, 9*, 28177–28193. https://doi.org/10.1109/ACCESS.2021.3052867
82. Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions. *Journal of Ambient Intelligece & Human Computing*. https://doi.org/10.1007/s12652-017-0494-4
83. Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M. (2020). Lightweight elliptic curve cryptography accelerator for internet of things applications. *Ad Hoc Networks, 103*, 102159. https://doi.org/10.1016/j.adhoc.2020.102159. ISSN 1570-8705.
84. Hatzivallis, G., Fysarakis, K., Papaefstathiou, I., & Manifavas, C. (2018). A review of lightweight block ciphers. *Journal of Cryptographic Engineering, 8*, 141–184.
85. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications, 38*, 8–27.
86. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access, 7*, 82721–82743. https://doi.org/10.1109/ACCESS.2019.2924045
87. Hammi, B., Fayad, A., Khatoun, R., Zeadally, S., & Begriche, Y. (2020). A lightweight ECC-based authentication scheme for internet of things (IoT). *IEEE Systems Journal, 14*(3), 3440–3450. https://doi.org/10.1109/JSYST.2020.2970167
88. Singh, P., Acharya, B., & Chaurasiya, R. K. (2021). Chapter 8—Lightweight cryptographic algorithms for resource-constrained IoT devices and sensor networks. In S. K. Sharma, B. Bhushan, & N. C. Debnath (Eds.), *Advances in ubiquitous sensing applications for healthcare, security and privacy issues in IoT devices and sensor networks* (pp. 153–185). Academic Press. https://doi.org/10.1016/B978-0-12-821255-4.00008-0 ISSN 25891014, ISBN 9780128212554.
89. Calmels, B., Canard, S., Girault, M., & Sibert, H. (2006). Low-cost cryptography for privacy in RFID systems. In J. Domingo-Ferrer, J. Posegga, & D. Schreckling (Eds.), *Smart card research and advanced applications CARDIS 2006 lecture notes in computer science.* (Vol. 3928). Springer. https://doi.org/10.1007/11733447_17
90. Sliman, L., Omrani, T., Tari, Z., Samhat, A. E., & Rhouma, R. (2021). Towards an ultra lightweight block ciphers for Internet of Things. *Journal of Information Security and Applications, 61*, 102897. https://doi.org/10.1016/j.jisa.2021.102897. ISSN 2214-2126.
91. Shibuya, Y., Iwai, K., Matsubara, T., & Kurokawa, T. (2022). FPGA implementation of stream cipher SOSEMANUK. In *2022 10th international symposium on computing and networking workshops (CANDARW), Himeji* (pp. 83–89). https://doi.org/10.1109/CANDARW57323.2022.00055
92. Ramya, K. V., Hs, M. R., & Reddy, R. (2023). Implementation and analysis of feistel and SPN structured ciphers—CLEFIA and PRESENT. In *2023 international conference on network, multimedia and information technology (NMITCON), Bengaluru* (pp. 1–6). https://doi.org/10.1109/NMITCON58196.2023.10275899
93. Mohammed, Z. A., & Hussein, K. A. (2023). Lightweight cryptography concepts and algorithms: A survey. In *2023 2nd international conference on advanced computer applications (ACA), Misan* (pp. 1–7). https://doi.org/10.1109/ACA57612.2023.10346914
94. Maitra, S., Sinha, N., Siddhanti, A., Anand, R., & Gangopadhyay, S. (2018). A TMDTO attack against lizard. *IEEE Transactions on Computers, 67*(5), 733–739. https://doi.org/10.1109/TC.2017.2773062
95. Potestad-Ordóñez, F. E., Tena-Sánchez, E., Mora-Gutiérrez, J. M., Valencia-Barrero, M., & Jiménez-Fernández, C. J. (2021). Trivium stream cipher countermeasures against fault injection attacks and DFA. *IEEE Access, 9*, 168444–168454. https://doi.org/10.1109/ACCESS.2021.3136609
96. Luo, H., Wu, Y., & Chen, W. (2020). Differential fault attack on TWINE block cipher with nibble. In *2020 IEEE 20th international conference on communication technology (ICCT), Nanning* (pp. 1151–1155). https://doi.org/10.1109/ICCT50939.2020.9295786
97. Degnan, B., Rose, E., Durgin, G., & Maeda, S. (2017). A modified Simon cipher 4-block key schedule as a hash. *IEEE Journal of Radio Frequency Identification, 1*(1), 85–89. https://doi.org/10.1109/JRFID.2017.2764389
98. Cheng, L., Xu, P., & Wei, Y. (2016). New related-key impossible differential attack on MIBS-80. In *2016 international conference on intelligent networking and collaborative systems (INCoS), Ostrava* (pp. 203–206). https://doi.org/10.1109/INCoS.2016.41
99. Luo, H., Chen, W., Ming, X., & Wu, Y. (2021). General differential fault attack on PRESENT and GIFT cipher with nibble. *IEEE Access, 9*, 37697–37706. https://doi.org/10.1109/ACCESS.2021.3062665
100. Zhang, B., & Gong, X. (2015). Another tradeoff attack on sprout-like stream ciphers. In T. Iwata & J. Cheon (Eds.), *Advances in cryptology—ASIACRYPT 2015. ASIACRYPT 2015. Lecture notes in computer science.* (Vol. 9453). Springer. https://doi.org/10.1007/978-3-662-48800-3_23

101. Mohd, B. J., Hayajneh, T., & Abu Khalaf, Z. (2015). Optimization and modeling of FPGA implementation of the Katan Cipher. In *2015 6th international conference on information and communication systems (ICICS), Amman* (pp. 68–72). https://doi.org/10.1109/IACS.2015.7103204
102. Li, L., Liu, B., & Wang, H. (2016). QTL: A new ultra-lightweight block cipher. *Microprocessors and Microsystems, 45*(Part A), 45–55. https://doi.org/10.1016/j.micpro.2016.03.011. ISSN 0141–9331.
103. Saha, S., Islam, M. R., Rahman, H., Hassan, M., & Hossain, A. A. (2014). Design and implementation of block cipher in hummingbird algorithm over FPGA. In *5th international conference on computing, communications and networking technologies (ICCCNT), Hefei* (pp. 1–5). https://doi.org/10.1109/ICCCNT.2014.6963084
104. Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., & Shirai, T. (2011). Piccolo: An ultra-lightweight blockcipher. In B. Preneel & T. Takagi (Eds.), *Cryptographic hardware and embedded systems—CHES 2011. CHES 2011. Lecture notes in computer science.* (Vol. 6917). Springer. https://doi.org/10.1007/978-3-642-23951-9_23
105. Mohammad Shah, I. N., Ismail, E. S., Samat, F., & Nek Abd Rahman, N. (2023). Modified generalized feistel network block cipher for the internet of things. *Symmetry, MDPI, 15*(4), 900. https://doi.org/10.3390/sym15040900
106. Cazorla, M., Marquet, K., & Minier, M. (2013). Survey and benchmark of lightweight block ciphers for wireless sensor networks. In *Proceedings of the SECRYPT*. http://eprint.iacr.org/2013/295
107. Rivest, R. L. (1994). The RC5 encryption algorithm. In *Proceeding of international workshop on fast software encryption* (pp. 86–96). Springer.
108. Mishra, Z., & Acharya, B. (2021). High throughput novel architectures of TEA family for high speed IoT and RFID applications. *Journal of Information Security and Applications, 61*, 102906. https://doi.org/10.1016/j.jisa.2021.102906. ISSN 2214-2126.
109. National Institute of Standards and Technology (NIST). (2001). Advanced encryption standard (AES). Federal information processing standards publication 197, November 26. http://csrc.nist.gov/publications/fps/fps197/fps-197.pdf
110. Chen, S., Fan, Y., Sun, L., Fu, Y., Zhou, H., Li, Y., Wang, M., Wang, W., & Guo, C. (2022). SAND: An AND-RX Feistel lightweight block cipher supporting S-box-based security evaluations. *Designs, Codes and Cryptography.* https://doi.org/10.1007/s10623-021-00970-9
111. Chen, W., Li, L., Guo, Y., & Huang, Y. (2023). SAND-2: An optimized implementation of lightweight block cipher. *Integration, 91*, 23–34. https://doi.org/10.1016/j.vlsi.2023.02.013. ISSN 0167-9260.
112. Guo, Y., Li, L., & Liu, B. (2021). Shadow: A lightweight block cipher for IoT nodes. *IEEE Internet of Things Journal, 8*(16), 13014–13023. https://doi.org/10.1109/JIOT.2021.3064203
113. Nallathambi, B., & Palanivel, K. (2020). Fault diagnosis architecture for SKINNY family of block ciphers. *Microprocessors and Microsystems, 77*, 103202.
114. Dalmasso, L., Bruguier, F., Benoit, P., & Torres, L. (2019). Evaluation of SPN-based lightweight crypto-ciphers. *IEEE Access, 7*, 10559–10567.
115. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., & Iwata, T. (2007). The 128-bit blockcipher CLEFIA (extended abstract). In *Fast software encryption (FSE 2007), LNCS, 4593* (pp. 181–195). Springer.
116. Cheng, X., Zhu, H., Xu, Y., Zhang, Y., Xiao, H., & Zhang, Z. (2021). A reconfigurable and compact hardware architecture of CLEFIA block cipher with multi-configuration. *Microelectronics Journal, 114*, 105144.
117. Lata, K., & Saini, S. (2020). Hardware software co-simulation of an AES-128 based data encryption in image processing systems for the internet of things environment. In *Proceedings of the 2020 IEEE international symposium on smart electronic systems (iSES) (Formerly iNiS), Chennai, India, 14–16 December 2020* (pp. 260–264).
118. Gunasekaran, M., Rahul, K., & Yachareni, S. (2021) Virtex 7 FPGA implementation of 256 bit key AES algorithm with key schedule and sub bytes block optimization. In *Proceedings of the 2021 IEEE international IOT, electronics and mechatronics conference (IEMTRONICS), Toronto, ON, Canada, 21–24 April 2021* (pp. 1–6).
119. Acharya, L. C., Purohit, J. P., Bairwa, S. K., & Kumawat, H. C. (2017). FPGA design & implementation of optimized RC5 block cipher. https://doi.org/10.1109/TEL-NET.2017.8343556
120. Harish, J., Madhuri, S. J., Yaswanth, V., Naidu, K., & Jagannadha. (2016). Low power ASIC implementation of RC5 algorithm. *International Journal of Chemical Sciences, 14*, 725–732.
121. Wheeler, D. J., & Needham, R. M. (1994). TEA, a tiny encryption algorithm. In *Proceeding of international workshop on fast software encryption* (pp. 363–366). Springer.
122. Hussain, M. A., & Badar, R. (2015). FPGA based implementation scenarios of TEA block cipher. https://doi.org/10.1109/FIT.2015.56
123. Hasan, M. N., Hasan, M. T., Toma, R. N., & Maniruzzaman, M. (2016). FPGA implementation of LBlock lightweight block cipher. In *2016 3rd international conference on electrical engineering and information communication technology (ICEEICT), Dhaka* (pp. 1–4). https://doi.org/10.1109/CEEICT.2016.7873062
124. Biryukov, A., Shamir, A., & Wagner, D. (2001). *Real time cryptanalysis of A5, 1 on a PC, Fast Software Encryption (FSE), LNCS* (Vol. 1978, pp. 1–18). Springer.
125. Hell, M., Johansson, T., & Meier, W. (2005). Grain—A stream cipher for constrained environments. In *Workshop on RFID and light-weight crypto: Workshop record, Graz.*
126. Boesgaard, M., Vesterager, M., Pedersen, T., Christiansenm, J., & Scavenius, O. (2003). *Rabbit: A new high-performance stream cipher, FSE, LNCS* (Vol. 2887, pp. 307–329). Springer.
127. De Canniére, C., & Preneel, B. (2005). Trivium—A stream cipher construction inspired by block cipher design principles. ECRYPT Stream Cipher. http://www.ecrypt.eu.org/stream/paper/sdir/2006/021.pdf
128. Hamann, M., Krause, M., & Meier, W. (2017). LIZARD—A lightweight stream cipher for power constrained devices. *IACR Transmission Symmetric Cryptology, 1*, 45–79. https://doi.org/10.13154/tosc.v2017.i1.45-79
129. Dubrova, E., & Hell, M. (2017). Espresso: A stream cipher for 5G wireless communication systems. *Journal of Cryptography and Communication, 9*(2), 273–289.
130. Ghafari, V. A., Hu, H., & Xie, C. (2016). *Fruit V2: Ultra-lightweight Stream Cipher with Shorter Internal State* (Cryptology ePrint Archive Report 2016/355). http://eprint.iacr.org/2016/355
131. Mikhalev, V., Armknecht, F., & Muller, C. (2017). On ciphers that continuously access the non-volatile key. *IACR Transmission Symmetric Cryptology, 2*, 52–79. https://doi.org/10.13154/tosc.v2016.i2.52-79
132. Fan, X., Mandal, K., & Gong, G. (2013). Wg-8: A lightweight stream cipher for resource-constrained smart devices. *International conference on heterogeneous networking for quality, reliability, security and robustness* (pp. 617–632). Springer.
133. Hell, M., Johansson, T., & Maximov, A. (2006). A stream cipher proposal, Grain-128. In *IEEE international symposium on information theory, Seattle* (pp. 1614–1618).
134. Bernstein, D. J. (2005). The Salsa20 stream cipher, slides of talk. In *ECRYPT STVL workshop on symmetric key encryption*. http://cr.yp.to/talks.html#2005.05.26

135. Aumasson, J.-P., Henzen, L., Meier, W., & Naya-Plasencia, M. (2010). Quark: A lightweight hash. In *International workshop on cryptographic hardware and embedded systems* (pp. 1–15). Springer.
136. Kavun, E. B., & Yalcin, T. (2010). A lightweight implementation of keccak hash function for radiofrequency identification applications. In *International workshop on radio frequency identification: security and privacy issues* (pp. 258–269). Springer.
137. Guo, J., Peyrin, T., & Poschmann, A. (2011). The PHOTON family of lightweight hash functions. In *CRYPTO 2011, LNCS 6841, international association for cryptologic research* (pp. 222–239).
138. Bogdanov, A., Knežević, M., Leander, G., Toz1, D., Varıcı, K, &Verbauwhede, I. (2011). SPONGENT: A lightweight hash function. In *CHES 2011, LNCS 6917, international association for cryptologic research* (pp. 312–325).
139. Maetouq, A., & Daud, S. M. (2020). HMNT: Hash function based on new mersenne number transform. *IEEE Access, 8*, 80395–80407. https://doi.org/10.1109/ACCESS.2020.2989820
140. Barreto, P. S. L. M., & Rijmen, V. (2011). Whirlpool. In H. C. A. van Tilborg & S. Jajodia (Eds.), *Encyclopedia of cryptography and security.* Springer. https://doi.org/10.1007/978-1-4419-5906-5_626
141. Handschuh, H. (2011). SHA-0, SHA-1, SHA-2 (secure hash algorithm). In H. C. A. van Tilborg & S. Jajodia (Eds.), *Encyclopedia of cryptography and security.* Boston: Springer. https://doi.org/10.1007/978-1-4419-5906-5_615
142. Gilbert, H., & Handschuh, H. (2004). Security analysis of SHA-256 and sisters. In M. Matsui & R. J. Zuccherato (Eds.), *Selected areas in cryptography. SAC 2003. Lecture notes in computer science.* (Vol. 3006). Springer. https://doi.org/10.1007/978-3-540-24654-1_13
143. Sklavos, N. (2012). Towards to SHA-3 hashing standard for secure communications: On the hardware evaluation development. *IEEE Latin America Transactions, 10*(1), 1433–1434. https://doi.org/10.1109/TLA.2012.6142498
144. Wang, X., Lai, X., Feng, D., Chen, H., & Yu, X. (2005). Cryptanalysis of the hash functions MD4 and RIPEMD. In R. Cramer (Ed.), *Advances in cryptology—EUROCRYPT 2005. EUROCRYPT 2005. Lecture notes in computer science.* (Vol. 3494). Springer. https://doi.org/10.1007/11426639_1
145. Dobbertin, H., Bosselaers, A., & Preneel, B. (1996). RIPEMD-160: A strengthened version of RIPEMD. In D. Gollmann (Ed.), *Fast software encryption. FSE 1996. Lecture notes in computer science.* (Vol. 1039). Springer. https://doi.org/10.1007/3-540-60865-6_44
146. Wong, D. S., Fuentes, H. H., & Chan, A. H. (2001). The performance measurement of cryptographic primitives on palm devices. In *17th annual computer security applications conference, New Orleans* (pp. 92–101). https://doi.org/10.1109/ACSAC.2001.991525
147. Bosselaers, A. (2005). Md4-Md5. In H. C. A. van Tilborg (Ed.), *Encyclopedia of cryptography and security.* Springer. https://doi.org/10.1007/0-387-23483-7_249
148. Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M. (2018). Elliptic curve lightweight cryptography: A survey. *IEEE Access, 6*, 72514–72550. https://doi.org/10.1109/ACCESS.2018.2881444
149. Rana, M., Mamun, Q., & Islam, R. (2023). Current lightweight cryptography protocols in Smart City IOT networks: A survey. Retrieved June 9, 2023, from arXiv:2010.00852.
150. Sankar, R., Subashri, T., & Vaidehi, V. (2011). Implementation and integration of efficient ECDH key exchanging mechanism in software based VoIP network. In *2011 international conference on recent trends in information technology (ICRTIT), Chennai* (pp. 124–128). https://doi.org/10.1109/ICRTIT.2011.5972416
151. Choi, J.-B., Kim, D.-S., Choe, J.-Y., Shin, K.-W. (2020). Hardware implementation of ECIES protocol on security SoC. In *2020 international conference on electronics, information, and communication (ICEIC), Barcelona* (pp. 1–4). https://doi.org/10.1109/ICEIC49074.2020.9051263
152. Bernstein, D. J., & Lange, T. (2014). SafeCurves: Choosing safe curves for elliptic-curve cryptography. Retrieved December 1, 2014, from https://safecurves.cr.yp.to
153. Jintcharadze, E., & Abashidze, M. (2023). Performance and comparative analysis of elliptic curve cryptography and RSA. In *2023 IEEE east-west design & test symposium (EWDTS), Batumi* (pp. 1–4). https://doi.org/10.1109/EWDTS59469.2023.10297088
154. Manoj Chowdary, G. N., Sri Rama Lakshmi, M. P., Nylu, Y., Deepthi, B., Prasad, K., & Kannaiah, S. K. (2023). Elliptic curve cryptography for network security. In *2023 International conference on inventive computation technologies (ICICT), Lalitpur* (pp. 1500–1503). https://doi.org/10.1109/ICICT57646.2023.10134492
155. Khan, M. R., et al. (2023). Analysis of elliptic curve cryptography & RSA. *Journal of ICT Standardization, 11*(4), 355–378. https://doi.org/10.13052/jicts2245-800X.1142
156. Ulla, M. M., Khan, M. S., & Sakkari, D. S. (2023). implementation of elliptic curve cryptosystem with bitcoin curves on SECP256k1, NIST256p, NIST521p, and LLL. *Journal of ICT Standardization, 11*(4), 329–353. https://doi.org/10.13052/jicts2245-800X.1141
157. Oladipupo, E. T., et al. (2023). An efficient authenticated elliptic curve cryptography scheme for multicore wireless sensor networks. *IEEE Access, 11*, 1306–1323. https://doi.org/10.1109/ACCESS.2022.3233632
158. Kaur, M., et al. (2023). EGCrypto: A low-complexity elliptic galois cryptography model for secure data transmission in IoT. *IEEE Access, 11*, 90739–90748. https://doi.org/10.1109/ACCESS.2023.3305271
159. Reddy, K .K., & Subshri, T. (2009). Confidentiality and integrity of VOIP data using efficient ECDH key exchanging mechanism. In *National level conference*. NIT.
160. Martínez, V. G., Hernández Encinas, L., & Sánchez Ávila, C. (2010). A survey of the elliptic curve integrated encryption scheme. *Journal Of Computer Science And Engineering, 2*, 7–13.
161. Dutta, I. K., Ghosh, B., & Bayoumi, M. (2019). Lightweight cryptography for internet of insecure things: A survey. In *2019 IEEE 9th annual computing and communication workshop and conference (CCWC), Las Vegas* (pp. 0475–0481). https://doi.org/10.1109/CCWC.2019.8666557
162. Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems, 129*, 77–89. https://doi.org/10.1016/j.future.2021.11.011. ISSN 0167-739X.
163. Gunathilake, N. A., Buchanan, W. J., & Asif, R. (2019). Next generation lightweight cryptography for smart IoT devices: Implementation, challenges and applications. In *2019 IEEE 5th world forum on internet of things (WF-IoT), Limerick* (pp. 707–710). https://doi.org/10.1109/WF-IoT.2019.8767250
164. Zhou, R., Zhang, X., Wang, X., Yang, G., Guizani, N., & Du, X. (2021). Efficient and traceable patient health data search system for hospital management in smart cities. *IEEE Internet of Things Journal, 8*(8), 6425–6436. https://doi.org/10.1109/JIOT.2020.3028598
165. Yu, S., Das, A. K., Park, Y., & Lorenz, P. (2022). SLAP-IoD: Secure and lightweight authentication protocol using physical unclonable functions for internet of drones in smart city environments. *IEEE Transactions on Vehicular Technology, 71*(10), 10374–10388. https://doi.org/10.1109/TVT.2022.3188769
166. Pandey, S., & Bhushan, B. (2023). Exploring the viability and effectiveness of lightweight cryptographic techniques in

enhancing the Iot data security of smart cities. In *2023 international conference on computational intelligence and sustainable engineering solutions (CISES), Greater Noida* (pp. 295–300). https://doi.org/10.1109/CISES58720.2023.10183537

167. Bajwa, N. T., Anjum, A., & Khan, M. A. (2023). A blockchain-based lightweight secure authentication and trust assessment framework for IoT devices in fog computing. In *2023 IEEE 20th international conference on smart communities: improving quality of life using AI, robotics and IoT (HONET), Boca Raton* (pp. 30–35). https://doi.org/10.1109/HONET59747.2023.10374800
168. Othman, W., Fuyou, M., Xue, K., & Hawbani, A. (2021). Physically secure lightweight and privacy-preserving message authentication protocol for VANET in smart city. *IEEE Transactions on Vehicular Technology, 70*(12), 12902–12917. https://doi.org/10.1109/TVT.2021.3121449
169. Esfahani, A., et al. (2019). A lightweight authentication mechanism for M2M communications in industrial IoT environment. *IEEE Internet of Things Journal, 6*(1), 288–296. https://doi.org/10.1109/JIOT.2017.2737630
170. Karati, A., Islam, S. H., & Karuppiah, M. (2018). Provably Secure and Lightweight Certificateless Signature Scheme for IIoT Environments. *IEEE Transactions on Industrial Informatics, 14*(8), 3701–3711. https://doi.org/10.1109/TII.2018.2794991
171. Kharghani, E., Aliakbari, S., Bidad, J., & Modarres, A. M. A. (2023) A lightweight authentication protocol for M2M communication in IIoT using physical unclonable functions. In *2023 31st international conference on electrical engineering (ICEE), Tehran* (pp. 676–683). https://doi.org/10.1109/ICEE59167.2023.10334808
172. Gupta, D. S. (2023). PiLike: Post-quantum identity-based lightweight authenticated key exchange protocol for IIoT environments. *IEEE Systems Journal*. https://doi.org/10.1109/JSYST.2023.3335217
173. Chen, B., Wu, L., Kumar, N., Choo, K.-K.R., & He, D. (2021). Lightweight searchable public-key encryption with forward privacy over IIoT outsourced data. *IEEE Transactions on Emerging Topics in Computing, 9*(4), 1753–1764. https://doi.org/10.1109/TETC.2019.2921113
174. Fan, K., Zhu, S., Zhang, K., Li, H., & Yang, Y. (2019). A lightweight authentication scheme for cloud-based RFID healthcare systems. *IEEE Network, 33*(2), 44–49. https://doi.org/10.1109/MNET.2019.1800225
175. Thilagaraj, M., Arul Murugan, C., Ramani, U., Ganesh, C., & Sabarish, P. (2023). A survey of efficient light weight cryptography algorithm for internet of medical things. In *2023 9th international conference on advanced computing and communication systems (ICACCS), Coimbatore* (pp. 2105–2109). https://doi.org/10.1109/ICACCS57279.2023.10112818
176. John, J., & Sinciya, P. O. (2023). Real-time distant healthcare monitoring IoT system secured by light weight cryptography. In *2023 annual international conference on emerging research areas: international conference on intelligent systems (AICERA/ICIS), Kanjirapally* (pp. 1–6). https://doi.org/10.1109/AICERA/ICIS59538.2023.10420248
177. Maram, B., Majji, R., Gopisetty, G. K. D., Garg, A., Daniya, T., & Kumar, B. S. (2023). Lightweight cryptography based deep learning techniques for securing IoT based E-healthcare system. In *2023 2nd international conference on automation, computing and renewable systems (ICACRS), Pudukkottai* (pp. 1334–1341). https://doi.org/10.1109/ICACRS58579.2023.10404726
178. Kp, B. M., & Patwari, N. (2023). Embedded light-weight cryptography technique to preserve privacy of healthcare wearable IoT device data. In *2023 international conference on distributed computing and electrical circuits and electronics (ICDCECE), Ballar* (pp. 1–6). https://doi.org/10.1109/ICDCECE57866.2023.10151002
179. Padmashree, M. G., Khanum, S., Arunalatha, J. S., & Venugopal, K. R. (2019). SIRLC: Secure information retrieval using lightweight cryptography in HIoT. In *TENCON 2019—2019 IEEE region 10 conference (TENCON), Kochi* (pp. 269–273). https://doi.org/10.1109/TENCON.2019.8929266
180. Nimmy, K., Sankaran, S., Achuthan, K., & Calyam, P. (2022). Lightweight and privacy-preserving remote user authentication for smart homes. *IEEE Access, 10*, 176–190. https://doi.org/10.1109/ACCESS.2021.3137175
181. Nyangaresi, V. O. (2022). Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. *Journal of Systems Architecture, 133*, 102763. https://doi.org/10.1016/j.sysarc.2022.102763. ISSN 1383-7621.
182. Ammi, M., Alarabi, S., & Benkhelifa, E. (2021). Customized blockchain-based architecture for secure smart home for lightweight IoT. *Information Processing & Management, 58*(3), 102482. https://doi.org/10.1016/j.ipm.2020.102482. ISSN 0306-4573.
183. An, H., He, D., Peng, C., Luo, M., & Wang, L. (2023). Efficient certificateless online/offline signcryption scheme without bilinear pairing for smart home consumer electronics. *IEEE Transactions on Consumer Electronics*. https://doi.org/10.1109/TCE.2023.3307697
184. Verma, G., Pachauri, S., Kumar, A., Patel, D., Kumar, A., & Pandey, A. (2023) Smart home automation with smart security system over the cloud. In *2023 14th international conference on computing communication and networking technologies (ICCCNT), Delhi* (pp. 1–7). https://doi.org/10.1109/ICCCNT56998.2023.10306548
185. Bauer, J., Helmke, R., Zimmermann, T., Bothe, A., Löpmeier, M., & Aschenbruck, N. (2019). Crypto can't—Confidentiality and privacy forCAN/ISOBUS networks in precision agriculture. *IEEE Conferenceon Local Computer Networks (LCN)*. https://doi.org/10.13140/RG.2.2.24012.97920
186. Grgić, K., Pejković, A., Zrnić, M., & Spišić, J. (2021). An overview of security aspects of IoT communication technologies for smart agriculture. In *2021 16th international conference on telecommunications (ConTEL), Zagreb* (pp. 146–151). https://doi.org/10.23919/ConTEL52528.2021.9495985
187. Abu-Tair, M., Djahel, S., Perry, P., Scotney, B., Zia, U., Carracedo, J. M., & Sajjad, A. (2020). Towards secure and privacy-preserving IoT enabled smart home: architecture and experimental study. *Sensors, 20*(21), 6131. https://doi.org/10.3390/s20216131
188. Prvulović, P., Radosavljević, N., & Babić, Đ. (2021). Analysis of lightweight cryptographic protocols in precision agriculture—A case study. In *2021 15th international conference on advanced technologies, systems and services in telecommunications (TELSIKS), Nis* (pp. 295–298). https://doi.org/10.1109/TELSIKS52058.2021.9606294
189. Itoo, S., Khan, A. A., Ahmad, M., & Idrisi, M. J. (2023). A secure and privacy-preserving lightweight authentication and key exchange algorithm for smart agriculture monitoring system. *IEEE Access, 11*, 56875–56890. https://doi.org/10.1109/ACCESS.2023.3280542
190. Saini, R. (2023). A lightweight secure authentication and key exchange algorithm for smart agriculture monitoring systems. In *2023 international conference on data science and network security (ICDSNS), Tiptur* (pp. 1–7). https://doi.org/10.1109/ICDSNS58469.2023.10245284
191. Garg, S., Kaur, K., Kaddoum, G., Rodrigues, J. J. P. C., & Guizani, M. (2020). Secure and lightweight authentication scheme for smart metering infrastructure in smart grid. *IEEE Transactions on Industrial Informatics, 16*(5), 3548–3557. https://doi.org/10.1109/TII.2019.2944880

192. Abbasinezhad-Mood, D., & Nikooghadam, M. (2018). Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications. *Future Generation Computer Systems, 84*, 47–57. https://doi.org/10.1016/j.future.2018.02.034. ISSN 0167-739X.
193. Gope, P., & Sikdar, B. (2019). Lightweight and privacy-friendly spatial data aggregation for secure power supply and demand management in smart grids. *IEEE Transactions on Information Forensics and Security, 14*(6), 1554–1566. https://doi.org/10.1109/TIFS.2018.2881730
194. You, X., et al. (2023). A lightweight authentication scheme in electric internet of things. In *2023 2nd international conference on smart grids and energy systems (SGES), Guangzhou* (pp. 368–372). https://doi.org/10.1109/SGES59720.2023.10366947
195. Wang, W., Huang, H., Zhang, L., Han, Z., Qiu, C., & Su, C. (2020). BlockSLAP: Blockchain-based secure and lightweight authentication protocol for smart grid. In *2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom), Guangzhou* (pp. 1332–1338). https://doi.org/10.1109/TrustCom50675.2020.00179
196. Jyoti, D., Mehta, P. J., Parne, B. L., & Patel, S. J. (2022). ALKAF: An anonymous lightweight key agreement framework for smart grid network. In *2022 IEEE 19th India council international conference (INDICON), Kochi* (pp. 1–6). https://doi.org/10.1109/INDICON56171.2022.10040081
197. Wang, J., Lim, M. K., Wang, C., & Tseng, M. L. (2021). The evolution of the Internet of Things (IoT) over the past 20 years. *Computers & Industrial Engineering, 155*, 107174. https://doi.org/10.1016/j.cie.2021.107174. ISSN 0360-8352.
198. Liu, C., Zhang, Y., Xu, J., Zhao, J., & Xiang, S. (2022). Ensuring the security and performance of IoT communication by improving encryption and decryption with the lightweight cipher uBlock. *IEEE Systems Journal, 16*(4), 5489–5500. https://doi.org/10.1109/JSYST.2022.3140850
199. Kundu, N., Debnath, S. K., & Mishra, D. (2021). A secure and efficient group signature scheme based on multivariate public key cryptography. *Journal of Information Security and Applications., 58*, 102776. https://doi.org/10.1016/j.jisa.2021.102776
200. Panchami, V., & Mathews, M. M. (2023). A substitution box for lightweight ciphers to secure internet of things. *Journal of King Saud University—Computer and Information Sciences, 35*(4), 75–89. https://doi.org/10.1016/j.jksuci.2023.03.004. ISSN 1319-1578.
201. Thabit, F., Can, O., Alhomdy, S., Al-Gaphari, G. H., & Jagtap, S. (2022). A novel effective lightweight homomorphic cryptographic algorithm for data security in cloud computing. *International Journal of Intelligent Networks*. https://doi.org/10.1016/j.ijin.2022.04.001
202. AiyshwariyaDevi, R., & Arunachalam, A. R. (2023). Enhancement of IoT device security using an Improved elliptic curve cryptography algorithm and malware detection utilizing deep LSTM. *High-Confidence Computing, 3*(2), 100117. https://doi.org/10.1016/j.hcc.2023.100117. ISSN 2667-2952.
203. Dofe, J., Frey, J., Pahlevanzadeh, H., & Yu, Q. (2015). Strengthening SIMON implementation against intelligent fault attacks. *IEEE Embedded Systems Letters, 7*(4), 113–116. https://doi.org/10.1109/LES.2015.2477273
204. Roy, I., Rebeiro, C., Hazra, A., & Bhunia, S. (2020). SAFARI: automatic synthesis of fault-attack resistant block cipher implementations. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 39*(4), 752–765. https://doi.org/10.1109/TCAD.2019.2897629
205. Potestad-Ordóñez, F. E., Tena-Sánchez, E., Acosta-Jiménez, A. J., Jiménez-Fernández, C. J., & Chaves, R. (2022). Design and evaluation of countermeasures against fault injection attacks and power side-channel leakage exploration for AES block cipher. *IEEE Access, 10*, 65548–65561. https://doi.org/10.1109/ACCESS.2022.3183764
206. Song, J., Kim, Y., & Seo, S. C. (2021). High-speed fault attack resistant implementation of PIPO block cipher on ARM cortex-A. *IEEE Access, 9*, 162893–162908. https://doi.org/10.1109/ACCESS.2021.3133888
207. DeCnudde, T., & Nikova, S. (2017). Securing the PRESENT block cipher against combined side-channel analysis and fault attacks. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 25*(12), 3291–3301. https://doi.org/10.1109/TVLSI.2017.2713483
208. Liu, Q., Ning, B., & Deng, P. (2019). Information theory-based quantitative evaluation method for countermeasures against fault injection attacks. *IEEE Access, 7*, 141920–141928. https://doi.org/10.1109/ACCESS.2019.2944024
209. Wang, B., et al. (2017). Exploration of benes network in cryptographic processors: A random infection countermeasure for block ciphers against fault attacks. *IEEE Transactions on Information Forensics and Security, 12*(2), 309–322. https://doi.org/10.1109/TIFS.2016.2612638
210. Xu, A., Wu, Y., Yang, J., Zhu, M., Zhao, Q., & Liu, L. (2022). A high-throughput hardware implementation of ZUC-256 stream cipher. In *2022 4th international conference on communications, information system and computer engineering (CISCE), Shenzhen* (pp. 24–27). https://doi.org/10.1109/CISCE55963.2022.9851111
211. Pandey, J. G., Goel, T., Nayak, M., Mitharwal, C., Karmakar, A., & Singh, R. (2018). A high-performance VLSI architecture of the present cipher and its implementations for SoCs. In *2018 31st IEEE International System-on-Chip Conference (SOCC), Arlington* (pp. 96–101). https://doi.org/10.1109/SOCC.2018.8618487
212. SenGupta, S., Chattopadhyay, A., Sinha, K., Maitra, S., & Sinha, B. P. (2013). High-performance hardware implementation for RC4 stream cipher. *IEEE Transactions on Computers, 62*(4), 730–743. https://doi.org/10.1109/TC.2012.19
213. Amdouni, R., Gafsi, M., Guesmi, R., Hajjaji, M. A., Mtibaa, A., & Bourennane, E. B. (2022). High-performance hardware architecture of a robust block-cipher algorithm based on different chaotic maps and DNA sequence encoding. *Integration, 87*, 346–363. https://doi.org/10.1016/j.vlsi.2022.08.002. ISSN 0167-9260.
214. Kumar, A., Singh, P., Patro, K. A. K., & Acharya, B. (2023). High-throughput and area-efficient architectures for image encryption using PRINCE cipher. *Integration, 90*, 224–235. https://doi.org/10.1016/j.vlsi.2023.01.011. ISSN 0167-9260.
215. Manoj, G. S., Sravanthi, B., Thirumal, G., & Venishetty, S. R. (2018). VLSI implementation of SMS4 cipher for optimized utilization of FPGA. In *2018 2nd international conference on inventive communication and computational technologies (ICICCT), Coimbatore* (pp. 1225–1231). https://doi.org/10.1109/ICICCT.2018.8472979
216. Ashaq, S., Nazish, M., Ali, M., Sultan, I., & Tariq Banday, M. (2022). FPGA implementation of PRESENT block cypher with optimised substitution box. In *2022 smart technologies, communication and robotics (STCR), Sathyamangalam* (pp. 1–6). https://doi.org/10.1109/STCR55312.2022.10009366
217. Tang, Y., Gong, Z., Sun, T., Chen, J., & Liu, Z. (2022). WBMatrix: An optimized matrix library for white-box block cipher implementations. *IEEE Transactions on Computers, 71*(12), 3375–3388. https://doi.org/10.1109/TC.2022.3152449
218. Kim, Y., & Seo, S. C. (2022). Optimized implementation of PIPO block cipher on 32-Bit ARM and RISC-V processors. *IEEE Access, 10*, 97298–97309. https://doi.org/10.1109/ACCESS.2022.3205617

219. Nakhate, S., & Kumar, A. R. (2020). Fast hartley transform based elliptic curve cryptography for resource constrained devices. In *2020 international conference on emerging smart computing and informatics (ESCI), Pune* (pp. 71–76). https://doi.org/10.1109/ESCI48226.2020.9167611
220. They, Y.-S., Phang, S.-Y., Lee, S., Lee, H. J., & Lim, H. (2008). CPOP: Cryptography process offloading proxy for resource constrained devices. In *2008 international conference on information security and assurance (ISA 2008), Busan* (pp. 289–294). https://doi.org/10.1109/ISA.2008.107
221. Li, X., Jiang, C., Du, D., Fei, M., & Wu, L. (2023). A novel revocable lightweight authentication scheme for resource-constrained devices in cyber-physical power systems. *IEEE Internet of Things Journal, 10*(6), 5280–5292. https://doi.org/10.1109/JIOT.2022.3221943
222. Ding, X., Wang, X., Xie, Y., & Li, F. (2022). a lightweight anonymous authentication protocol for resource-constrained devices in internet of things. *IEEE Internet of Things Journal, 9*(3), 1818–1829. https://doi.org/10.1109/JIOT.2021.3088641
223. Farha, F., Ning, H., Ali, K., Chen, L., & Nugent, C. (2021). SRAM-PUF-based entities authentication scheme for resource-constrained IoT devices. *IEEE Internet of Things Journal, 8*(7), 5904–5913. https://doi.org/10.1109/JIOT.2020.3032518
224. Xu, D., et al. (2022). Ring-ExpLWE: A high-performance and lightweight post-quantum encryption scheme for resource-constrained IoT devices. *IEEE Internet of Things Journal, 9*(23), 24122–24134. https://doi.org/10.1109/JIOT.2022.3189210
225. Shahbazi, K., & Ko, S.-B. (2021). Area-efficient Nano-AES implementation for internet-of-things devices. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 29*(1), 136–148. https://doi.org/10.1109/TVLSI.2020.3033928
226. Prakasam, P., Madheswaran, M., Sujith, K. P., & Sayeed, M. S. (2021). An enhanced energy efficient lightweight cryptography method for various IoT devices. *ICT Express*. https://doi.org/10.1016/j.icte.2021.03.007
227. Asare, B. T., Quist-Aphetsi, K., & Nana, L. (2019) A hybrid lightweight cryptographic scheme for securing node data based on the feistel cipher and MD5 hash algorithm in a local IoT network. In *2019 international conference on mechatronics, remote sensing, information systems and industrial information technologies (ICMRSISIIT), Ghana* (pp. 1–5). https://doi.org/10.1109/ICMRSISIIT46373.2020.9405869
228. Chatterjee, R., & Chakraborty, R. (2020). A modified lightweight PRESENT cipher for IoT security. In *2020 international conference on computer science, engineering and applications (ICCSEA), Gunupur* (pp. 1–6). https://doi.org/10.1109/ICCSEA49143.2020.9132950
229. Muzaffar, S., Waheed, O. T., Aung, Z., & Elfadel, I. M. (2021). Lightweight, single-clock-cycle, multilayer cipher for single-channel IoT communication: design and implementation. *IEEE Access, 9*, 66723–66737. https://doi.org/10.1109/ACCESS.2021.3076468
230. Tao, H., Bhuiyan, M. Z. A., Abdalla, A. N., Hassan, M. M., Zain, J. M., & Hayajneh, T. (2019). Secured data collection with hardware-based ciphers for IoT-based healthcare. *IEEE Internet of Things Journal, 6*(1), 410–420. https://doi.org/10.1109/JIOT.2018.2854714
231. Aboushosha, B., Ramadan, R. A., Dwivedi, A. D., El-Sayed, A., & Dessouky, M. M. (2020). SLIM: A lightweight block cipher for internet of health things. *IEEE Access, 8*, 203747–203757. https://doi.org/10.1109/ACCESS.2020.3036589
232. Tanizawa, K., & Futami, F. (2018). PSK Y-00 quantum stream cipher with 217 levels enabled by coarse-to-fine modulation using cascaded phase modulators. In *2018 European conference on optical communication (ECOC), Rome* (pp. 1–3). https://doi.org/10.1109/ECOC.2018.8535443
233. Li, Y., Pu, T., Zheng, J., Xiang, P., Li, J., & Zhang, X. (2021). Experimental demonstration of an optical domain decryption method for PSK quantum noise randomized cipher. In *2021 19th international conference on optical communications and networks (ICOCN), Qufu* (pp. 1–3). https://doi.org/10.1109/ICOCN53177.2021.9563786
234. Futami, F., Tanizawa, K., & Kato, K. (2020). Y-00 quantum-noise randomized stream cipher using intensity modulation signals for physical layer security of optical communications. *Journal of Lightwave Technology, 38*(10), 2774–2781. https://doi.org/10.1109/JLT.2020.2985709
235. Lei, C., et al. (2021). 16 QAM quantum noise stream cipher coherent transmission over 300 km without intermediate amplifier. *IEEE Photonics Technology Letters, 33*(18), 1002–1005. https://doi.org/10.1109/LPT.2021.3081797
236. Nakazawa, M., et al. (2017). qam quantum noise stream cipher transmission over 100 km with continuous variable quantum key distribution. *IEEE Journal of Quantum Electronics, 53*(4), 1–16. https://doi.org/10.1109/JQE.2017.2708523
237. Yang, X., Zhang, J., Li, Y., Zhao, Y., Gao, G., & Zhang, H. (2019). DFTs-OFDM based quantum noise stream cipher system. *Optical Fiber Technology., 52*, 101939. https://doi.org/10.1016/j.yofte.2019.101939
238. Zakaria, A. A., Azni, A. H., Ridzuan, F., Zakaria, N. H., & Daud, M. (2020). Extended RECTANGLE algorithm using 3D bit rotation to propose a new lightweight block cipher for IoT. *IEEE Access, 8*, 198646–198658. https://doi.org/10.1109/ACCESS.2020.3035375
239. Kim, T.-H., Kumar, G., Saha, R., Buchanan, W. J., Devgun, T., & Thomas, R. (2021). LiSP-XK: extended light-weight signcryption for IoT in resource-constrained environments. *IEEE Access, 9*, 100972–100980. https://doi.org/10.1109/ACCESS.2021.3097267

Shraiyash Pandey has completed his prior education in the United States of America and is currently working towards his Bachelor Degree (Bachelor of Technology in Computer Science and Engineering) at School of Engineering and Technology, Sharda University. His current CGPA is 9.1 on a 10-point scale. He has several noteworthy publications under his name related to Cybersecurity, and Cryptography. Additionally, he has presented his work in prestigious IEEE and Springer conferences across the globe. He has also hosted the keynote sessions of a few conferences such as ICCCIS-2023. Moreover, he has worked on various projects and actively presentedthem indifferent Hackathons.

Bharat Bhushan is an Assistant Professor of Department of Computer Science and Engineering (CSE) at School of Engineering and Technology, Sharda University, Greater Noida, India. He received his Undergraduate Degree (BTech in Computer Science and Engineering) with Distinction in 2012, received his Postgraduate Degree (M-Tech in Information Security) with Distinction in 2015 and Doctorate Degree (PhD Computer Science and Engineering) in 2021 from Birla Institute of Technology, Mesra, India. In the year 2021 and 2022, Stanford University (USA) listed Dr. Bharat Bhushan in the top 2% scientists list. He earned numerous international certifications such as CCNA, MCTS, MCITP, RHCE and CCNP. He has published more than 150 research papers in various renowned International Conferences and SCI indexed journals. He has contributed with more than 30 book chapters in various books and has edited 20 books from the most famed publishers like Elsevier, Springer, Wiley, IOP Press, IGI Global, and CRC Press. In the past, he worked as an assistant professor at HMR Institute of Technology and Management, New Delhi and Network Engineer in HCL Infosystems Ltd., Noida. In addition to being the senior member of IEEE, he is also a member of numerous renowned bodies including IAENG, CSTA, SCIEI, IAE and UACEE.