Wireless Networks (2021) 27:1515–1555
https://doi.org/10.1007/s11276-020-02535-5

Security of internet of things based on cryptographic algorithms: a survey

Seyyed Keyvan Mousavi[1] · Ali Ghaffari[2] · Sina Besharat[1,3] · Hamed Afshari[4]

Accepted: 26 December 2020 / Published online: 15 January 2021

Abstract
Internet of Things (IoT) is a new concept in Information and Communications Technology and its structure is based on smart objects communications. It contributes to controlling, managing, and administrating devices through the Internet. IoT is emerging as a key component of the Internet and a vital infrastructure for millions of interconnected objects. Thus, the security of IoT is highly important. Scalable applications and services are vulnerable to various attacks and information leakage, demanding greater levels of security and privacy. For instance, hacking personal information is a challenge in this regard. The present study is an investigation of symmetric, asymmetric and hybrid encryption algorithms for IoT security. Asymmetric key encryption to ensure secure communication between multiple users and thereby avoiding distributing key on an insecure channel. All algorithms are compared based on security factors. Results indicate that Elliptic Curve Cryptography (ECC) has a better performance than other algorithms in the study. ECC to generate smaller, faster and reliable cryptography keys. Also, ECC decreases the memory requirements and the execution encryption/decryption time. This study helps to understand the importance of several security factors in IoT and advancements in cryptography algorithms.

Keywords Internet of things · Security · Cryptography algorithm · Cyberattacks

1 Introduction

The world around us is replete with things or objects, such as Radio Frequency Identification (RFID), sensors, and actuators, mobile phones and many other smart devices that use an accurate addressing mechanism to work with each other and obtain a predefined goal. The omnipresence of these objects is felt stronger, in recent years, in wireless networks [1–3].

IoT is one of the hottest topics in the current period that has possessed many researchers due to its prevalent applications [4, 5]. IoT is the world of virtual, rather than real, entities where each person or thing on the internet has a correspondence that can be addressed, located and reached [6]. The virtual objects have the capacity to work around a common goal through producing and consuming services. For instance, a smart phone gets data from a host of devices connected to the body of a person to identify his physical and mental state and make due decisions on his behalf. Similarly, a high-tech system embedded in a swimming pool communicates its data with other virtual

✉ Ali Ghaffari
a.ghaffari@iaut.ac.ir

Seyyed Keyvan Mousavi
mosavikeyvan90@gmail.com

Sina Besharat
s.besharat@urmia.ac.ir

Hamed Afshari
h.afshari@iaurmia.ac.ir

[1] Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran

[2] Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran

[3] Department of Water Engineering, Faculty of Agricultural Sciences, Urmia University, Urmia, Iran

[4] Department of Mechanical and Bio Mechanical Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran

things connected to it. Thus, IoT is expected to expand its domain to cover anything or anyone at anytime and anywhere [7].

1.1 Motivation

Security factors such as privacy, secure storage and management, authorization, and communication as well as access control are the essential and challenging issues in the IoT environment. The large-scale stabilization of IoT devices and services outcomes in many vulnerabilities and threats in the nodes. Due to the limited processing capability, common security models suffer from different setbacks and often do not detect the physical threats in the network. Thus, the IoT security should be enhanced with the guaranteed communication and allows only the authorized user to access the data and updated frequently for the smart applications. Cryptography algorithms are the best algorithms for the security of IoT resources.

It is noteworthy that governments and organizations have tried to conceptualize IoT since it was invented, but their efforts have been rather sporadic and inconsistent. In simple words, IoT is defined as a widespread network of interrelated objects equipped with virtual devices that are around users and act based on sense and supervision. Objects in IoT are identified with six major characteristics listed below [8, 9]:

- **Existence:** all real things in this world, like a computer, have a physical existence but technologies are not pinned in the real world and only exist in a virtual arena.
- **Self-identity:** Everything has a characteristic that distinguishes it from other objects. For example, a BMW car has an explicit and implicit identity. Information processing, decision making and independent working are characteristics of many objects.
- **Communication:** objects can communicate with other things in their immediate environment as well as those in remote locations. This facilitates locating and addressing them.
- **Interaction:** things contribute to producing and consuming a wide range of services in their collaboration with many different entities in real or virtual spaces. This includes interactions with machines or humans.
- **Dynamicity:** things are dynamic and engage in working with other objects in different ways, whenever and wherever needed. They are not bound to a specific physical position and use different interface types, making them enter and leave a network when they need to.
- **Environmental Awareness:** things receive and process real and virtual information about their environments via sensors and are aware of what is going on around them. However, not all things have this capacity, like a device with lower-end radio frequency identification (RFID) tag.

IoT facilitates flawless and transparent connectivity between a host of different devices from a wide range of networks [10, 11]. This is the case when convenience, smartness, providing high-quality services and cost management are of the highest importance. Thus, IoT finds application in many development plans in urban, rural and civil projects like smart cities.

Another significant area of concern is the security of IoT applications in business. Once a smart object from a big business department is hacked by an outside intruder, its sensing information is seized by the attacker for spying purposes in the enterprise. Other classified information about the business may also be captured in these cyberattacks. Therefore, IoT security may be more demanding than internet security in general [12, 13]. This is because IoT is a combination of different networks that call for establishing security in many areas such as the Internet, sensor network and mobile networks. When various networks are connected in this way, new problems such as management, access control, authentication, and privacy emerge [14–16].

1.2 Main contributions

Since the IoT is an intricate, distributed and heterogeneous system, it faces various challenges regarding security and privacy. Privacy-preservation and data-protection are key to IoT applications. Sensors in a wireless sensor network and RFID systems are both equipped with password encryption technology to protect information confidentiality and integrity in IoT [17]. In this regard, asymmetric and symmetric encryptions are used for such purposes. The connection between two entities in a given network is established through identity authentication and access control to ensure that authentic and valid data is exchanged and the true identity of both sided are identified while avoiding disguised attacks [18].

The security of IoT devices is a significant issue due to the increasing numbers of services and users in IoT networks. The integration of IoT devices and smart environments creates smart objects more effective. However, the impacts of IoT security vulnerabilities are very calamitous in essential smart environments used in fields such as intelligent irrigation and industry. In IoT-based smart environments without robust security, applications and services will be at risk. Integrity, confidentiality, and availability are three substantial security concepts of applications and services in IoT-based smart environments;

thus, to address these concerns, information security in IoT systems requires greater research focus.

Data encryption allows for delivering confidential and integrated messages to authentic end-users or systems and ensures non-repudiation of transactions. Here, authentication helps both sides of a communication process determine the true identity of each other and spot their correct targets. Confidential delivery means that the contents of a message are not disclosed. Integration ensures that message content remains as it was sent from the original user [19]. By non-repudiation, it is meant that both sides of communication feel bound to their duty of protecting and performing for each other. In this paper, cryptographic algorithms will be further examined. Our contribution can be summarized as follows:

- This literature reviews collects and reviews state-of-the-art symmetric, and asymmetric cryptography algorithms for IoT data security.
- A comparative analysis of the cryptography algorithms has been carried out in terms of Confidentiality, Integrity, Authentication, Authorization, Availability, Non-repudiation, Accountability, Anonymity and type of attacks.
- This paper reviews IoT security threats based on cryptography algorithms that lead to IoT adoption.
- Scrutiny of related works based on preventing attacks by adopting cryptography algorithms.
- In the end, a statistical overview of published papers on cryptography algorithms based IoT security (security factors and detecting the type of attack by cryptographies) has been presented which will help researchers to give an idea about published research on a particular area of interest and its potentiality.

In this study, several papers were investigated based on cryptography algorithms. These papers mainly study the design and implementation of encryption for use in the IoT paradigm that can be applied in smart environments. The most important difference between this paper and previous studies is that in this paper, only the cryptographic algorithms used in the IoT were investigated and analyzed. Also, important security factors are extracted from the done studies and given to researchers an overview of the most important threats in IoT.

1.3 Organization of the paper

The rest of the paper is organized as follows: In Sect. 2, we briefly explain the IoT Architecture. Section 3, explains Security of IoT based on cryptography algorithms. Section 4, discusses the open problems and issues in IoT security based on cryptography. Finally, Sect. 5 concludes this study.

2 IoT architecture

In 1999, Kevin Ashton from Massachusetts Institute of Technology proposed IoT as a new concept based on RFID [20]. The RFID technology enabled all things in the network to be interconnected, easily identified and managed. Today, the internet helps connect many sensing devices such as RFID, ZigBee, IR (Infrared), GPS, WIFI and UMTS (Universal Mobile Telecommunications System). These devices use a variety of protocols to communicate with each other and exchange information. Objects provide for information exchange in remote areas. IoT contains a considerable amount of sensing devices that transmit a great deal of data that needs to be securely delivered [21]. Any sensing device in IoT has its own specific identity and identifier (an IP address or URI). Smart IoT interfaces allow users to observe their status, implement remote control and management, perform infrastructural configuration, and search devices [21]. Devices in IoT are mounted on an information network o be able to communicate data with other systems and devices. These devices can identify and be identified by other similar devices on the network in order to exchange information. This helps make the IoT system work even smarter because individual devices are integrated and work proficiently with the infrastructural system. This way, data from different interconnected devices are gathered and processed. For instance, data from a host of weather monitoring IoT devices are collected to be used for forecast purposes.

In simple words, IoT system is made up of hierarchical layers that together compose the IoT architecture. Out of several layers, the most important ones are the application layer, network layer, and perception layer. Each layer has its own distinct technology, and even devices in the same layer may use a specific technology of its own. This is to provide for the widest possible services in the network that have their own requirements and limitations [21]. However, one drawback is that it becomes significantly hard to manage these heterogeneous devices and technologies. To care for this difficulty, a middleware layer is often inserted to deal with various service types. This middleware layer is responsible for collecting network layers information and then storing them in the cloud and database. It also provides data processing. Therefore, a fourth layer is added to the IoT architecture, as illustrated in Fig. 1. These layers are discussed in detail below.

2.1 Application layer

It is the outer visible layer of IoT architecture that seeks to supply industrial demands and realize intellectual needs. The application layer performs many tasks in different

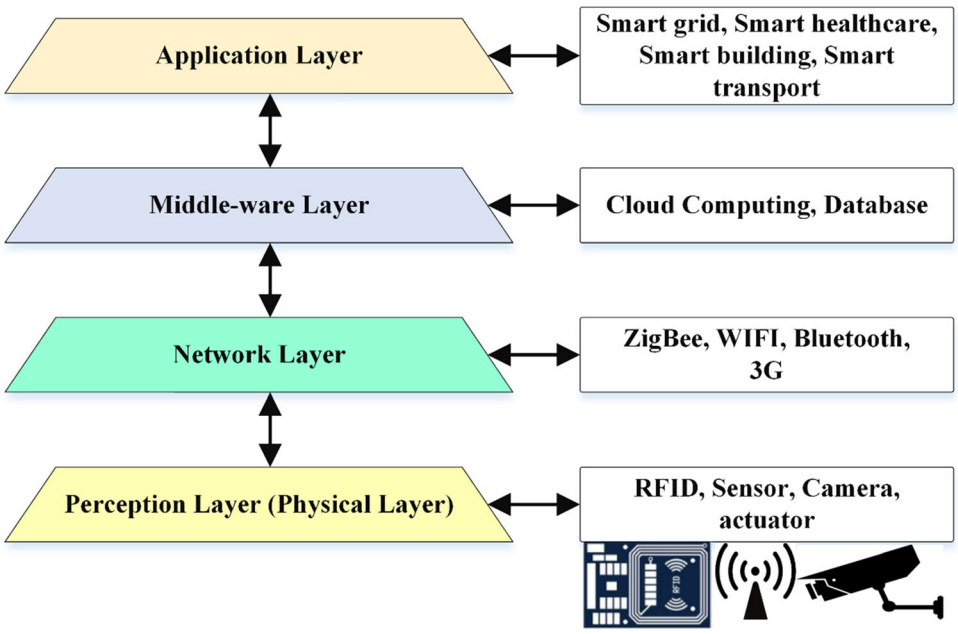

Fig. 1 Four-layer architecture of IoT

contexts. It receives data from the middleware layer, then it processes this data to offer quality services to the end user. The problem of the application layer mainly occurs in the operation of sensitive data, such as illegal access to data, malicious rectification of data, and the lifetime of permission. Therefore, hackers can have access to sensitive data and even manipulate them [21].

The application layer offers a host of services in the network. As said above, it processes data from the middleware layer and this procedure includes monitoring devices and services, identifying events, managing communications, administrating policies, managing input/output, logging information and remote management. Each of these services has a direct correspondence to the perception layer. The middleware layer is the mediator between the application and perception layers to provide information transfer and data process.

2.2 Middleware layer

This layer is responsible for receiving data from the network layer to process and store system data in the cloud and database. It also feeds the application layer with the required APIs. The storage and computational capacity of the middleware layer is a function of advanced cloud computing and IoT development. Service quality in the application layer is also determined by the security of the cloud and database [21].

The processing procedure is twofold: authentication and processing. Data authentication includes Devices and Services Monitoring Agent (DSMA), Authentication Center (AC) and Information Logging. On the other hand, remote management, managing communication, managing policies, and identifying events are associated with data processing. Once the obtained data are authenticated, they are stored with a signature in the information logging, and then transferred to the application layer.

The middleware layer is accountable for service management over IoT devices to make connections between IoT devices that provide the same service [22, 23]. Moreover, the middleware layer stores the information coming from the network layer in a database to facilitate decision-making on the basis of information processing operations [24].

2.3 Network layer

The network layer provides infrastructural connectivity of the IoT. It aggregates data from the perception layer and transfers them via a wired or wireless medium to the middleware layer. ZigBee, WIFI, Bluetooth, 3G are some technologies used for data transmission. The layer has to prevent pervasive attacks that undermine coordination and information sharing between the devices [21].

2.4 Perception layer

In the perception layer, the objects are identified and the information is collected to be changed to digital signals. The main technologies used in this layer are RFID tags, cameras, sensors, and wireless sensor network. The major technologies in this layer are RFID, Wireless Sensor Networks (WSNs) [25–29], RSN, GPS, etc. the performance of the perception layer is determined by its computational

power and energy supply. A sensing device may be used in a perilous situation that is vulnerable to intentional or unintentional attacks which may affect identification technology. This also disrupts the data collection process and undermines system efficiency [21]. The two main components of the perception layer are perception node and perception network. The former includes sensors or controllers and is used for data collection and control. The latter transmits the acquired data to the gateway or feeds the controller with the control instruction.

The perception layer is a hardware layer that consists of sensors and physical objects in different forms. These hardware elements provide identification, information storage, information collection, and information processing [30–32].

The differences between IoT and Cyber-Physical System (CPS) are as follows [33]: Both IOT and CPS have physical aspect as well as cyber aspect. IoT emphasizes on connectivity while CPS emphasizes on embedded part. CPS is not necessarily connected to the Internet. CPS consists of five levels, namely the connection, conversion, cyber, cognition, and configuration levels. In CPS, embedded computation and communication devices, together with sensors and actuators of the physical substratum, are federated in heterogeneous, open, and systems-of-systems.

3 Security of IoT based on cryptography algorithms

IoT faces many security challenges including the configuration of the system, storage and management of information, privacy-preservation, access control, and authentication [34]. IoT devices adapt to human needs and facilitate communication and convenience through providing sensitive services and responsive care. Nevertheless, security may be compromised, particularly when user information is disclosed or privacy is threatened [35]. Users need to be reassured of their privacy and personal information. Therefore, security is the pivotal concern of the IoT, particularly because its traditional method of communication is the internet which is an open environment to attacks by public and individual cybercriminals. Security measures are not limited only to infrastructure and the system but may call for hardware and physical security [36].

Security is any measure taken in a computer system to protect it against illegitimate access and abuse of information by an intruder. Disclosure of personal information, credit card thefts, leakage of economic information, virus attacks to computer systems are some examples of malicious attacks on a daily basis. The following criteria are necessary for establishing computer system security:

- **Confidentiality**: it guarantees that system information is protected against illegal access from an outside source. Data confidentiality is preserved in different ways. However, cryptographic measures and access control are the most common ones for this purpose. Cryptography is the technique by which the target data is encoded and cannot be used by any entity unless it possesses the decryption key. Some common encryption algorithms are RSA, DSA, AES. In access control process, unauthorized access to sensitive information is denied to anyone whose identity is not verified. Nevertheless, IoT never ensures effective protection because complex encryption and verification algorithms can't be applied [37].
- **Integrity**: integrated data are those which have not been manipulated by an unintelligible entity [38].
- **Authentication**: the process by which the identity of the user of system resources is verified is called authentication [38].
- **Non-repudiation**: Once the original node performs an action, such as sending a message, it can never deny it.
- **Availability**: system resources are accessible to authorized users.
- **Privacy**: it guarantees that the identity of the user can't be traced from his actions in the system [37].
- **Anonymity**: as part of the privacy-preservation, the tag's identity is kept anonymous in RFID authentication scheme.
- **Authorization**: Authorization is a security way used to determine user privileges or access levels related to system resources, including computer programs, files, services, data and application features.

Application of IoT is increasing by rapid developments in communication technologies which supply unfailing availability to information resources at any place and time. The concept of future Internet poses some concerns in terms of system security and network scalability, but offers an enriched experience for users. Providing integrated, confidential and authentic information is the major security challenge of IoT [39].

There are traditional models of cryptography such as the Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA) and ECC which work on systems that have the abundant computational power and memory capacities, but they cannot perform well with embedded systems and sensor networks. In IoT, the computing power of sensors, smart cards and other micro-devices is often limited. Hence, lightweight cryptography models are suggested to overcome many of the problems of common cryptography when applied to systems having constraints related to

physical size, computational requirements, energy consumption, and limited memory. Lightweight cryptography allows the application of secure encryption for devices with limited resources.

In general, encryption is a tool for securing systems that lightweight encryption is a good way to ensure data security. The International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) are maintaining standards about information and communication technology. According to these standards the algorithms to be considered as "lightweight cryptography" should follow requirements related to:

- **Security Strength for Lightweight Cryptography:** The minimum is 80-bit, but is proposed that at least 112-bit security should be utilized for systems that will give security for maximum longer periods. Smaller key size in order to attain power consumption with limited battery life, the key size must be small in a lightweight.
- **Software Implementation Attributes:** The code size and required RAM size should have fewer resource requirements than in existing standards for the same platform.
- **Hardware Implementation Attributes:** The chip area covered by the cryptographic model and the energy consumption should be less compared to existing ISO standards.

Stream ciphers are symmetric key ciphers that synthesize plaintext digits with a pseudorandom key stream to generate an output cipher stream. They are also called state ciphers because they comprise a secret internal state, which is used to produce the pseudorandom key stream. In the encryption procedure, the key stream is usually combined with the plaintext by applying a bit-wise XOR operator. At the receiver side, the same key stream is produced and is utilized to decrypt the cipher back to the main plaintext.

Block Ciphers are cryptography algorithms that procedure data in chunks called blocks. Plaintext blocks are composed with a key to generate ciphertext blocks. It is utilized to data encryption, message authentication, random bit generation, message hashing and so on. Presumably, the most important block ciphers in the world are AES and DES which have been developed as different international standards.

Cryptography is preserving the security of a message of any type in any given network while sending the data. A wide range of encryption algorithms is used for this purpose. The two main methods are symmetric (secret key encryption) algorithm for decryption and asymmetric (public-key) algorithm for encryption. Figure 2 demonstrates the use of cryptography algorithms in IoT. As can be seen, ECC (42%), AES (18%), and ABE (17%) are commonly used algorithms. ECC is more appropriate for devices that need lightweight cryptography due to their lesser resources such as computational power, memory, and energy.

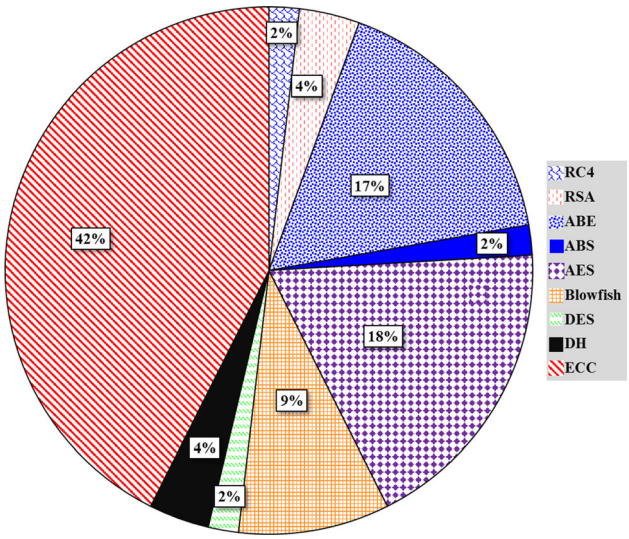

Fig. 2 Use of cryptography algorithms in IoT

Figure 3 shows use of cryptography algorithms in IoT based on year of publication. As can be seen, use of these algorithms increases after 2017. According to Fig. 4, 2018 had the very best frequency of published papers. Enormous number of research publications in journals and conferences are found associated with IoT. To illustrate the ongoing research work, we filtered the number of publications from 2011 to 2019-April through different database.

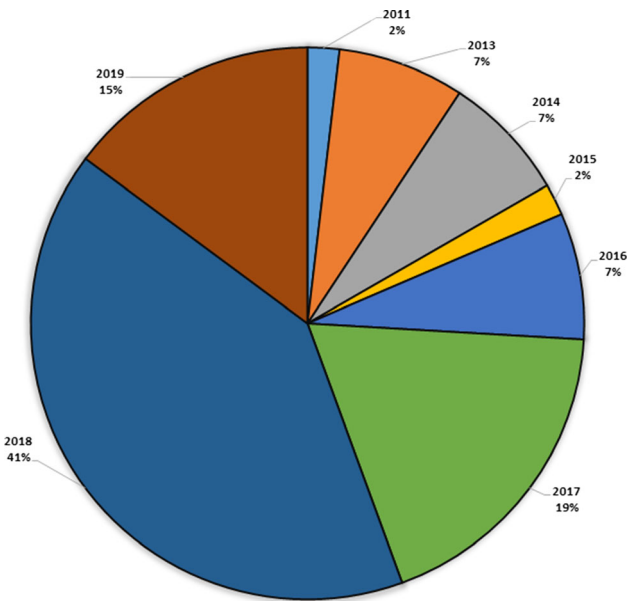

Fig. 3 Use of cryptography algorithms in IoT based on year of publication

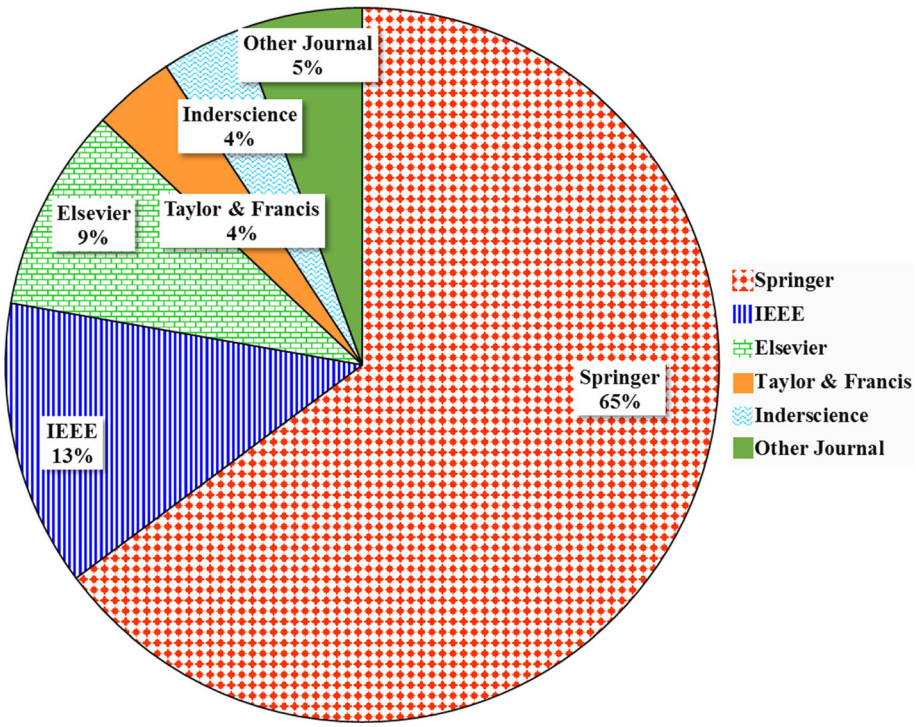

Fig. 4 Use of cryptography algorithms in IoT by publishers

Figure 4 illustrates use of cryptography algorithms in IoT by publishers. As can be seen, Springer is the most active publisher (65%), followed by IEEE (13%) and Elsevier (9%). Also, Taylor and Francis are 4% and Inderscience is 4%, and Other Journal is 5%. Given these percentages, it can be concluded that most reputable databases have discussed on IoT security based on cryptography algorithms.

3.1 Classification of lightweight cryptography algorithms

A classification of lightweight cryptographic algorithms is shown in Fig. 5. There are two major types of cryptography algorithms: asymmetric and symmetric.

3.2 Asymmetric algorithms

Cryptography is the process of securing communications to prevent cyberattacks. This is done through analyzing and designing the crucial protocols. Asymmetric algorithms have recently been used to provide for higher levels of security, some of which are discussed below. An asymmetric algorithm AE = (G, K, E, D) consists of four algorithms [40]:

- G(k): The common key production algorithm takes as inputting a security parameter k and outputting a common key I, defined by $I \leftarrow G(k)$;
- K(I): The key production algorithm takes as inputting the common key I and returning a public/private key pair (pk, sk), defined by $(pk, sk) \leftarrow K(I)$;
- $E_{pk}(m, r)$: The encryption algorithm takes as inputting a public key pk, a plaintext $m \in M$ and a random coin $r \in \Omega$, and returning a ciphertext C, defined by $C \leftarrow Epk(m, r)$. When the random coins are useless in the discussion, defined by $C \leftarrow E_{pk}(m)$;
- $D_{sk}(C)$: The decryption algorithm takes as inputting the secret key sk and a ciphertext C, and returning the corresponding plaintext m or a special symbol indicating that the ciphertext is invalid, defined by $m \leftarrow Dsk(C)$.

3.2.1 RSA

RSA is a public key cryptographic system and is named after its inventors (*Rivest*, *Shamir and Adleman*) in 1977 which offered encryption and digital signature [41]. It is based on difficulty in computational analysis of factorization of large prime numbers. In the process of encrypting and decrypting information, a public key (e, n) and a private key (d, n), both positive integers, are used. This process is as follows:

$$C = E(M) = M^e \ mod \ n, \ where \ M = message$$

$$D(C) = C^d mod \ n, \ where \ C = cipher \ text$$

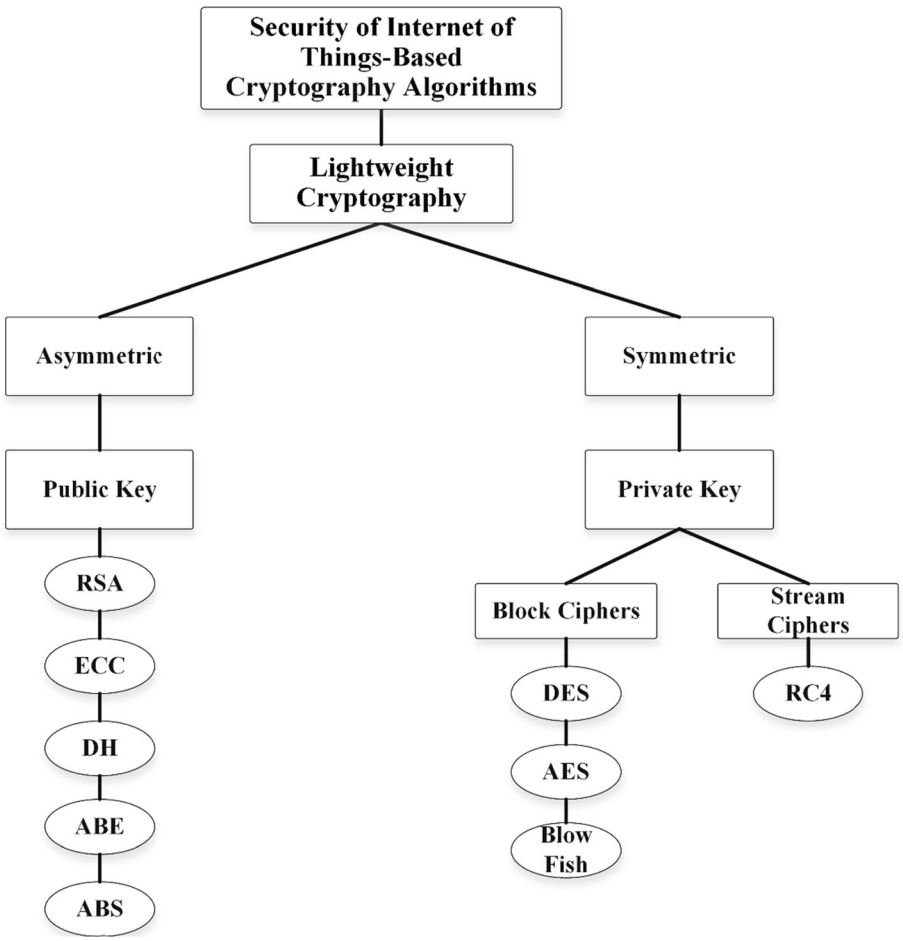

Fig. 5 Security of IoT based cryptography algorithms

$n = product\ of\ two\ large\ prime\ numbers\ p\ and\ q(n = p * q)$

$d = large\ random\ relative\ prime\ to\ p(i.e.gcd(d, (p-1) * (q-1)) = 1)$

$e = multiplicative\ inverse\ of\ d\ modulo\ (p-1) * (q-1)$

Opportunistic IoT systems have a subclass of opportunistic network. On the other hand, opportunistic use of IoT devices is applicable when the presence of devices is not clear. Therefore, in [42], the authors proposed an asymmetric RSA-based security scheme for opportunistic use of IoT scenarios. Here, messages are secured by RSA approach and data routing is done by forecasting the location of the node from its probable movement towards its destination and using Markov chain. Public encryption key is used and shared with all things in the network. However, the decryption key is kept private. Results of stimulations show that the proposed *RSASec* algorithm offers a high level of security in comparison with other approaches and protects users against eavesdropping and cryptography attacks. Low latency, fewer message dropout and high rate of message delivery are key features of this algorithm.

In [43], a secure communication protocol based on REWE homomorphic encryption in IoT convergence cloud environment is offered. The user and IoT gateway were first authenticated, followed by user registration and key-creation protocol design. The resulting data from the device was sent to a sever to perform cloud computations. Then, a mechanism for creating and managing an index was designed. Once key creation, user registration, and data management procedures were finished, a communication protocol was designed to increase privacy and prevent information disclosure. The present study offers a hash tree-based technique for managing certificate in signature value management to respond to data falsification. Cloud and gateway identification values, as well as user information were all set by the proposed RLWE. Then, we used encryption communication system to analyze security level. In addition, complexity of time and space was analyzed by RLWE and security against attacks was confirmed. Other threats regarding message disclosure, user privacy, resource and availability were also safeguarded in

RLWE. Unlike existing encryption communication protocol, RLWE was flexible for device scalability.

3.2.2 ECC

ECC was proposed in 1985 by Victor S. Miller and Neal Koblitz [44]. A key attribute of ECC is operating on finite domains. Suppose p is prime number and *Fp* is a finite domain including values smaller than p. then, the elliptic curve E is defined by Eq. (1) as follows:

$$y^2 = x^3 + ax + b \quad (1)$$

where $a, b \in F_p$ and $4a^3 + 27b^2 \neq 0(modp)$. Moreover, a and b change to different elliptic curve equations. If (x, y) realize on a point, it belongs to the elliptic curve. In addition, $E(F_p)$ is the set of all points on the elliptic curve, and G is a point of E. In ECC-based cryptography, a random number x (1, n-1) in the field F_p is selected and considered as the private key. Then, public key P_u is calculated as $P_u = P_r G$, where G is a point on elliptic curve and P_r is the private key. in ECC, each character is converted to bites that represent (x, y) points encrypted on elliptic curve. The encrypted points are then converted to bites (Fig. 6).

The elliptic curve is encrypted as follows:

1) Initialization. Each side of the curve select E and G of p order.
2) Public key generation: public key is generated as $P_u = P_r G$. Here, P_u is accessible as the public key to sender and receiver. P_r is the private key that used for decryption.
3) Encryption: A random number r is selected, and encryption of the message is performed using Eq. (2). Sender uses C to send message m to the receiver.

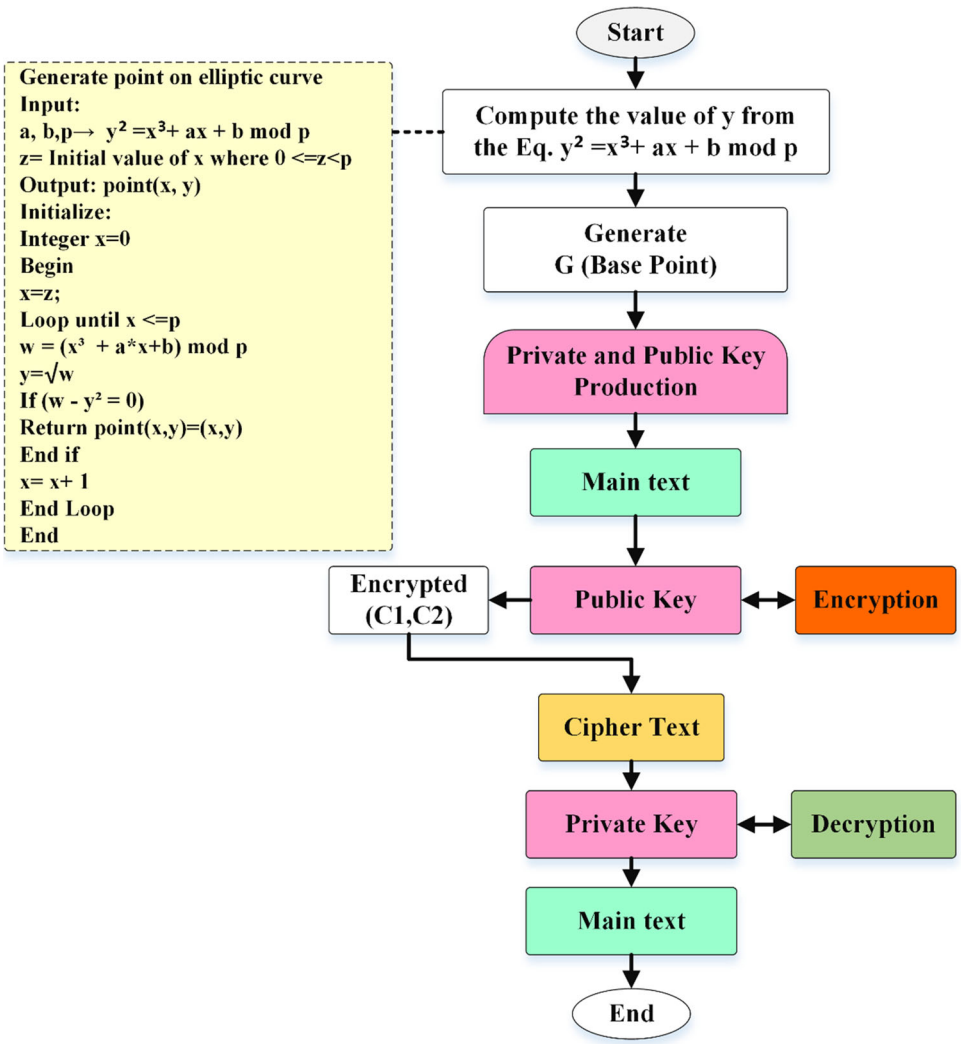

Fig. 6 Block diagram of ECC

$$C = Enc(m) = \begin{cases} c_1 = rG \\ c_2 = m + rP_u \end{cases} \rightarrow Enc(m) = (c_1, c_2) \quad (2)$$

4) Decryption: Upon the reception of C, the receiver obtains the value of m using P_r and Eq. (3).

$$Dec(C) = c_2 - P_r.c_1 = m + rP_u - P_r rG = m + rP_r G - P_r rG = m \quad (3)$$

ECC a lightweight cryptography based on the algebraic structure that benefits from small message size and fewer key production compared to other public key systems, while offering the same level of cybersecurity.

Communication security in cluster-based WSNs was proposed in [45] using a secure data transmission scheme (SDTS) that is based on ECC as it provides small key size with the same security level. The proposed method was introduced to prevent data disclosure and provide data security. It proved efficient in preventing brute force attack, replay attack, and sinkhole attack while meeting requirements of security, including integrity, authentication and confidentiality. SDTS also reduced costs of communication. Before the collected data are sent, ECC is used by sensors to encrypt the sensed data.

IoT devices are expected to optimally promote computational speed and reduce energy consumption without bargaining device security. Security standards in ECC are better managed than other typical algorithms, adding to its improved performance. The authors in [46] proposed an ECSM (elliptic curve scalar multiplication) algorithm over a prime filed Fp in affine coordinates. The proposed model is fast and field efficient and only has point operations that are involved in modular arithmetic operations (addition, subtraction, multiplication and inversion). ECSM is performed by these operations and is computed by a binary left–right method. The present study tried to optimize some major components like hardware implementation space and speed of computation in ECC. It showed an efficient method for sharing hardware resource and scheduling group operations of ECC. The obtained scalar multiplication hardware architecture is characterized with significantly fewer cycle count and acceptable area delay. The proposed architecture has been implemented with 256 bits in both Xilinx Kintex-7 and Virtex-7 FPGA devices. The FPGA synthesis results show that a throughput of 68.52 kbps at a clock frequency of 124.2 MHz is achieved for F256 and the computation time is reduced around 1 MS without using any DSP slices.

A secure ECC-based protocol was proposed in [47] to analyze the communication between the server and IoT devices. The proposed ECIOT protocol uses a DH protocol, which is based on NIST p-192 prime curve, to create a secret session key. This key is then used by the symmetric key cipher XOR to perform subsequent communication. IoT devices in ECIOT have a longer lifespan because it reduces power consumption and memory use. The authors in [48] used CoAP to improve data security in the sensor network of remote health monitoring of patients. This can also be done by asymmetric cryptography methods such as ECC and RSA which are also implemented to provide for integrity, authentication and confidentiality between the end nodes and users. These public key algorithms are compared in terms of key generation time, power and energy consumption, radio duty check, verification and generation of signature to evaluate their performance in hostile environments. Results showed that ECC is faster than RSA in key and signature generation but RSA shows faster verification time. Furthermore, small key size in ECC is an advantage in constrained situations where message delivery, verification and data security are key concerns. Since smaller key size is needed in ECC, less storage space is required while security level remains the same as RSA. Thus, in cases where storage, power and computation are key parameters, ECC has a better performance than RSA.

Widespread and prevalent use of IoT and cloud computing, real-time monitoring of patients by a remote medical professional is becoming more possible and the prospect of patient care at home is closer. A cloud server stores patient's medical records in a cloud-IoT network but because these are highly sensitive information, the network is subject to cyberattacks. To ensure security of these medical records, user identification is essential to be established in centralized healthcare systems. For instance, an ECC-based identification protocol in cloud-IoT networks is proposed in [49]. As Fig. 7 shows, this protocol includes, (a) a three-factor authentication of medical professionals; (b) a two-sided authentication of cloud server and medical professionals; (c) secure session key generation; (d) key freshness maintenance. The proposed protocol allows only for two message exchanges and reduces costs of computation and communication. AVISPA (Automated Validation of Internet Security Protocols and Applications) was used for security and performance analysis and the results showed that the protocol is effective in terms of security and generates a balance between performance and security in healthcare applications in cloud-IoT environments.

Today, automatic identification of objects is mostly done by RFID technology, making it a good candidate in IoT applications. RFID is characterized with good authentication and privacy protection. Many protocols have been suggested to establish privacy, efficiency and security of RFID techniques, but most of them have failed to meet the required standards for security and performance. An

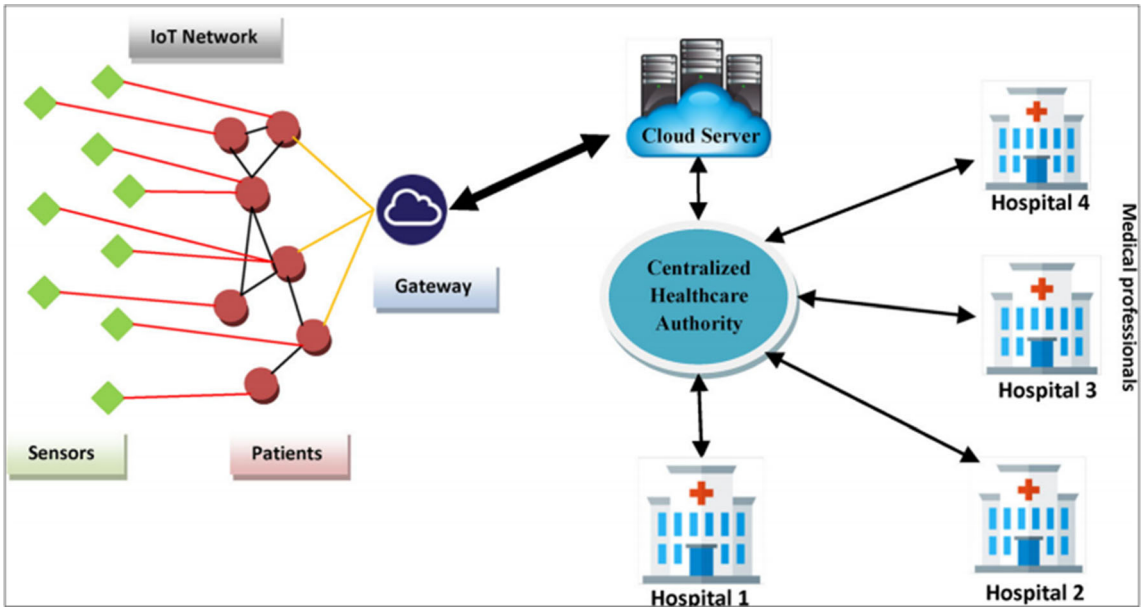

Fig. 7 Cloud-IoT healthcare service architecture [49]

ECC-based lightweight anonymous authentication protocol was proposed for RFID systems in [50] with an acceptable level of anonymity, confidentiality, authentication, and resistance against replay, impersonation and modification attacks. Performance analysis of the proposed protocol also showed costs of computations and communication reduced 3 times and 50%, respectively, as compared to earlier RFID protocols.

Similarly, another ECC-based authentication algorithm was proposed in [51] in situations where a new device is added to the network. The proposed protocol was effective in preventing attacks and providing security. Rapid growth of data in IoT calls for improving levels of security and privacy to reduce its weaknesses. Studies show that IP security protocols and algorithm have technical shortcomings and are not suitable for IoT. When a new device is added to a network, it should be authenticated and its level accessibility to network properties should be allocated. If not, the new device will bring about more vulnerabilities to the network and will expose it to different types of cyberattacks. Results of analysis showed that the proposed algorithm is resistant to DOS attack, Man in the middle, and Injection input attacks and provides sufficient security in the network.

In [52], an authenticated key agreement (AKAIOTS) was proposed for IoT to offer a secure shared key and secure data transfer between the cloud server and WSN clients. WSNs allow for Internet-based collection and transmission of data to cloud servers and hence are significant for IoT. Since sensor nodes are devices with resource constraints, designing a secure encryption system for IoT is difficult. The authenticated key agreement scheme offers different security properties and has a lightweight computation. In the random oracle model under computation Diffe-Hellman (DF) assumption, this scheme is still secure. BN-P158, SECG-P160, and NIST-P192 are three curves used in this context. Results of implementation demonstrate that, in all the three curves tested, computational efficiency and memory use from total ROM and RAM are 5–52% and 59–62%, respectively. Thus, SECG-P160 seems to be a good candidate for establishing data security in IoT because it has reasonable computation time and less power consumption than the other two curves.

A new scalar point-multiplication scheme based on ECC, with low energy consumption, is proposed in [53] that accelerates computation time and keeps power consumption at a low level without reducing security level. Implementation of the proposed architecture allows the citizens to have better things for all applications in smart settings to supply a secure exchange of information between internet services and IoT. Once again, encryption ensures that user integrity, confidentiality, privacy, and authentication are preserved. In the present study, ECC cryptographic algorithm and its energy efficiency in Android mobile devices are examined. Our results show that the proposed ECC-based method outperforms ECC-based binary method as well as ECC-based NAF method because doubling and number of scalar additions are reduced. Furthermore, battery life in the proposed algorithm is increased compared to other ECC methods. Asymmetric cryptographic algorithm preserves privacy and security of mobile device applications and exchanges

secured data between internet services and IoT networks. Nevertheless, ECC algorithms do not prevent DOS attacks.

In [54], three randomized access control protocols (EC-RAC1) as secure identity transfer schemes with enhanced security are proposed for IoT security. In EC-RAC1 protocol, if the received identity verifier is found in the database, the tag will be authenticated. EC-RAC2 is a sort of identity transfer system within which the server authenticates the tag when received identity verifier and its corresponding correct password in stored in the database. EC-RAC3 protocol is a technique for identity and password transfer security. If the received identity verifier is in the database and the associated password is correct, the tag will be authenticated.

IoT devices are applied in continuously changing environments and need to use adaptable software. Multi-agent solutions offer an adaptive IoT environment. Smart things in IoT are given global intelligence and interoperability by mobile agents. Therefore, user data security needs to be established for ever-increasing IoT devices when personal data of users are carried by agents. ECC algorithm has proved to be an attractive and efficient public key cryptographic scheme. An ECC-based Broadcast Mobile Agent Protocol (BROSMAP) is proposed in [55] that establishes integrity, non-reputation, confidentiality, authentication, and responsibility. The authors tried to promote BROSMAP to fit with requirements of multi-agent multi-agents. The improved ECC-BROSMAP has a better performance than its past version in terms of computational cost and execution time. It is found that ECC-BROSMAP is much faster than RSA 2048 BROSMAP and its performance is 4 times better than RSA 3072.

A secure ECC model is proposed in [56]. ECC is effective in using digital signature foe data encryption/decryption. Both private and public keys need to be generated in ECC. It offers an acceptable level of security and privacy and is often compared with RSA and DF algorithms. It achieves highest security in devices with low computing power.

Authors in [54] analyzed ECC for secure communication in IoT because existing protocols are not adaptable because of high storage, computation and communication demands. That is why ECC-based lightweight protocols are commonly used in such settings because they have a better computational performance than other algorithms like RSA.

Signcryption is a subcategory of cryptography that offers digital signature along with public key encryption in a logical single step. In conventional certificate-based cryptosystems, identity-based encryption was used because it was assumed that users' identity was used as his public key. In [57], a novel ECC-based signcryption method based on identity is proposed where security is established by ECDLP and ECDHP. It proves highly effective in security of low-end resource devices such as PDA, and internet-based mobile services like mobile banking.

Karla and Sood proposed an ECC-based authentication technique for the communication between IoT and cloud servers and demonstrated its security against cyberattacks. However, the proposed method is unable to deter offline password guessing and insider attacks in different scenarios. In addition, it has certain shortcomings such as lack of mutual authentication, session key agreement, and anonymity, excluding it from practical applications. An enhanced authentication scheme was proposed in [58] to compensate for the above shortcomings in the Karla and Sood model. Results of comparative analysis showed that the proposed model has an acceptable performance in combating various attacks.

A similar mutual authentication scheme is proposed in [59] for the communication between an ECC server and IoT devices which proves to be efficient in preventing attacks and reducing communication overhead. It also provides an enhanced security level.

Threat model and security challenges were two concerns of IoT systems covered in [60]. ECC has attracted the attention of researcher in recent years because of its higher computational efficiency than RSA. This is even more tangible where cost and performance measures are essential. Developing mechanisms and technologies that provide a desired level of security for platforms is of high importance. On the other hand, the great bulk of personal information to be kept private necessitates new scalable solutions that are adaptive and respond to new needs. Analysis of existing mechanisms show that ECC proves effective in managing real-time security of embedded devices. The prospect of ECC performance is also promising considering industrial optimization in this regard.

RFID authentication was reviewed in [61] as a three-part component: tags, the reader and the server. The communication route between the reader and the tags was not safe and secure. First, attacker can easily obtain personal data of users. Second, attackers appear in the disguise of tags or servers and disrupt uniqueness in the network. Thus, RFID is expected to raise its security authentication. A novel ECC-based RFID authentication scheme was proposed to overcome the above challenges and proved efficient for practical applications.

DCAPBAC (distributed capability-based access control approach) was proposed in [62] which is based mainly on lightweight and flexible design to be applied in resource-constrained devices and to enhance end-to-end security, interoperability and scalability of IoT. The proposed scheme was further verified using AVISPA and then implemented on JENNIC/NXP JN5148 chipset based on a

32-bit RISC CPU in a real scenario. Results of analysis showed its potential in being an optimal solution for IoT security.

RFID systems have found their ways into many applications including healthcare system, transportation and home appliances. Symmetric key and public key cryptography have been used to establish RFID security. Existing RFID protocols mostly concentrate on tag identification or authentication. IoT is widely used as a public network where any physical object from the real world will interact with a great number of objects through the internet. Therefore, IoT infrastructure needs to integrate many different technologies such as sensor networks, RFID system, embedded system, conventional desktop environment, and mobile communications. RFID systems will prove effective in this regard because it will offer more security features for internet applications. A secure and sustainable RFID system for IoT infrastructure was proposed in [63] that established data confidentiality, key establishment and mutual authentication.

An ECC-based public key cryptography (PKC) was proposed in [64] with a focus on mathematical optimization of cryptographic algorithms. PKC is adopted in IoT because of its advantages in providing interoperable, self-identifying and scalable properties, particularly for resource-constrained devices such as microprocessor Texas Instrument MSP430. The paper proposes a scalar multiplication ECC with 160-bit keys within 5.4 million clock cycles over MSP430 devices with no need to more hardware multiplier.

In [65], a security scheme was proposed with an ECC-based biometric aid to establish the desired security. The authors aimed at promoting communication between devices and implementing OTA firmware updates. Real system issues and integrated new optimizations using novel technologies led to establishing a secure framework that was 35% faster and 5% more efficient that other algorithms like ECC and OTA.

Future IoT is mainly concerned with providing security of small yet smart devices because certain technologies like 6LoWPAN provide Internet-based access to the real world. Computational capacity, communication band-with, storage space, and power consumption are major constrains of 6LoWPAN devices which necessitates scalable and optimized cryptographic techniques that feature integrity, authentication and privacy in communications. The authors in [66] concentrated on mathematical optimization of PKC cryptographic primitives based on ECC for 6LoWPAN that are based on microprocessor Texas Instrument MSP430. Montgomery multiplication operation is the focus of optimization mechanism which is achieved through bit shifting, and defining certain pseudo-Mersenne primes known as shifting primes. Once these optimizations are performed, scalar multiplication for ECC operations reduces to 1.2665 s, showing 42.8% enhances performance compared to Tiny-ECC (2.217 s). Table 1 summarizes security factors of ECC-based IoT.

3.2.3 DH

A common authentication protocol for resources-constrained devices in IoT is Ephemeral DH over COSE (EDHOC) that replaces TLS and adopts different approaches [67]. EDHOC has considerable resistance against attacks but one drawback is that it is hard to fix any shortcomings in its design.

In [68], a DH-based Cloud of Things (CoT) for a multifactor authentication system was proposed. CoT is a concept that integrates cloud computing with IoT and allows for ease of access for IoT services, virtual control and greater scalability. However, despite its prospective advantages, security, user authentication and identification are big challenges in CoT.

3.2.4 ABE

In [69], the authors proposed a new architecture to enhance security and privacy of information exchange that takes advantages of effectiveness of symmetric key encryption and flexible feature of CP-ABE. AES with symmetric keys are used for data encryption. The keys are also encrypted using access policies of original data sender. The data are decrypted by using CP-AES algorithm to recover the symmetric key.

As Fig. 8 indicates, CP-ABE encryption operation is a demanding task and is not performed by data sources but rather are assigned to the ABE proxy. Moreover, other considerations such as functionalities offered by IoT cloud platform are taken into account to facilitate data storage and retrieval and to manage AES- encrypted symmetric keys. For instance, Key Generation Service (KGS) uses data consumer attributes obtained from his profile to feed the ABE proxy with information required for encryption.

Similarly, an ABE-based secure smart health (SSH) system for IoT architecture was proposed in [70] which is characterized with less aggregate signature, anonymous certificates, and anonymous CP-ABE scheme composed of four algorithms including Setup, AttributeKeyGen, AnonEncrypt, and AnonDecrypt. To provide for access control, aggregate authentication, and privacy issues, SSH hides sensitive data and identity information of users. Once a user uploads SHR, the cloud service checks that for any threats to filter invalid SHR to the cloud. The performance of SSH in reducing costs of communication and computation is acceptable.

Table 1 Security factors of ECC-based IoT

References	Title	Confidentiality	Integrity	Authentication	Authorization	Availability	Non-repudiation	Accountability	Anonymity	Prevent attacks	Year	Publisher
[45]	Secure Data Transmission Scheme Based on Elliptic Curve Cryptography for Internet of Things	×	✔	✔	×	×	×	✔	×	Replay Attack, Sinkhole Attack, Brute force attack	2019	Springer
[46]	High-performance ECC processor architecture design for IoT security applications	✔	✔	✔	✔	✔	×	✔	×	–	2019	Springer
[47]	Revisiting of Elliptical Curve Cryptography for Securing Internet of Things (IOT)	×	✔	✔	✔	✔	×	✔	×	Passive attacks	2018	IEEE
[48]	Performance Analysis of ECC and RSA for Securing CoAP-Based Remote Health Monitoring System	✔	✔	×	✔	✔	×	×	×	–	2018	Springer
[49]	Multi-factor user authentication scheme for IoT-based healthcare services	✔	✔	✔	✔	✔	✔	✔	✔	Denial of service (DoS) attack, replay attack, impersonation attack, stolen verifier attack, stolen smart device attacks, man-in-the-middle attack, insider attack	2018	Springer

Table 1 continued

References	Title	Confidentiality	Integrity	Authentication	Authorization	Availability	Non-repudiation	Accountability	Anonymity	Prevent attacks	Year	Publisher
[50]	An Improved Lightweight RFID Authentication Protocol for Internet of Things	✔	×	✔	×	×	×	✔	✔	Replay attack, Impersonation attack, Modification attack, DOS attack	2018	Springer
[51]	An ECC-Based Algorithm to Handle Secure Communication Between Heterogeneous IoT Devices	×	×	✔	✔	✔	✔	✔	×	XSS attack, Injection input attack, DOS attack, Man in the middle attack	2018	Springer
[52]	AKAIOTS: authenticated key agreement for Internet of Things	✔	×	✔	×	×	×	✔	×	Eavesdropping attack, Impersonation attack, The denial-of-service (DoS)	2018	Springer
[53]	Achieving energy efficiency using novel scalar multiplication based ECC for android devices in Internet of Things environments	✔	x	✔	×	×	×	✔	×	–	2018	Springer
[54]	Three elliptic curve cryptography-based RFID authentication protocols for Internet of Things	×	×	✔	×	×	✔	✔	✔	Man-in-the-middle attack, Impersonation attack, replay attack, Tracking attack	2017	Springer
[55]	Secure Lightweight ECC-Based Protocol for Multi-Agent IoT Systems	✔	✔	✔	✔	✔	✔	✔	×	Replay, DoS	2017	IEEE

Table 1 continued

References	Title	Confidentiality	Integrity	Authentication	Authorization	Availability	Non-repudiation	Accountability	Anonymity	Prevent attacks	Year	Publisher
[56]	elliptic curve cryptography security in the context of internet of things	×	✔	×	×	×	✔	✔	×	–	2017	Other Journal
[54]	Elliptic Curve Based Cybersecurity Schemes for Publish-Subscribe Internet of Things	✔	×	✔	✔	✔	✔	✔	×	Man-in-the-middle of attack	2017	Springer
[57]	A secure ID-based signcryption scheme based on elliptic curve cryptography	×	✔	✔	✔	×	✔	×	×	Replay attack, man-in-the-middle attack	2017	Inderscience
[58]	A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers	✔	✔	✔	✔	✔	✔	✔	×	Replay attack, man-in-the-middle attack, Impersonation attack, Insider attack	2017	Springer
[59]	A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices	✔	×	✔	✔	✔	×	×	×	Replay, DoS	2017	Inderscience
[60]	Elliptic Curve Cryptography for Real Time Embedded Systems in IoT Networks	✔	✔	✔	✔	✔	×	✔	✔	Replay, DoS	2016	IEEE

Table 1 continued

References	Title	Confidentiality	Integrity	Authentication	Authorization	Availability	Non-repudiation	Accountability	Anonymity	Prevent attacks	Year	Publisher
[61]	Efficient RFID Authentication Using Elliptic Curve Cryptography for the Internet of Things	✔	×	✔	×	×	×	×	✔	Replaying attack and the server spoofing attack	2016	Springer
[62]	DCAPBAC: embedding authorization logic into smart things through ECC optimizations	✔	✔	✔	×	×	✔	✔	×	Replay attacks	2014	Taylor & Francis
[63]	Strong Security and Privacy of RFID System for Internet of Things Infrastructure	✔	✔	✔	×	×	×	×	×	–	2013	Springer
[64]	Shifting primes: Optimizing elliptic curve cryptography for 16-bit devices without hardware multiplier	✔	✔	✔	✔	✔	×	×	×	–	2013	Elsevier
[65]	A Secure Framework for OTA Smart Device Ecosystems Using ECC Encryption and Biometrics	×	×	✔	✔	×	✔	✔	×	Replay attack, man-in-the-middle attack, DoS	2013	Springer
[66]	Shifting Primes: Extension of Pseudo-Mersenne Primes to Optimize ECC for MSP430-Based Future Internet of Things Devices	✔	✔	×	✔	✔	✔	×	×	DoS attack	2011	Springer

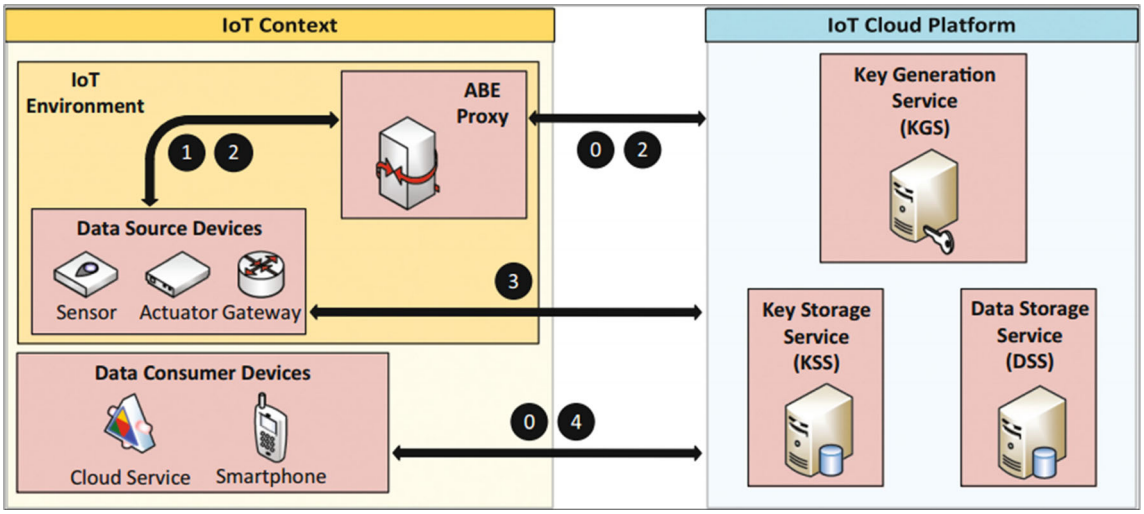

Fig. 8 Overview of CP-ABE architecture for IoT Cloud Platform [69]

A flexible keyword search mechanism for encrypted data to promote data retrieval in IoT is proposed in [71] that uses the reciprocal mapping of Lagrange polynomials technology to perform search inquiries over large encrypted texts. The proposed mechanism applies ABE technology to limit data access to authorized users. Finally, it enhances decryption at client side by outsourcing the decryption process, making it a good candidate in IoT scenarios.

ABE is a form of public key encryption where the information is encrypted under a Boolean formula (called access policy) which other parties must satisfy in order to decrypt the cipher text [72]. This cryptographic scheme is particularly useful on IoT since it simultaneously provides fine-grained access control and encryption.

A novel identity-based proxy re-encryption (IBPRE) has been proposed [73]. Cryptographic proxy re-encryption is a very useful primitive which is capable of transforming a cipher text under one public key PK1 into a new cipher text under another public key PK2 without private information leakage, while the two cipher texts are encryptions of the same message. Re-encryption schemes at first are constructed under the public-key encryption (PKE) scenario. While it is a powerful primitive naturally required in not only PKE but also other scenarios, various extensions from PKE to other advanced encryption schemes like identity-based encryption (IBE), ABE as well as functional encryption (FE) are needed as well.

IoUT (Internet of underwater things) is a new technique that is being widely used, though security and efficiency of using resources in the network are still an issue in such systems because it relies on working with smart things. In [74], a cloud-based scheme is proposed to reduce energy consumption and data exchange while providing for real-time monitoring and management of IoUT in different contexts. This is particularly interesting for smart cities to increase their efficiency and help them be really green. Results of stimulations showed that the proposed scheme has a better performance than existing systems in terms of security and privacy.

End-to-End security issue, which is mostly neglected in other IoT protocols such as CoAP and MQTT which rely only on security of DTLS, has been considered in [75] involving an IoT application, an IoT broker, and IoT devices, where devices are deployed on the boundary of the broker. Sensing data of devices in the area of the broker are collected and managed by the broker. The sensing data are used by the IoT application which is responsible for providing IoT services to users. In healthcare settings, security gains ever more importance because real-time healthcare services deal with sensitive information from medical records of patients. Encryption of sensitive date is done using a symmetric key and ABE. This framework also reduced costs of communication and computation.

Several researchers have introduced ABE approach and access controls in cloud computing environments for improving the protection of Web applications. Moreover, the established systems did not consider a massive number of devices as feature of IoT. In [76], an IoT encryption scheme based on context is suggested. Data owner conducts encryption and decryption by background extraction dependent upon identification. Every consumer can decrypt requested data only during the decryption process. Thus, even though there is a large amount of system, users may receive data in low overhead area.

ABE facilitates the application of fine-grained, unified access control dependent on a user's property or characteristics, drawing attention to the implementation of decentralized access control in large and complex networks such as mesh networks, IoT and cloud computing.

Table 2 Security factors in IoT based on algorithm ABE

References	Title	Confidentiality	Integrity	Authentication	Authorization	Availability	Non-repudiation	Accountability	Anonymity	Prevent attacks	Year	Publisher
[69]	Towards the CP-ABE Application for Privacy-Preserving Secure Data Sharing in IoT Contexts	✔	✔	✔	×	×	×	✔	×	Resistant to attack	2018	Springer
[70]	Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things	✔	×	✔	✔	✔	×	✔	✔	Replay attack	2018	Elsevier
[71]	Secure and flexible keyword search over encrypted data with outsourced decryption in Internet of things	✔	✔	✔	✔	✔	✔	×	×	Non-vulnerable to attacks	2018	Springer
[72]	Migrating Monitors + ABE: A Suitable Combination for Secure IoT?	×	✔	✔	✔	×	✔	✔	×	Non-vulnerable to attacks	2018	Springer
[73]	Identity-based re-encryption scheme with lightweight re-encryption key generation	✔	✔	✔	×	×	×	×	×	Non-vulnerable to attacks	2018	Taylor & Francis
[74]	A secure cloud-based solution for real-time monitoring and management of Internet of underwater things (IOUT)	✔	✔	✔	✔	✔	✔	×	×	DoS attack, Eavesdropping	2018	Springer
[75]	Secure IoT framework and 2D architecture for End-To-End security	✔	×	✔	×	✔	✔	×	×	Malicious broker, Eavesdropping, spoofing attack, Replay attack	2016	Springer
[76]	A Work in Progress: Context based encryption scheme for Internet of Things	✔	✔	✔	×	✔	✔	×	×	–	2015	Elsevier
[77]	New Model and Construction of ABE: Achieving Key Resilient-Leakage and Attribute Direct-Revocation	×	✔	✔	√	×	✔	×	✔	Non-vulnerable to attacks	2014	Springer

Nevertheless, the intruder will blow down the actual implementation of cryptosystems in open networks, and then obtain internal hidden states including pseudo-random number, internal score, and secret key to crack the device. In [77], Zhang first model a fine-grained attribute revocable (cipher text-policy) ABE in the presence of key leakage, and then give a concrete construction with security and resilient-leakage performance analysis. Their scheme is the first creator to possess the following property at the same time: (I) Support direct revocation feature, which does not influence the secret key of any other customer. (II) Tolerate the key to be partly exposed to suit the challenged cipher file. (III) Provide a primary maintenance method to enable consistent tolerance to leakages. Table 2 shows ABE-based security algorithms in IoT.

3.2.5 ABS

An articulate attribute-based signature scheme (EPASS) has been suggested for a novel ABS system that uses the attribute tree and communicates some strategy consisting of AND, OR threshold gates under the computational DH problem [78]. The IoT offers links everywhere, anywhere, anywhere, for which consumer privacy is fragile and methods of authentication that support regulation over attributes are essential. Therefore, a signature scheme is required that considers user privacy and implements a policy on attributes. Emerging attribute-based signature (ABS) schemes enable a resource requester to create a signature with policy-satisfying attributes without leaking out more details. Nonetheless, few current methods, under the traditional DH principle, at the same time accomplish an articulate strategy and stability. Users can not counterfeit signatures with characteristics that they do not own, and the signature offers guarantees that the document can only be supported by a person with sufficient attributes that fulfill the protocol, resulting in unforgeable capabilities. Legitimate signers, though, remain anonymous and are unique among all users whose attributes meet the regulation providing the signer with privacy attributes. Their solution provided enhanced performance compared to existing systems by rising the computing costs and signature scale.

3.3 Symmetric algorithms

Symmetric encryption applies the common key for both encryption and decryption of data. This method of encryption is secure and relatively faster. The main disadvantage of symmetric key encryption is the sharing of the key between the two communicating parties. An attacker can decrypt the data if he has access to the key. Symmetric key algorithms assure the confidentiality and integrity of data but do not guarantee authentication.

A symmetric encryption scheme $SE = (K^{sym}, E^{sym}, D^{sym})$ consists of three algorithms [40]:

- $K^{sym}(k)$: The key production algorithm takes as inputting the security parameter k and returning a symmetric key K, defined by $\mathrm{K} \leftarrow K^{sym}(k)$;
- $E_K^{sym}(m)$: The encryption algorithm takes as inputting the symmetric key K and a plaintext, $m \in M$ and outputting a ciphertext C, defined by $C \leftarrow \mathrm{E}_K^{sym}(m)$;
- $D_K^{sym}(C)$: The decryption algorithm takes as inputting the symmetric key K and a ciphertext C, and outputting the plaintext m, defined by $m \leftarrow D_K^{sym}(C)$.

Security on resource-constrained devices such as RFID tags and WSNs nodes can be provided based on lightweight block cipher algorithms.

3.3.1 DES

A stable DES-based protocol is proposed in [79] in which a DES algorithm is used to transfer data between users through sensor nodes without any safety loss. Compared with other cryptography algorithms, the DES algorithm provides security and takes less time to execute encryption and decryption operations. Results of the experiment revealed that the proposed mechanism took less time to do encryption and decryption.

3.3.2 AES

An AES-based Protection System for IoT Environments in Intelligent Grids is proposed [80]. The following sequence of steps was suggested to determine the validity of this coordination model: (1) testing of the IP compatibility. Firstly, the client's IP address submitting the request is checked in a server whitelist where each IP address is listed that is authorized to make encryption key requests to the server. All non-listed IP address links are denied. (2) Implement encryption algorithms. Through using the AES symmetric encryption algorithm to encrypt and decrypt messages sent between each node, and using digital signatures and verification through the asymmetric RSA algorithm, the secrecy of the information sent and retrieved by each node in the grid is incorporated. (3) Encryption of the communication channel. This can be achieved with a security certificate through the TSL / SSL program that allows encryption of all data moving through the communications channel. (4) Verification of the integrity of the channel of communication. To satisfy the data integrity criteria, HMAC was applied; this system operates with a message authentication method (MAC) to ensure that the

message sent on the way to its destination was not intercepted or changed by means of a hash function and a token. AES algorithm uses a single key for encrypt and decrypt the data. AES key length is 128, 192, and 256.

In [81], the focus was on securing agricultural data from hackers. Farmers are going to remote control devices especially in the field of agriculture, due to lack of manpower. To improve the reliability of an existing system, additional methods such as checksum formation, data segmentation, and data shuffling have been introduced extension of the AES 128-bit encryption method to give greater protection. They measured the time and processing time for both encryption and decryption with and without using the suggested form of encryption to protect farm records.

It was suggested to introduce and evaluate cryptographic ciphers in FPGA on the basis of AES [82]. The 128-bit key is sub-divided into 16-bits sub-blocks, the first 96 bits for the initial round are the six K1 to K6 sub-keys. So, 32-bits (i.e. 97–128) of the primary key is unused after the first round.

A lightweight shared authorization system has been developed for an IoT environment's real-world physical objects [83]. It's a payload centered encryption system that uses a clear four-way handshake method to check participant entity identities. The real-world artifacts connect with one another using the interface paradigm client–server. Their suggested scheme uses the Constrained Application Protocol (CoAP) lightweight functionality to help clients to identify energy-efficient resource residing on the server. They used AES for the establishment of a protected resource observation session with a key duration of 128 bits. The scheme offer efficient computations, requires less overhead and, simultaneously, protects against attacks such as resource depletion, Denial-of-Service, replay and physical exploitation.

AES algorithm to ZigBee protocol in IoT was suggested in [84]. The current implementation status at home and abroad is first outlined to research the use of the ZigBee protocol in the IoT protection algorithm and ZigBee technology is implemented in depth. After that, the AES-128 algorithm theory is evaluated and the decryption algorithm measures are modified, so that the decryption method becomes symmetrical in form and encryption algorithm. Alternatively, the AES-128 encryption and decryption method are implemented using C technology. Depending on the usability and low-cost characteristics of the ZigBee platform, the two optimization algorithms are designed and implemented based on the performance of the protection algorithm based on the simplicity and efficiency study. Review and test results demonstrate that the two optimization algorithms are quicker and more complicated than the UN optimized algorithm. In sum up, the outcome comparison shows that the speed and difficulty of the optimization algorithm for the round process is higher than that of the optimization algorithm for column obfuscation. The emergence of IoT and its implementations in many areas such as sensing, healthcare and manufacturing has culminated in an exponential increase in digital data, which needs to be shared through vulnerable networks.

A speed-up version of the SIMON algorithm has been proposed in [85] for software implementation based on AES. The improvement benefited from interesting features contained in a separate algorithm named SPECK to change the original work of SIMON, which obtained appealing performance. The modification resulted in an increase of interesting performance measures, making SIMON with block sizes 32, 48, 64, 96-bits win between AES 128/128. The changed SIMON with 32, 48, 64, 96-bits block sizes displayed remarkable speed-up compared to the original SIMON, where some of them were found to be slower than AES. The integrated SIMON with all the block models indicates a percentage increase ranging from 20 to 26% with the exception of block size 64 displaying a percentage increase similar to 13 percent. The deployment study looked at both aspects of applications operating the algorithm, i.e. execution time as well as resource use.

Hu et al. [86] suggested grouping of data with symmetrical AES encryption to protect anonymity. In addition, we provide the machines with a One-time Pad to improve stability. We use homomorphic encryption scheme to protect private information for secure communication between devices and their corresponding aggregator. The aggregator will achieve the data aggregation outcome in a residential area in the proposed systems, without knowing the actual results of each unit. Neither the curious and collusive devices can infer data about private use of other devices. The scheme consists of five phases: (I) Division of data: (II) encryption and distribution, (III) decryption and uncertainty, (IV) encryption and reporting; (V) authentication and aggregation.

LORAWAN, as defined by the LORA Alliance as a Long-Range Wide Area Network standard, is a low-power and long-distance networking protocol appropriate for IoT settings. LORAWAN eliminates contact capacity by establishing multiple transmitting latencies for different end devices; however, AES does not recognize the encryption ability of its end device. A highly secure yet low power consumption communication system for the LORAWAN, called the Protected Low Power Communication (SELPC) process, is suggested in [87] to further minimize the data encryption power of end devices by the AES encryption cycles. Encryption key and D-Box upgrade protocol are provided in the SELPC to increase the security level and simplify the AES encryption method to further reduce power demand. The findings of the study

Table 3 AES-based security algorithms in IoT

References	Title	Confidentiality	Integrity	Authentication	Authorization	Availability	Non-repudiation	Accountability	Anonymity	Prevent attacks	Year	Publisher
[80]	Security Scheme for IoT Environments in Smart Grids	√	√	√	√	√	×	×	×	–	2019	Springer
[81]	Methodology to Secure Agricultural Data in IoT	×	×	√	√	√	×	×	×	Prevent of hackers	2019	Springer
[82]	Implementation and Analysis of Cryptographic Ciphers in FPGA	√	√	×	×	×	√	×	×	DoS attack	2019	Springer
[83]	A payload-based mutual authentication scheme for Internet of Things	×	✔	✔	✔	✔	✔	×	✔	Resource exhaustion, Denial-of-Service, replay and physical tampering	2019	Springer
[84]	Security algorithm of Internet of Things based on ZigBee protocol	✔	✔	×	×	×	✔	×	×	Malicious broker, Eavesdropping, spoofing attack, Replay attack	2018	Springer
[85]	Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications	✔	✔	✔	✔	✔	✔	×	×	Resistant against difference attack	2018	Springer
[86]	An Efficient Privacy-Preserving Data Aggregation Scheme for IoT	✔	✔	✔	✔	×	×	×	×	External Attack, Internal Attack, Collusion Attack	2018	Springer
[87]	AES-128 Based Secure Low Power Communication for LORAWAN IoT Environments	✔	✔	✔	✔	✔	✔	✔	×	Known-key, replay, and eavesdropping attacks	2018	IEEE

Table 3 continued

References	Title	Confidentiality	Integrity	Authentication	Authorization	Availability	Non-repudiation	Accountability	Anonymity	Prevent attacks	Year	Publisher
[88]	Efficient and High-Speed FPGA Bump in the Wire Implementation for Data Integrity and Confidentiality Services in the IoT	×	✓	✓	✓	✓	✓	✓	×	DoS attack	2017	Springer
[89]	Encryption Node Design in Internet of Things Based on Fingerprint Features and CC2530	✓	✓	✓	×	×	×	×	×	–	2013	IEEE

reveal that the SELPC will reduce the encryption strength by up to 26.2 per cent compared to the traditional AES. The SELPC can also survive three threats including known-key, replay, and eavesdropping assaults, and is practically useful in LORAWAN IoT settings.

To provide IPSec, the core symmetric cryptographic and hash functions that are needed for its operation must be introduced. In this job, it applies the AES and the SHA-3 (Secure Hash Algorithm-3) [88]. The AES design allows use of the new Xilinx FPGAs BRAM (Block Memory) and LUT memory tools. The AES key generation scheme is installed as a separate module and for each respective round provides the round keys to the AES core. Only 56 clock cycles are required to completely implement the AES. The cryptographic hash function, SHA-3 is implemented to provide the data integrity security service. SHA-3 is used because it is the most reliable and freshly chosen cryptographic hash function available to date.

IoT sensing node is commonly designed as a core chip with TI's CC2530 in [89]. A pair of encryption nodes, encryption sensing node and access control node are designed based on AES algorithm, and CC2530′s AES protection coprocessor is used to ensure the security of sensitive data transmitted between the nodes, and access authorization control for the sensing node. Hash function generates the 128-bit key for AES whose inputs are fingerprint feature data coming from the fingerprint module. Different data on fingerprints can generate numerous keys to form a key bank. The administrator can assign these keys to different nodes to form a sub-key register, depending on the access authorization for different users. Keys can be dynamically changed at sub-key branch. The encryption node that has been built will handle the access permission and enforce user authentication. Encryption node framework and hardware design strategies are described. Experiments are performed on data transmission between nodes. The results show that the encryption nodes must accomplish wireless security communication for the data of the network, in order to ensure its reliability. Table 3 shows AES-based security algorithms in IoT.

3.3.3 Blowfish

Bruce Schneier created blowfish block cipher in 1993 [90]. It uses a 64-bit fixed block, with a key-length ranging from 32 to 448 bits. It also uses large S-boxes, depending on the switch. Compared to DES, it has a cipher structure with a 16-round Feistel. It is an open source algorithm that wasn't cracked yet. It is also one of the quickest public-use ciphers.

Cloud computing gave the information technology sector tremendous potential changes and outstanding prospects. In most networked transactions, it is particularly

useful. Data security issues associated with cloud computing common issues. Information is secure if it meets the three requirements of confidentiality, integrity and availability. Data is safe if the three requirements, including security, honesty and availability, are met. Security in cloud computing is gained by authentication. Symmetric algorithms demonstrated overwhelming popularity in cryptography, especially the Blowfish algorithm. A Modified Blowfish Algorithm Approach using Shuffle Algorithm was applied in [91], and the encryption, decryption speed, and throughput were tested. The Modified Blowfish Algorithm Approach based on S-box permutation using Shuffle Algorithm has been attempted. The result shows the higher the accuracy, the greater the file encryption capacity.

A comparison of the Blowfish Algorithm's serial and parallel implementations was made in [92]. The concurrent architecture was then checked with different number of cores over networks. Implementation integrates a parallel execution of the function F along with the division of the data into 64-bit chunks and the parallel processing. Results show that parallel implementation delivers better efficiency than serial implementation, and this implementation offers a higher throughput when the number of cores is expanded, allowing implementation effective in situations where a large number of cores are present.

In [93] a Cryptographic Ciphers Performance Assessment on IoT Devices was done. The numerous protection methods such as Blowfish, Blowfish, DES, 3DES, AES, RC2, RC4, and ChaCha20 have been tested. On the IoT systems these ciphers are checked by running them on different file sizes varying from 1 MB to 128 Gb. Blowfish algorithm has the highest speed among all the ciphers.es chains.

In [94], Suresh and Neema discussed security challenges and IoT protection frameworks. In the unsecured channel, which connects different IoT nodes or IoT nodes and WSN nodes, a major share of the same occurs by analyzing different security problems associated with IoT. Cryptographic methods may be used to provide protection for the transmission of information in the network layer. Of all the cryptographic algorithms, the Blowfish algorithm is the best in terms among execution time, memory use, performance, power consumption and reliability and is therefore ideally adapted for IoT purposes. Software installation of the initial and improved Blowfish was performed using Verilog HDL in Xilinx Virtex-5 XC5VLX50 T FPGA. The updated version displayed an increase of 16.9% and 18.7% in terms of encryption period and throughput as compared with both.

In data communications information security has become an important issue. One way of ensuring data security is by using cryptographic process. Cryptography is a way of storing the information so that the other side does not decrypt the information. A significant amount of computer resources is used to execute the cryptography. Different blowfish algorithm implementation framework for data encryption sent from an IoT physical network that has IP-based data can be introduced. In [95], FPGA implements blowfish algorithm using VHDL programming language and controls the amount of FPGA tools used. The blowfish algorithm is tested for device stability by computing such outputs of metrics such as protection, encryption time, avalanche effect, and throughput from multiple test scenarios. The testing showed that when implemented in FPGA, blowfish algorithm provided good performance and showed a good alternative to proposed IoT as network security.

3.3.4 RC4

RC4 algorithm for encryption and decryption on IoT was introduced in [96]. In this paper the security and privacy concerns of industrial IoT are assessed, then the common security risks and attacks are studied, and several forms of fluent security measures are used, bringing forward the Fingerprint encryption security program. RC4 algorithm characterized by the algorithm is quick, easy, and the main duration is variable, 1–256 bytes (8–2048-bits) variable range. The software incorporates the fingerprint identification system, PDF417 code and RC4 encryption process, matching the data to be decoded via the fingerprint. Since the fingerprint knowledge is special, whether the match's performance will dictate whether the project is by itself, and then settle on the next move, preserves the security and privacy of the individual to a great extent.

RC4 is a stream symmetric algorithm characterized by fast encryption/decryption, low resource consumption, easy implementation, less special, and temporal complexity. Stream ciphers continuously process inputs and sequential encrypt data. Though block ciphers are more common, stream ciphers are occasionally a better choice. The key length in RC4 is 8–2048-bits. It is based on a random permutation that generates a pseudorandom stream of bits. RC4 is composed of Key Scheduling Algorithm (KSA) and Pseudo-Random Generation Algorithm (PRGA) that run sequentially. The encryption key is generated by KSA and the pseudorandom string is generated by PRGA which yields a plain XOR text. Encryption is done only by XOR operator. RC4 is deployed by the security protocol of transmission layer to prevent data leakage between servers and users. However, it was designed three decades ago and is vulnerable to new cyberattacks.

In KSA, a key K of size k (≤ 256) bytes is given as input and formation a state array S of size N (= 256) to determine over Z_N. The key K is implicitly supposed to be

Key Scheduling Algorithm (KSA)

Input: Secret key *K*
K: key length
Output: Internal state *S*
1) $j = 0$;
// State Initialization
2) **for** $i = 0$ to $N - 1$ **do**
3) S [i] = i;
// State Randomization
4) **for** $i = 0$ to $N - 1$ **do**
5) $j = (j + S[i] + K[i \bmod k]) \bmod N$;
6) Swap (S [i], S [j]);

Pseudo-Random Generation Algorithm (PRGA)

Input: Internal state *S*, generated by KSA
Output: keystream *Z*
1) i=0;
2) j= 0;
3) **for** *each new message byte* **do**
4) $i = (i + 1) \bmod N$;
5) $j = (j + S[i]) \bmod N$;
6) Swap (S [i], S [j]);
7) Z= S [(S [i] + S [j]) mod N];
8) output *Z*;

Fig. 9 The KSA and PRGA in RC4

stretched to size N = 256 bytes by iterate the same key (if k does not divide N, then the last iteration is imperfect). The PRGA uses the scrambled permutation S to produce pseudo-random bytes $Z1, Z2, \ldots$, from state S, that are bitwise XOR-ed with the next plaintext/ciphertext byte to carry out encryption/decryption. The KSA and PRGA are defined in Fig. 9.

3.4 Hybrid

A healthcare protection paradigm has been developed to protect a transfer of medical data in IoT environments [97]. The model suggested consists of four continuous processes: (1) the data of the sensitive patient is authenticated using a new hybrid encryption scheme built from both AES and RSA encryption algorithms. (2) The encrypted data is hidden on a cover image using either 2D-DWT-1L or 2D-DWT-2L and a stego image is made. (3) It extracts embedded data. (4) For the retrieval of the original data, the recovered data is decrypted. The proposed model was initiated by encrypting the secret data; it then hides the result using 2D-DWT-1L or 2D-DWT-2L in a cover image. To hide various text types, both color and gray-scale pictures are used as cover images. The efficiency of the proposed system was assessed on the basis of six statistical parameters: peak signal-to-noise ratio (PSNR), mean square error (MSE), bit error rate (BER), structural similarity (SSIM), structural quality (SC) and correlation. In the case of color images, the PSNR values ranged from 50.59 to 57.44 and with the gray scale photos from 50.52 to 56.09. For the color images, the MSE values ranged from 0.12 to 0.57, and for the gray photos from 0.14 to 0.57. For both images, the BER values were negative, while for both images, SSIM, SC, and correlation values were those.

A privacy-preserving and user-controlled approach for IoT data sharing has been suggested focused on ABS and CP-ABE [98]. The proposed model involved the following steps: Using block chain and several attribute-based cryptosystems, the architecture can achieve privacy-preserving, user-self-controlled data sharing, and decentralization. ABS and CP-ABE have fine grained access control capabilities. IoT data were initially secured (e.g., AES). Next, smart contract technology is combined with an AES to understand the fine-grained sharing. The access policies are set on the encrypted key (the encrypted key is encrypted by attributes, ABE) to determine who can get this encrypted key to decrypt the text in the cipher.

A hybrid model has been suggested to ensure the data's stability, validity and legitimacy during transmission [99]. The software is applying two highly powerful cryptographic algorithms; SHA-1, hash generation algorithm, and AES method for message encryption and decryption. This paper also addresses several other cryptographic algorithms, and why they choose AES and SHA-1. It uses AES and SHA-1 as an 8-bit architecture which reduced hardware resource consumption, thereby reducing the cost to a greater extent. RFID demands low power consumption and low cost, which their proposed model greatly provides.

In [100] a two-way IoT encryption authentication mechanism based on existing Internet standards has been suggested, precisely the Datagram Transport Layer Encryption (DTLS) protocol. Through depending on a proven norm, it is possible to reuse existing architectures, engineering techniques, and security infrastructure which

Table 4 the encryption and decryption steps based on RSA-AES

Sending cycle	Receiving cycle
Washing Process: In which, they washed (encrypted) the one-time pad key portion using AES algorithm and a cryptographic random session key using ANSI X9.17 standard generator	Key Extraction Process: In which, they extracted the encrypted AES session key using the RSA public-key algorithm
Key Exchange Process: In which, they encrypted the AES session key using the RSA public-key algorithm	Washing Process: In which, they washed (encrypt) the one-time pad key portion using AES algorithm and the extracted AES session key
Digital Envelope Process: In which, they encrypted the message (file) with OTP, and completed message formatting to be ready to transmit to the receiver supported with electronic digital signature of the sender	Digital Envelope Opening Process: In which, they opened message to extract the different message segments. They decrypted the receiving message (file) and validate the digital signature of the sender and the integrity of the message

allows easy security uptake. The suggested encryption scheme utilizes two algorithms for the public key cryptography, RSA and ECC, adapted to the heterogeneous existence of IoT apps. The proposed two-way authentication approach is designed to work on common connectivity stacks that offer Low Power Wireless Personal Area Networks (LoWPANs) UDP / IPv6 networking. In the sense of a system architecture, a conceptual implementation of DTLS is provided here, and the viability of the scheme (low overheads and strong interoperability) is illustrated by comprehensive assessments on the DTLS-supporting framework OPAL as a cluster-head with children from specific IoT hardware platform.

A modern RSA-based Cipher-Text Policy (CP-ABE) system with Constant Size Secret Keys and Cipher-Texts (CSKCs) and $O(1)$ Time Complexity for each decryption and encryption has been introduced in [101]. Their scheme is then proven to be safe against a chosen ciphertext opponent and an effective approach with descriptive AND gate control structures. Since most mobile devices are battery-limited, key design specifications should include a constant size secret key and constant size ciphertext in a CP-ABE system, as well as a cost-effective encryption and decryption process. The suggested scheme is thus ideal for implementation on mobile devices which are battery-limited. CP-ABE is a feasible solution for cloud implementation in particular, since a cryptographer will compose the access policy so that only authorized users can decode and access the data.

A new proposed cyber security scheme for IoT has been introduced to promote additional level of security by including a new level of key-hierarchy [102]. We discussed the closed system framework, the suggested plan, the services provided, message type sharing and the four level core hierarchies employed. They used application level encryption to selectively secure information to conserve power and improve the processing pace that is useful for IoT and wireless applications. Based on the strength of symmetric algorithms such as RSA and AES algorithms, the design of the suggested scheme is addressed. The integration of a single pad with the RSA and AES cryptosystems enhances the protection of the single pad key through the washing process. The scheme suggested offers four levels; of key-hierarchy. The first is the secret to a single board. It is used after the Washing process to encrypt the post. The second of these is the AES session key used in the washing process. The third one is the default RSA key used to encrypt the AES session keys and the OTP reference. The fourth is a transfer phrase used to secure private key encryption. The proposed cryptosystem combines the one-time pad, called the theoretically unbreakable Vernam cipher, with standard encryption algorithms, the public-key RSA algorithm, and the secret-key algorithm AES. Table 4 shows RSA-AES-based encryption and decryption stages.

In an IoT environment, billions of users connect their devices to the cloud to utilize the services of it. Cloud enables these IoT devices to store the data on the cloud servers. In order to provide a secure access, user authentication is required. Therefore, hybrid method for authentication is proposed in [103] to promote secure access of data. A biometric authentication is a more secure way of storing and accessing the data from the cloud. The proposed paper discussed about the Iris based authentication to access the data from the cloud through any authorized IoT device. The authentication algorithm proposed in this paper is the hybrid application of Blowfish and RSA Algorithm which generates a binary template for an iris. A two-stage authentication is provided, thus enhancing more security and reliability.

A modern ECC-based authentication protocol for radiofrequency recognition was introduced in [104] to remove vulnerabilities. We also use elliptic curve DH (ECDH) key agreement protocol to create a temporary mutual key used to encrypt the messages subsequently transmitted. The protocol achieves a range of protection properties such as shared authorization, encryption, secrecy, forward security, position safety, man-in—the-

medium attack resistance, replay attack resistance and impersonation attack resistance. Evaluation of the results reveals that their suggested approach is more effective and requires much less time compared to others.

In [105] the remote monitoring system performed data cleaning and encryption technology between server and mobile terminal. The authors investigated the Sorted Neighborhood Method and improved its performance for networking data transmission in remote monitoring systems. It identifies and deals with the collected duplicate data in the data source to reduce the connectivity burden between the device client and the server; the cleaned data is encrypted with the RSA and MD5 algorithms to enhance system security and avoid application data from leakage. MD5 uses hash feature, which is used to classify key in areas of digital signatures and password protection, compact byte string of random duration to a certain range of large integer numbers. MD5 converts arbitrary-length byte array into a broad 128bit integer. MD5 is an immutable string exchange, in the sense that even if one has knowledge of the source code and the method definition, the MD5 value cannot be translated back to the original string. Based on these characteristics, MD5 is highly secure and is thus often applied in the domains where top-secret measures are required. We conducted experiments, the findings of which demonstrate that their approach to data cleaning and encryption will significantly increase data transfer rate between server and mobile device, resulting in better solutions to practical problems.

Proposed Information Encryption and Transmission Software for IoT Protection Cotton focused on DES-RSA [106]. This paper describes the knowledge information analysis in the cotton warehouse area in terms of the IoT transmission protection. A combination of DES and RSA methods is used to ensure the security and speed of encryption and decryption of information, i.e. DES key is encrypted with RSA based on plaintext data encryption by DES. Set M be plaintext; C is encrypted as a cipher text; K_D is key of DES encryption and decryption, K_{E2} is a public key of RSA, K_{E1} is a private key of RSA; DES's encryption process is denoted as f_1, the decryption's process is denoted as f_1^{-1}; RSA's encryption process is denoted as f_2, the decryption's process is denoted as f_2^{-1}. DES is ideal for large volume data encryption; DES encryption and information decryption will hold the output. RSA encrypting the DES-generated keys, even if a hacker steals critical data, the hacker's gotten data is garbled. DES-RSA stage shall be as follows:

- The transmitting end produces the DES algorithm key KD, encrypts the plain text M to construct cipher text C1
- Encrypts DES cipher-text algorithms using the public key KE2 of the receiving end of the RSA to produce cipher-text C2
- Send C2 cipher text and encryption key through network to the receiving terminal C2
- The receiving end decrypts the sent cipher-text C2 with its own RSA decryption key KE1 and gets the initial DES cipher-text C1; because DES encryption and decryption key are similar, cipher-text C1 is encrypted with DES key KD to retrieve the plaintext M sent by the sender.

The gateway for security is installed between data center servers at the central level and the local machine cotton repositories, the design of the data transfer framework.

Hybrid cipher algorithm is easy to calculate and key distribution, fast speed, AES advantage and ECC hybrid encryption algorithm is easy to understand and implement, with high security [107]. It is suggested to identify and protect the security of the authenticity and transmission of data sources in the IoT-based information security transmission system to ensure that information, confidentiality and integrity cannot be denied. Hybrid Cipher Algorithm in non-symmetric cryptography and symmetric cryptography in one, with high security and fast speed, small storage space, more fitting in such a limited environment for IoT.

A lightweight, non-coupling ECC-based ABE system is introduced for resource-constraint Unit IoT-based applications to tackle secure communication and cipher-text access control [108]. ABE is a popular solution in the distributed environment such as IoT to achieve secure data transmission, storage, and sharing. The latest ABE systems, though, are based on costly bilinear matching, which renders them unsuitable for resource-constrained IoT implementations. A lightweight, ECC-based no-pairing ABE system is introduced in this paper to tackle the security and privacy problems in IoT. Instead of bilinear DH assumption, the reliability of the proposed scheme is based on the ECDDH assumption. The comparative analyzes with the current ABE systems was rendered in depth by explicitly deciding the parameters and specifying the indicators for calculating the contact overhead and the numerical overhead. The results show that the new system has increased quality of implementation and low cost of contact. Additionally, it's also discussing its limitations and improving directions.

Certificate-less cryptography seeks to merge the benefits of public key cryptography and identity-based cryptography in order to avoid the issue of certificate administration and key scanning. In [109], the ECC's novel certificate-less public key encryption scheme over the loop, whose protection is based on the assumption of toughness of the Bilinear DH problem and factoring the large number as in

an RSA protocol. In fact, since our system needs only one decryption pairing process, it is considerably more effective than other similar schemes. In fact, they are also introducing a protocol based on their encryption system to secure the secrecy and privacy of knowledge in the IoT scenario with resource nodes limited. Table 5 compares hybrid encryption algorithms for IoT security.

4 Discussion

IoT is a contemporary system that has the ability to connect all real-world objects/things around us and allocate a unique ID to connect to the Internet. It ID lets the consumer quickly get the data from the artifacts without requiring direct human-to-thing activity to a web data connection. The word IoT essentially implies that connectivity between objects is used through the standard Internet protocol. Often, the term can be entrusted as the Web of All. This domain's success is due to the fact that this IoT device conveniently works in the Internet infrastructure. The main aim of this domain is to encourage us to gradually connect things around us regardless of the time, venue, and person using any network and service. This comprises of environmental monitoring, network maintenance, energy conservation, home and office control, housing, medical and health-care services, and a particularly aggressive smart city program. Via national networking, smart cities can enclose all devices within the city into one network. The groundbreaking approach can now be incorporated in the implementation of daily tasks in the workplace, in households and almost anywhere to achieve better results with minimal work.

Like any program, it is necessary to secure the public IoT network against common opponents such as spammers, hackers and malware [110]. An opponent applies to any unauthorized party that intrudes into the system in order to discourage legitimate users from achieving their anonymity, honesty, and data quality goals. Attacker can attempt to access secret data, exploit the data in the network, fake a lawful sender or receiver's identity, and many more. That segment would outline the potential threats to data stored on the IoT platform by the consumers and critical safety criteria. IoT networks experience the same collection of similar threats that any traditional network might encounter. Nevertheless, the IoT servers become a convenient and tempting option for the attackers due to the huge amount of data that is being held on the IoT servers. Those risks / attacks may originate with their adversary models from different entities. The threats unique to IoT are as follows:

Eavesdropping: This attack refers to the illegitimate interception of a two-way communication. Such attacks can occur when it is out of curiosity that the cloud service provider accesses data stored on the server. Such threats are dangerous as they are hard to identify and unknowingly store sensitive data on the file, such as passwords [111].

Integrity: Integrity assault on data integrity happens when an intruder tries to alter or manipulate data without owner's permission. The attack usually takes place via malware program which deletes or modifies a smart device's contents.

Denial attack: One of the negotiating actors in this assault rejects either any or some component of the communication functions.

Denial of service: This attack occurs when a cloud server is inundated with a huge number of requests for resources that it cannot manage.

Replay: Such an attack occurs when the hostile party spies on the internal contact between the two parties. The malicious entity collects the authenticated information, such as shared session key, and then attempts to contact the receiver with that key later on. The attacker simply replays the eavesdropped message.

Impersonation: In this assault, the defendant tries to impersonate a legal entity and seeks to interact as a valid individual with the other entity [112].

Stolen verifier: In such assaults, the intruder succeeds during capturing critical server knowledge either from the latest sessions or from previously successful ones.

Insiders: These attacks occur when the intruder is a known party that has allowed access to the network and also has full knowledge of the infrastructure underlying it.

Man-in-the-middle: These attacks occur when the intruder may secretly relay and also alter the connection between two people that believe they interact with each other [112].

Clone: An adversary can capture a sensor node during clone attack and copy its information to another node known as cloned node. This cloned sensor node can then be mounted to collect network information. The competitor may also insert false information, or exploit the information that passes across cloned nodes. The prevention of unintended interference and replication is not feasible with regular physical surveillance of nodes. So effective and rapid detection schemes are needed to fight these attacks [113].

RSA and ECC for cryptographic applications are the most common and effective forms of public key encryption. Yet, in recent years, ECC has been adopted in the disruptive communication technologies sectors by increasing wireless applications like IoT. ECC provides high cryptographic security relative to RSA in terms of key

Table 5 A comparison of hybrid encryption algorithms for IoT security

References	Title	Hybrid algorithms	Confidentiality	Integrity	Authentication	Authorization	Availability	Non-repudiation	Accountability	Anonymity	Prevent attacks	Year	Publisher
[97]	Secure Medical Data Transmission Model for IoT-Based Healthcare Systems	AES-RSA	✔	✔	✔	✔	✔	×	×	×	–	2018	IEEE
[98]	BaDS: Block chain-Based Architecture for Data Sharing with ABS and CP-ABE in IoT	ABS-ABE	✔	×	✔	✔	✔	×	×	✔			
	Impersonation Attack, Collision Attack, Man-in-the-Middle Attack, Link Attack	2018	Springer										
[99]	A hybrid cryptographic algorithm based on AES and SHA-1 in RFID	AES-SHA1	✔	✔	✔	✔	✔	✔	✔	✔	Resistant to attacks	2018	Other Journals
[100]	Two-Way Authentication for the Internet-of-Things	RSA-ECC	✔	✔	√	×	×	×	×	×	Man-in-the-middle attack	2017	Springer
[101]	Expressive CP-ABE Scheme for Mobile Devices in IoT Satisfying Constant-Size Keys and Ciphertexts	RSA-ABE	✔	✔	✔	✔	✔	✔	×	×	Resistant to attacks	2017	IEEE
[102]	A New Hybrid Cryptosystem for Internet of Things Applications	RSA-AES	×	✔	✔	✔	✔	×	×	×	–	2017	Springer

Table 5 continued

References	Title	Hybrid algorithms	Confidentiality	Integrity	Authentication	Authorization	Availability	Non-repudiation	Accountability	Anonymity	Prevent attacks	Year	Publisher
[103]	A Hybrid Approach for Secure Iris-Based Authentication in IoT	Blowfish and RSA	✔	✔	✔	✔	×	×	×	×	–	2020	Springer
[104]	A secure ECC-based RFID mutual authentication protocol for internet of things	ECC-DH	✔	✔	✔	✔	✔	✔	✔	✔			
	Impersonation attack, Replay attack	2016	Springer										
[105]	Data Encryption for Remote Monitoring System Based on Internet of Things in Mobile Mode	RSA-MD5	✔	✔	✔	✔	✔	×	×	×	Resistant to attacks	2015	Springer
[106]	Data Encryption and Transmission Technology for Cotton of IoT Security	DES-RSA	×	✔	✔	✔	✔	×	×	×	–	2015	Springer
[107]	A Mixed Encryption Algorithm Used in Internet of Things Security Transmission System	AES-ECC	✔	✔	✔	×	×	×	×	×	Dos	2015	IEEE
[108]	A lightweight attribute-based encryption scheme for the Internet of Things	ECC-ABE	✔	×	✔	✔	✔	×	×	×	Resistant to attacks	2015	Elsevier

Table 5 continued

References	Title	Hybrid algorithms	Confidentiality	Integrity	Authentication	Authorization	Availability	Non-repudiation	Accountability	Anonymity	Prevent attacks	Year	Publisher
[109]	Certificateless Public Key Encryption Scheme with Hybrid Problems and Its Application to Internet of Things	ECC-RSA	✓	✓	✓	✓	✓	×	×	×	Resistant against		
difference attack	2014	Hindawi											

sizes, high protection and good performance. In fact, ECC is appealing to fundamentally resource-restricted areas such as storage, memory, power consumption, transmitting and computer-specific CPU architectures. ECC can offer a higher level of safety than traditional cryptosystems such as RSA, for example, the level of security provided by ECC with 160–256 bits, which is equivalent to RSA security with 1024–3072 bits level of security.

In the public key cryptography environment, ECC performs better than other protocols such as RSA in terms of key sizes, power or energy consumption, performance and memory specifications. For this purpose, ECC is favored for resource-critical applications, especially in wireless communication systems. Using other traditional symmetric key or secret key cryptography techniques such as the AES algorithm, verification, code signatures, and key agreement systems are difficult to deliver. ECC seems to be the preferable solution for stable IoT implementations, based on the comparisons made above. In fact, public key can be exchanged with insecure networks that can be used to encrypt data, however private key must be kept secret, so private key identifying and decrypting knowledge from the public key cryptosystem is hard to find.

ECC is a type of public key cryptography that can be used in restricted devices to achieve a high level of security. Compared with other asymmetric techniques already in use, ECC needs small keys and guarantees high safety. Security levels are more important for greater key sizes, for example, a 256-bit symmetric key has to be encrypted using more than 15,000-bit RSA, while a 512-bit asymmetric ECC can provide equivalent protection. ECC with smaller key size makes cost savings in terms of the necessary memory and processing power. This makes ECC highly recommended for the design of lightweight and quicker cryptographic operations that can work well on restricted tiny chips. Because of this smaller amount of heat is generated, and less processing power is used, which makes it highly desirable for use in resource-constrained applications. When addressing Elliptic curve cryptography, it could be concluded that ECC provides shorter keys, lower use of central processing unit (CPU) and lower use of memory for the same protection power. ECC presented the mathematical history, curve forms, the method for encryption and decryption, and different implementations.

The principal reason for using the ECC is the switch's relatively modest scale. For cases where processing power, power consumption, and memory capacity become limited Elliptic Curve cryptography attributable to only smaller, quicker, and more efficient cryptographic keys, the key size is optimal. The ECC security system is best suited for wireless communications, such as mobile phones and smart cards, personal information such as financial transactions or some classified medical reports, confidential data where

protected data is the main consideration. The ECC framework is used to provide an effective RFID authentication system as it can offer enhanced security with limited key size. Since key size is small, the computational power needed is also relatively low. Since ECC authentication schemes require low processing, RFID tags can be implemented as relatively less computational capacity is required.

Some tools and network devices such as the RFID, cellular sensor networks, and cloud computing were used in the IoT to extend the functionality of the IoT. The RFID system has drawn worldwide attentions from various fields as an important building block of IoT. During the Second World War the RFID system was developed as an effective automated recognition and data capture tool. Use radio waves, it could distinguish various objects, including products and livestock. The RFID system has many benefits as compared to traditional barcode technology [114]: (1): providing both read and write capabilities; (2): providing synchronous reading of many tags; (3): no line-of-sight communication needed. ECC is extremely secure, quicker and easier to handle main. While ECC is deemed safe, RFID is too restrictive to enforce. ECC is very difficult because it depends on complicated mathematical computations, and this difficulty requires high power that the RFID device can not satisfy. Table 6 compares encryption algorithms in IoT environments.Kindly check and confirm the layout of Table 6.We were confirmed.

General data encryption can be enforced at three connectivity levels: path encryption, node encryption, and end-to-end encryption. For any innermost node in encryption, the message received from the previous link will be decrypted into plaintext and the plaintext will then be encrypted into ciphertext using the secret key of the next link. Nevertheless, unlike path encryption, node encryption does not require messages in plaintext form to be stored in a network node. Hence it can provide strong network data coverage. The code is not decrypted when using end-to-end encryption until it is transmitted to the target. Because messages are always present as ciphertext throughout the transmission, information leakage doesn't occur. Data encryption algorithm is classified into two categories: symmetric encryption algorithm and public key encryption algorithms. Since the computing power and storage space of the sensor nodes are both small, the computational complexity and energy consumption of the asymmetric encryption algorithm makes it difficult to extend it to WSNs. Symmetric encryption algorithm is commonly used in WSNs owing to its simple calculation and small amount of computation. In a symmetric encryption algorithm, the message authentication code is usually used for authentication, which increases the communication load, and requires more storage space, causing extra power consumption.

4.1 Physical layer security

The physical layer has two highlight features for data security compared to cryptography algorithms. First, physical layer security methods do not depend on computational complexity, which implies that the attained level of security will not be compromised even if the unauthorized smart devices in the IoT network have powerful computational capabilities. Unauthorized devices have insignificant computational capabilities for hard mathematical problems. Second, physical layer security methods have a high scalability. In the IoT network, devices are always connected to the nodes with various powers and computation capabilities at the various levels of the hierarchical architecture. As a consequence, cryptography algorithms management become very challenging. To cope with this, physical layer security can be used to either provide direct secure data communication or facilitate the distribution of cryptography keys in the IoT network [115].

For instance, any unauthorized node is able of extending DoS activities at the physical layer by maliciously producing interferences for disrupting the desired communications between valid users, which is also known as a jamming attack. In order to combat jamming attacks, IoT typically consider the employment of cryptography algorithms, including AES, DES, RSA, and SHA [116].

Attackers use IoT network links to infiltrate networks and nodes. If the structure of IoT layers is based on cryptography, attackers will not be able to eavesdrop and steal information. The physical layer should be designed based on physical-security principles to act as a security protector [117, 118].

In the IoT, a secure channel must be defined for each application. Unsecured communication channels cause the aggressor to infiltrate the IoT network and declare itself as an authorized node to the network devices. Physical layer is used to ensure the security in such networks. However, the dynamic nature of IoT network can make the secret key distribution process vulnerable [119].

According to the role of the eavesdropper in IoT, the security design goals of the physical layer can be considered as follows [120]:

- Security designs against external eavesdropping.
- Security designs against internal eavesdropping.

Securing operations should be performed inside nodes, switches and routers. User identification should be based on authentication steps. Secure links required for the exchange of private keys must be guaranteed in cryptography algorithms. Counteract with eavesdropping and

Table 6 General comparison of cryptographic algorithms in IoT environments

Cryptography	References	Confidentiality	Integrity	Authentication	Authorization	Availability	Non-repudiation	Accountability	Anonymity	Replay attack	Eavesdropping
Asymmetric	[42]	√	√	√	√	√	x	x	x	x	√
	[43]	x	√	√	x	√	√	x	x	√	x
	[45]	x	√	√	x	x	x	√	x	√	x
	[46]	√	√	√	√	√	x	√	x	x	x
	[47]	x	√	√	√	√	x	√	x	√	√
	[48]	√	√	x	√	√	x	x	x	x	x
	[49]	√	√	√	√	√	√	√	√	√	x
	[50]	√	x	√	x	x	x	√	√	√	x
	[51]	x	x	√	√	√	√	√	x	x	x
	[52]	√	x	√	x	x	x	√	x	x	√
	[53]	√	x	√	x	x	x	√	x	x	x
	[54]	x	x	√	x	x	√	√	√	x	x
	[55]	√	√	√	√	√	√	√	x	√	x
	[56]	x	√	x	x	x	√	√	x	x	x
	[54]	√	x	√	√	√	√	√	x	x	x
	[57]	x	√	√	√	x	√	x	x	√	x
	[58]	√	√	√	√	√	√	√	x	√	√
	[59]	√	x	√	√	√	x	x	x	√	x
	[60]	√	√	√	√	√	x	√	√	√	x
	[61]	√	x	√	x	x	x	x	√	√	x
	[62]	√	√	√	x	x	√	√	x	√	x
	[63]	√	√	√	x	x	x	x	x	x	x
	[64]	√	√	√	√	√	x	x	x	x	x
	[65]	x	x	√	√	x	√	√	x	√	x
	[66]	√	√	x	√	√	√	x	x	x	x
	[67]	√	x	√	√	√	x	√	x	√	x
	[68]	√	√	√	√	x	x	√	x	√	x
	[69]	√	√	√	x	x	x	√	×	√	√
	[70]	√	x	√	√	√	x	√	√	√	x
	[71]	√	√	√	√	√	√	x	x	x	x
	[72]	x	√	√	√	x	√	√	x	x	√
	[73]	√	√	y	x	x	x	x	x	√	x
	[74]	√	√	√	√	√	√	x	x	x	√
	[75]	√	x	√	x	√	√	x	x	√	√
	[76]	√	√	√	x	√	√	x	x	√	x
	[77]	x	√	√	√	x	√	x	y	x	√

Table 6 continued

Cryptography	References	Confidentiality	Integrity	Authentication	Authorization	Availability	Non-repudiation	Accountability	Anonymity	Replay attack	Eavesdropping
	[78]	√	√	√	x	x	x	√	x	√	√
Symmetric	[79]	√	√	√	√	√	x	x	x	√	x
	[80]	√	√	√	√	√	x	x	x	√	x
	[81]	×	×	√	√	√	x	x	x	√	x
	[82]	√	√	x	x	x	√	x	x	x	x
	[83]	×	√	√	√	√	√	x	√	√	x
	[84]	√	√	x	x	x	√	x	x	√	√
	[85]	√	√	√	√	√	√	x	x	√	√
	[86]	√	√	√	√	x	x	x	x	x	x
	[87]	√	√	√	√	√	√	√	x	√	√
	[88]	x	√	√	√	√	√	√	x	x	x
	[89]	√	√	√	x	x	x	x	x	√	√
	[91]	√	√	√	√	√	x	x	x	√	x
	[92]	√	√	√	√	√	x	x	x	√	x
	[93]	x	x	x	√	√	√	√	√	x	√
	[94]	√	x	√	√	√	x	x	x	x	x
	[95]	x	√	x	√	√	√	√	x	x	√
	[96]	√	√	√	√	√	√	√	x	x	√
Hybrid	[97]	√	√	√	√	√	x	x	×	√	x
	[98]	√	×	√	√	√	x	x	√	x	x
	[99]	√	√	√	√	√	√	√	√	√	√
	[100]	√	√	√	x	x	x	x	x	x	x
	[101]	√	√	√	√	√	√	x	x	√	√
	[102]	x	√	√	√	√	x	x	x	√	x
	[103]	√	√	√	√	x	x	x	x	√	x
	[104]	√	√	√	√	√	√	√	√	√	x
	[105]	√	√	√	√	√	x	x	x	√	√
	[106]	x	√	√	√	√	x	x	x	√	x
	[107]	√	√	√	x	x	x	x	x	x	x
	[108]	√	x	√	√	√	x	x	x	√	√
	[109]	√	√	√	√	√	x	x	x	√	√

Table 6 continued

Cryptography	Man-in-the-middle attack	DoS attack	Spoofing attack	Impersonation attack	Brute-force attack	Insider attack	Sinkhole Attack	Tracking attack	Message modification	flooding attacks
Asymmetric	x	√	x	x	x	x	x	x	√	√
	x	x	x	√	x	√	x	x	x	x
	x	x	x	x	√	x	√	x	x	x
	x	x	x	x	x	x	x	x	x	x
	x	√	x	x	x	x	x	x	√	x
	x	x	x	x	x	x	x	x	x	x
	√	√	x	√	x	√	x	x	√	x
	x	√	√	x	x	√	x	x	√	x
	√	√	√	x	x	√	x	x	√	x
	x	√	x	√	x	x	x	x	x	x
	x	x	x	x	x	x	x	x	x	x
	√	√	x	√	x	√	x	√	x	x
	x	√	x	x	x	x	x	x	x	x
	x	x	x	x	x	x	x	x	x	x
	√	x	x	x	x	x	x	x	x	x
	√	x	x	x	x	x	x	x	√	x
	x	x	x	√	√	x	x	√	x	x
	x	√	x	x	x	x	x	x	x	x
	x	√	x	x	x	x	x	x	x	x
	x	√	√	x	x	x	x	x	√	x
	x	x	x	x	x	x	x	√	x	x
	x	x	x	x	x	√	x	x	x	x
	x	x	x	x	x	x	x	x	x	x
	√	√	x	x	x	x	x	x	x	x
	x	√	x	x	x	x	√	x	√	x
	√	x	x	x	√	x	√	√	x	x
	√	x	√	√	x	x	x	√	√	x
	√	x	x	x	x	x	x	√	√	x
	x	x	x	x	x	x	x	x	x	x
	x	x	√	√	√	√	x	x	x	x
	√	√	x	x	√	x	x	x	√	√
	x	√	x	x	x	x	√	x	x	x
	x	x	x	√	x	x	x	x	x	x
	√	x	x	√	√	x	√	√	x	x
	x	x	√	x	x	x	x	√	√	x

Table 6 continued

Cryptography	Man-in-the-middle attack	DoS attack	Spoofing attack	Impersonation attack	Brute-force attack	Insider attack	Sinkhole Attack	Tracking attack	Message modification	flooding attacks
	x	√	x	√	√	x	√	x	x	√
	√	√	√	√	√	x	x	√	√	x
Symmetric	x	√	x	x	√	x	x	√	√	x
	x	x	x	x	x	x	x	x	x	x
	x	x	x	√	√	√	√	√	x	x
	x	√	x	x	x	x	x	x	x	x
	x	√	x	x	x	x	x	√	x	x
	√	√	x	x	x	x	x	x	√	x
	√	x	√	x	√	√	√	√	x	x
	x	√	√	√	√	√	√	√	x	√
	√	√	√	√	√	x	x	x	x	x
	x	√	x	x	x	x	x	x	x	x
	√	√	√	√	x	x	x	√	√	√
	x	√	x	√	x	x	√	√	√	x
	√	x	√	√	√	√	√	√	√	x
	x	√	√	x	x	√	√	x	x	√
	√	√	√	√	√	√	√	x	x	x
	x	√	x	x	x	√	√	√	√	√
	√	√	√	√	√	√	x	√	√	x
Hybrid	x	x	x	x	x	x	x	x	x	x
	√	x	x	x	x	√	x	√	√	x
	√	√	√	√	√	√	√	√	√	√
	√	x	x	x	x	x	x	x	x	x
	√	√	√	√	√	√	√	√	√	√
	x	x	x	x	x	x	x	x	x	x
	x	x	x	x	x	x	x	x	x	x
	x	x	x	√	x	x	x	x	x	x
	√	√	√	√	√	√	√	√	√	√
	x	x	x	x	x	x	x	x	x	x
	x	√	x	x	x	x	x	x	x	x
	√	√	√	√	√	√	√	√	√	√
	√	√	√	√	√	√	√	x	√	√

active attacks are guaranteed by the new evolution of cryptography algorithms capabilities, especially considering Boolean operations [121].

5 Conclusion and future works

The IoT has become an exciting and welcoming technology that allows real-time collection of knowledge on all interconnected products. Such integrated physical machines provide unique identifiers and the ability to communicate and transfer data over a network using its sensor technology. The information collected also provides a significant opportunity for different companies to gain insight into these data by applying effective data analytics. IoT has also revealed a huge vulnerability in security ranging from authentication to trust management, and a threat to its embedded devices. This paper dealt with IoT security Based on cryptographic algorithms. Security should be an important factor during the design of the IoT environment. Cryptography algorithms are a very effective tool for ensuring the protection of the physical layer of the network and are necessary for ensuring the security of the entire network infrastructure.

Recently many lightweight cryptography algorithms have been used in securing the resource constraint devices in IoT. Reducing computation time and reducing memory usage are two important factors in IoT resources. Security is an important field in the IoT. Combining asymmetric algorithms to increase the complexity of cryptography is a great method for intrusion prevention into IoT resources. Future research directions, the challenges of deal with attacks on IoT resources and open issues are also reviewed for security scenarios.

References

1. Diène, B., Rodrigues, J. J. P. C., Diallo, O., Ndoye, E. L. H. M., & Korotaev, V. V. (2020). Data management techniques for internet of things. *Mechanical Systems and Signal Processing, 138,* 106564. https://doi.org/10.1016/j.ymssp.2019.106564.
2. Alqahtani, F., Al-Makhadmeh, Z., Tolba, A., & Said, O. (2020). TBM: A trust-based monitoring security scheme to improve the service authentication in the internet of things communications. *Computer Communications, 150,* 216–225. https://doi.org/10.1016/j.comcom.2019.11.030.
3. Mousavi, S. K., Ghaffari, A., Besharat, S., & Afshari, H. (2020). Improving the security of internet of things using cryptographic algorithms: A case of smart irrigation systems. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-020-02303-5.
4. Jazebi, S. J., & Ghaffari, A. (2020). RISA: Routing scheme for internet of things using shuffled frog leaping optimization algorithm. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-020-01708-6.
5. Seyfollahi, A., & Ghaffari, A. (2020). Reliable data dissemination for the internet of things using Harris hawks optimization. *Peer-to-Peer Networking and Applications*. https://doi.org/10.1007/s12083-020-00933-2.
6. HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2019). A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things*. https://doi.org/10.1016/j.iot.2019.100129.
7. Hou, J., Qu, L., & Shi, W. (2019). A survey on internet of things security from data perspectives. *Computer Networks, 148,* 295–306. https://doi.org/10.1016/j.comnet.2018.11.026.
8. Barbosa, G., Endo, P. T., & Sadok, D. (2019). An internet of things security system based on grouping of smart cards managed by field programmable gate array. *Computers & Electrical Engineering, 74,* 331–348. https://doi.org/10.1016/j.compeleceng.2019.02.013.
9. Bhoyar, P., Sahare, P., Dhok, S. B., & Deshmukh, R. B. (2019). Communication technologies and security challenges for internet of things: A comprehensive review. *AEU—International Journal of Electronics and Communications, 99,* 81–99. https://doi.org/10.1016/j.aeue.2018.11.031.
10. Zeadally, S., Das, A. K., & Sklavos, N. (2019). Cryptographic technologies and protocol standards for internet of things. *Internet of Things*. https://doi.org/10.1016/j.iot.2019.100075.
11. Li, W., & Wang, P. (2019). Two-factor authentication in industrial internet-of-things: Attacks, evaluation and new construction. *Future Generation Computer Systems, 101,* 694–708. https://doi.org/10.1016/j.future.2019.06.020.
12. Radoglou Grammatikis, P. I., Sarigiannidis, P. G., & Moscholios, I. D. (2019). Securing the internet of things: Challenges, threats and solutions. *Internet of Things, 5,* 41–70. https://doi.org/10.1016/j.iot.2018.11.003.
13. Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks, 141,* 199–221. https://doi.org/10.1016/j.comnet.2018.03.012.
14. Beheshtiasl, A., & Ghaffari, A. (2019). Secure and trust-aware routing scheme in wireless sensor networks. *Wireless Personal Communications, 107*(4), 1799–1814. https://doi.org/10.1007/s11277-019-06357-3.
15. Mohammadi, P., & Ghaffari, A. (2019). Defending against flooding attacks in mobile ad-hoc networks based on statistical analysis. *Wireless Personal Communications, 106*(2), 365–376. https://doi.org/10.1007/s11277-019-06166-8.
16. Seyfollahi, A., & Ghaffari, A. (2020). A lightweight load balancing and route minimizing solution for routing protocol for low-power and lossy networks. *Computer Networks, 179,* 107368. https://doi.org/10.1016/j.comnet.2020.107368.
17. Gheisari, M., Wang, G., & Chen, S. (2020). An edge computing-enhanced internet of things framework for privacy-preserving in smart city. *Computers & Electrical Engineering, 81,* 106504. https://doi.org/10.1016/j.compeleceng.2019.106504.
18. Perera, C., Barhamgi, M., Bandara, A. K., Ajmal, M., Price, B., & Nuseibeh, B. (2020). Designing privacy-aware internet of things applications. *Information Sciences, 512,* 238–257. https://doi.org/10.1016/j.ins.2019.09.061.
19. Beltrán, M. (2018). Identifying, authenticating and authorizing smart objects and end users to cloud services in internet of things. *Computers & Security, 77,* 595–611. https://doi.org/10.1016/j.cose.2018.05.011.
20. Ray, P. P. (2018). A survey on internet of things architectures. *Journal of King Saud University—Computer and Information Sciences, 30*(3), 291–319. https://doi.org/10.1016/j.jksuci.2016.10.003.

21. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of things security: A survey. *Journal of Network and Computer Applications, 88,* 10–28. https://doi.org/10.1016/j.jnca.2017.04.002.
22. Bovenzi, G., Ciuonzo, D., Persico, V., Pescapè, A., & Rossi, P. S. (2019). IoT-enabled distributed detection of a nuclear radioactive source via generalized score tests. In *Advances in signal processing and intelligent recognition systems*. Singapore: Springer Singapore.
23. Nesa, N., & Banerjee, I. (2017). IoT-based sensor data fusion for occupancy sensing using Dempster-Shafer evidence theory for smart buildings. *IEEE Internet of Things Journal, 4*(5), 1563–1570. https://doi.org/10.1109/JIOT.2017.2723424.
24. Ciuonzo, D., Gelli, G., Pescapé, A., & Verde, F. (2019). Decision fusion rules in ambient backscatter wireless sensor networks. In *2019 IEEE 30th annual international symposium on personal, indoor and mobile radio communications (PIMRC)*.
25. Azari, L., & Ghaffari, A. (2015). Proposing a novel method based on network-coding for optimizing error recovery in wireless sensor networks. *Indian Journal of Science and Technology, 8*(9), 859–867.
26. Ghaffari, A. (2014). Designing a wireless sensor network for ocean status notification system. *Indian Journal of Science and Technology, 7*(6), 809.
27. Ghaffari, A., & Rahmani, A. (2008). Fault tolerant model for data dissemination in wireless sensor networks. In *2008 international symposium on information technology*. IEEE.
28. Ghaffari, A., Rahmani, A., & Khademzadeh, A. (2011). Energy-efficient and QoS-aware geographic routing protocol for wireless sensor networks. *IEICE Electronics Express, 8*(8), 582–588.
29. Ghaffari, A., & Takanloo, V. A. (2011). QoS-based routing protocol with load balancing for wireless multimedia sensor networks using genetic algorithm. *World Applied Sciences Journal, 15*(12), 1659–1666.
30. Althunibat, S., Sucasas, V., & Rodriguez, J. (2017). A physical-layer security scheme by phase-based adaptive modulation. *IEEE Transactions on Vehicular Technology, 66*(11), 9931–9942. https://doi.org/10.1109/TVT.2017.2737885.
31. Althunibat, S., Sucasas, V., Mantas, G., & Rodriguez, J. (2018). Physical-layer entity authentication scheme for mobile MIMO systems. *IET Communications, 12*(6), 712–718. https://doi.org/10.1049/iet-com.2017.0518.
32. Alhasanat, M., Althunibat, S., Darabkh, K. A., Alhasanat, A., & Alsafasfeh, M. (2020). A physical-layer key distribution mechanism for IoT networks. *Mobile Networks and Applications, 25*(1), 173–178. https://doi.org/10.1007/s11036-019-01219-5.
33. Fatima, I., Malik, S. U. R., Anjum, A., & Ahmad, N. (2020). Cyber physical systems and IoT: Architectural practices. *Interoperability, and Transformation, IT Professional, 22*(3), 46–54. https://doi.org/10.1109/MITP.2019.2912604.
34. Rauscher, J., & Bauer, B. (2018). Safety and security architecture analyses framework for the internet of things of medical devices. In *2018 IEEE 20th international conference on e-health networking, applications and services (Healthcom)*.
35. Celia, L., & Cungang, Y. (2018). (WIP) Authenticated key management protocols for internet of things. *IEEE International Congress on Internet of Things (ICIOT)* 126–129.
36. Rajashree, S., Shah, P. G., & Murali, S. (2018). Security model for internet of things end devices. In *2018 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*.
37. Deshmukh, S., & Sonavane, S. S. (2017). Security protocols for internet of things: A survey. In *2017 International conference on Nextgen electronic technologies: Silicon to software (ICNETS2)*.
38. Lu, X., Pan, Z., & Xian, H. (2019). An integrity verification scheme of cloud storage for internet-of-things mobile terminal devices. *Computers & Security*. (**in press, corrected proof**).
39. Chahal, R. K., Kumar, N., & Batra, S. (2020). Trust management in social internet of things: A taxonomy, open issues, and challenges. *Computer Communications, 150,* 13–46. https://doi.org/10.1016/j.comcom.2019.10.034.
40. Zhang, X., & Hang, H. (2010). An efficient conversion scheme for enhancing security of Diffie-Hellman-based encryption. *Wuhan University Journal of Natural Sciences, 15*(5), 415–421. https://doi.org/10.1007/s11859-010-0676-9.
41. Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, 21*(2), 120–126.
42. Kandhoul, N., & Dhurandher, S. K. (2019). An asymmetric RSA-based security approach for opportunistic IoT. In *2nd international conference on wireless intelligent and distributed environment for communication*. Cham: Springer International Publishing.
43. Jin, B. W., Park, J. O., & Mun, H. J. (2019). A design of secure communication protocol using RLWE based homomorphic encryption in IoT convergence cloud environment. *Wireless Personal Communications, 105,* 599–618.
44. Miller, V. S. (1986). Use of elliptic curves in cryptography. In *Advances in cryptology—CRYPTO '85 proceedings*. Berlin, Heidelberg: Springer.
45. Harbi, Y., Aliouat, Z., Harous, S., & Bentaleb, A. (2019). Secure data transmission scheme based on elliptic curve cryptography for internet of things. In *Modelling and implementation of complex systems*. Cham: Springer International Publishing.
46. Kudithi, T., & Sakthivel, R. (2019). High-performance ECC processor architecture design for IoT security applications. *The Journal of Supercomputing, 75*(1), 447–474. https://doi.org/10.1007/s11227-018-02740-2.
47. Shah, D. P., & Shah, P. G. (2018). Revisting of elliptical curve cryptography for securing internet of things (IOT). *IEEE*, 1–3.
48. Sharma, C., & Sunanda. (2018). Performance analysis of ECC and RSA for securing CoAP-based remote health monitoring system. In *Ambient communications and computer systems*. Singapore: Springer Singapore.
49. Dhillon, P. K., & Kalra, S. (2018). Multi-factor user authentication scheme for IoT-based healthcare services. *Journal of Reliable Intelligent Environments, 4*(3), 141–160. https://doi.org/10.1007/s40860-018-0062-5.
50. Yang, X., Yi, X., Zeng, Y., Khalil, I., Huang, X., & Nepal, S. (2018). An improved lightweight RFID authentication protocol for internet of things. *Web Information Systems Engineering—WISE*, 111–126.
51. Sasirekha, S., Swamynathan, S., & Suganya, S. (2018). An ECC-based algorithm to handle secure communication between heterogeneous IoT devices. In *Advances in electronics, communication and computing*. Singapore: Springer Singapore.
52. Saeed, M. E. S., Liu, Q.-Y., Tian, G., Gao, B., & Li, F. (2019). AKAIoTs: Authenticated key agreement for internet of things. *Wireless Networks, 25*(6), 3081–3101. https://doi.org/10.1007/s11276-018-1704-5.
53. Kumar, K. S., & Sukumar, R. (2019). Achieving energy efficiency using novel scalar multiplication based ECC for android devices in internet of things environments. *Cluster Computing, 22*(5), 12021–12028. https://doi.org/10.1007/s10586-017-1542-8.
54. Diro, A. A., Chilamkurti, N., & Veeraraghavan, P. (2017). Elliptic curve based cybersecurity schemes for publish-subscribe internet of things. In *Quality, reliability, security and robustness in heterogeneous networks*. Cham: Springer International Publishing.

55. Hasan, H., Salah, T., Shehada, D., Zemerly, M. J., Yeun, C. Y., Al-Qutayri, M., & Al-Hammadi, Y. (2017). Secure lightweight ECC-based protocol for multi-agent IoT systems. In *2017 IEEE 13th international conference on wireless and mobile computing, networking and communications (WiMob)*.
56. Shruti, P., & Chandraleka, R. (2017). Elliptic curve cryptography security in the context of internet of things. *International Journal of Scientific & Engineering Research, 8*(5), 90–94.
57. Nayak, B. (2017). A secure ID-based signcryption scheme based on elliptic curve cryptography. *International Journal of Computational Intelligence Studies, 6*(2), 150–156.
58. Kumari, S., Karuppiah, M., Das, A. K., Li, X., Wu, F., & Kumar, N. (2018). A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. *The Journal of Supercomputing, 74*(12), 6428–6453. https://doi.org/10.1007/s11227-017-2048-0.
59. Tewari, A., & Gupta, B. B. (2017). A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices. *International Journal of Advanced Intelligence Paradigms (IJAIP)*, *9*(2).
60. Dhillon, P. K., & Kalra, S. (2016). Elliptic curve cryptography for real time embedded systems in IoT networks. In *2016 5th international conference on wireless networks and embedded systems (WECON)*.
61. Shen, H., Shen, J., Khan, M. K., & Lee, J.-H. (2017). Efficient RFID authentication using elliptic curve cryptography for the internet of things. *Wireless Personal Communications, 96*(4), 5253–5266. https://doi.org/10.1007/s11277-016-3739-1.
62. Hernández-Ramos, J. L., Jara, A. J., Marín, L., & Gómez, A. F. S. (2016). DCapBAC: Embedding authorization logic into smart things through ECC optimizations. *International Journal of Computer Mathematics, 93*(2), 345–366. https://doi.org/10.1080/00207160.2014.915316.
63. Das, M. L. (2013). Strong security and privacy of RFID system for internet of things infrastructure. In *International conference on security, privacy, and applied cryptography engineering, SPACE 2013: Security, privacy, and applied cryptography engineering* (pp. 56–69).
64. Marin, L., Jara, A., & Gomez, A. S. (2013). Shifting primes: Optimizing elliptic curve cryptography for 16-bit devices without hardware multiplier. *Mathematical and Computer Modelling, 58*(5), 1155–1174. https://doi.org/10.1016/j.mcm.2013.02.008.
65. Salas, M. (2013). A secure framework for OTA smart device ecosystems using ECC encryption and biometrics. In *Advances in security of information and communication networks*. Berlin, Heidelberg: Springer.
66. Marin, L., Jara, A. J., & Skarmeta, A. F. G. (2011). Shifting primes: Extension of pseudo-mersenne primes to optimize ECC for MSP430-based future internet of things devices. In *Availability, reliability and security for business, enterprise and health information systems*. Berlin, Heidelberg: Springer.
67. Bruni, A., Sahl Jørgensen, T., Grønbech Petersen, T., & Schürmann, C. (2018). Formal verification of ephemeral Diffie-Hellman over COSE (EDHOC). In *Security standardisation research.* Cham: Springer International Publishing.
68. Shah, R. H., & Salapurkar, D. P. (2017). A multifactor authentication system using secret splitting in the perspective of cloud of things. In *2017 international conference on emerging trends & innovation in ICT (ICEI)*.
69. Pérez, S., Rotondi, D., Pedone, D., Straniero, L., Núñez, M. J., & Gigante, F. (2018). Towards the CP-ABE application for privacy-preserving secure data sharing in IoT contexts. In *Innovative mobile and internet services in ubiquitous computing*. Cham: Springer International Publishing.
70. Zhang, Y., Deng, R. H., Han, G., & Zheng, D. (2018). Secure smart health with privacy-aware aggregate authentication and access control in internet of things. *Journal of Network and Computer Applications, 123,* 89–100. https://doi.org/10.1016/j.jnca.2018.09.005.
71. Zhang, Y., Wu, A., Zhang, T., & Zheng, D. (2019). Secure and flexible keyword search over encrypted data with outsourced decryption in Internet of things. *Annals of Telecommunications, 74*(7), 413–421. https://doi.org/10.1007/s12243-018-0694-8.
72. Pace, G. J., Picazo-Sanchez, P., & Schneider, G. (2018). Migrating monitors + ABE: A suitable combination for secure IoT? In *Leveraging applications of formal methods, verification and validation. Industrial practice*. Cham: Springer International Publishing.
73. Liu, L., & Ye, J. (2018). Identity-based re-encryption scheme with lightweight re-encryption key generation. *Journal of Discrete Mathematical Sciences and Cryptography, 21*(1), 41–57. https://doi.org/10.1080/09720529.2016.1160513.
74. Gopinath, M. P., Tamizharasi, G. S., Kavisankar, L., Sathyaraj, R., Karthi, S., Aarthy, S. L., & Balamurugan, B. (2019). A secure cloud-based solution for real-time monitoring and management of Internet of underwater things (IOUT). *Neural Computing and Applications, 31*(1), 293–308. https://doi.org/10.1007/s00521-018-3774-9.
75. Choi, J., In, Y., Park, C., Seok, S., Seo, H., & Kim, H. (2018). Secure IoT framework and 2D architecture for end-to-end security. *The Journal of Supercomputing, 74*(8), 3521–3535. https://doi.org/10.1007/s11227-016-1684-0.
76. Lee, J., Oh, S., & Jang, J. W. (2015). A work in progress: Context based encryption scheme for internet of things. *Procedia Computer Science, 56,* 271–275. https://doi.org/10.1016/j.procs.2015.07.208.
77. Zhang, M. (2014). New model and construction of ABE: Achieving key resilient-leakage and attribute direct-revocation. In *Information security and privacy*. Cham: Springer International Publishing.
78. Su, J., Cao, D., Zhao, B., Wang, X., & You, I. (2014). ePASS: An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the internet of things. *Future Generation Computer Systems, 33,* 11–18. https://doi.org/10.1016/j.future.2013.10.016.
79. Chandi, P., Sharma, A., Chhabra, A., & Gupta, P. (2019). A DES-based mechanism to secure personal data on the internet of things. In *ICCCE 2018*. Singapore: Springer Singapore.
80. Cruz-Duarte, S., Sastoque-Mahecha, M., Gaona-García, E., & Gaona-García, P. (2019). Security scheme for IoT environments in smart grids. In *Information systems and technologies to support learning*. Cham: Springer International Publishing.
81. Vidyashree, L., & Suresha, B. M. (2019). Methodology to secure agricultural data in IoT. In *Emerging technologies in data mining and information security*. Singapore: Springer Singapore.
82. Kiran Kumar, V. G., & Shantharama Rai, C. (2019). Implementation and analysis of cryptographic ciphers in FPGA. In *Emerging technologies in data mining and information security*. Singapore: Springer Singapore.
83. Jan, M. A., Khan, F., Alam, M., & Usman, M. (2019). A payload-based mutual authentication scheme for internet of things. *Future Generation Computer Systems, 92,* 1028–1039. https://doi.org/10.1016/j.future.2017.08.035.
84. Wang, Y., Chen, C., & Jiang, Q. (2019). Security algorithm of internet of things based on ZigBee protocol. *Cluster Computing, 22*(6), 14759–14766. https://doi.org/10.1007/s10586-018-2388-4.
85. Alassaf, N., Gutub, A., Parah, S. A., & Ghamdi, M. A. (2019). Enhancing speed of SIMON: A light-weight-cryptographic

algorithm for IoT applications. *Multimedia Tools and Applications, 78*(23), 32633–32657. https://doi.org/10.1007/s11042-018-6801-z.
86. Hu, C., Luo, J., Pu, Y., Yu, J., Zhao, R., Huang, H., & Xiang, T. (2018). An efficient privacy-preserving data aggregation scheme for IoT. In *Wireless algorithms, systems, and applications*. Cham: Springer International Publishing.
87. Tsai, K. L., Huang, Y. L., Leu, F. Y., You, I. I., Huang, Y. L., & Tsai, C. H. (2018). AES-128 based secure low power communication for LoRaWAN IoT environments, security and trusted computing for industrial internet of things. *IEEE*, 45325–45334.
88. Newe, T., Rao, M., Toal, D., Dooly, G., Omerdic, E., & Mathur, A., et al. (2017). Efficient and high speed FPGA bump in the wire implementation for data integrity and confidentiality services in the IoT. In O. A. Postolache (Ed.), *Sensors for everyday life: Healthcare settings* (pp. 259–285). Cham: Springer International Publishing.
89. Bohan, Z., Xu, W., Kaili, Z., & Xueyuan, Z. (2013). Encryption node design in internet of things based on fingerprint features and CC2530. In *2013 IEEE international conference on green computing and communications and IEEE internet of things and IEEE cyber, physical and social computing*.
90. Schneier, B. (1993). *Description of a new variable-length key, 64-bit block cipher (blowfish), fast software encryption, Cambridge security workshop proceedings*. Springer (pp. 191–204).
91. Corpuz, R. R., Gerardo, B. D., & Medina, R. P. (2018). *Using a modified approach of blowfish algorithm for data security in cloud computing, ICIT 2018, Hong Kong* (pp. 157–162).
92. Suchdeo, M., Mawane, D., Negandhi, M., Sarkar, S., & Prajapat, S. (2018). Towards performance analysis of symmetric key algorithm on n-core systems: An IOT perspective. *International Journal of Computer Sciences and Engineering, 6*(6), 1127–1129.
93. Deshpande, K., & Singh, P. (2018). *Performance evaluation of cryptographic ciphers on IoT devices, international conference on recent trends in computational engineering and technologies (ICTRCET'18)* (pp. 1–6).
94. Suresh, M., & Neema, M. (2016). Hardware implementation of blowfish algorithm for the secure data transmission in internet of things. *Procedia Technology, 25,* 248–255. https://doi.org/10.1016/j.protcy.2016.08.104.
95. Prasetyo, K. N., Purwanto, Y., & Darlis, D. (2014). An implementation of data encryption for internet of things using blowfish algorithm on FPGA. In *2014 2nd international conference on information and communication technology (ICoICT)*.
96. Xie, C., & Deng, S.-T. (2017). Research and application of security and privacy in industrial internet of things based on fingerprint encryption. In *Industrial IoT technologies and applications*. Cham: Springer International Publishing.
97. Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N., & Farouk, A. (2018). Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access, 6,* 20596–20608. https://doi.org/10.1109/ACCESS.2018.2817615.
98. Zhang, Y., He, D., & Choo, K. K. R. (2018). BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT. *Wireless Communications and Mobile Computing*, 1–9.
99. Sankaralingam, S. A., Usha, G., & Acharya, A. (2018). A hybrid cryptographic algorithm based on AES and SHA1 in RFID. *International Journal of Pure and Applied Mathematics, 118*(11), 835–840.
100. Schmitt, C., Kothmayr, T., Hu, W., & Stiller, B. (2017). Two-way authentication for the internet-of-things. In D. P. Acharjya & M. K. Geetha (Eds.), *Internet of things: Novel advances and envisioned applications* (pp. 27–56). Cham: Springer International Publishing.
101. Odelu, V., Das, A. K., Khan, M. K., Choo, K. R., & Jo, M. (2017). Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size keys and ciphertexts. *IEEE Access, 5,* 3273–3283. https://doi.org/10.1109/ACCESS.2017.2669940.
102. Darwish, A., El-Gendy, M. M., Hassanien, A. E., & New, A., et al. (2017). Hybrid cryptosystem for internet of things applications. In A. E. Hassanien (Ed.), *Multimedia forensics and security: Foundations, innovations, and applications* (pp. 365–380). Cham: Springer International Publishing.
103. Mohammed, A. F., & Qyser, A. A. M. (2020). A hybrid approach for secure iris-based authentication in IoT. In *ICICCT 2019—system reliability, quality control, safety, maintenance and management*. Singapore: Springer Singapore.
104. Alamr, A. A., Kausar, F., Kim, J., & Seo, C. (2018). A secure ECC-based RFID mutual authentication protocol for internet of things. *The Journal of Supercomputing, 74*(9), 4281–4294. https://doi.org/10.1007/s11227-016-1861-1.
105. Qiaohong, Z., Xiaoyu, Y., & Xie, W. (2015). Data encryption for remote monitoring system based on internet of things in mobile mode. In *Human centered computing*. Cham: Springer International Publishing.
106. Zhao, X., Qi, L., Li, Y., Chen, J., & Shen, H. (2015). Data encryption and transmission technology for cotton of IoT security. In *LISS 2014*. Berlin, Heidelberg: Springer.
107. Xin, M. (2015). A mixed encryption algorithm used in internet of things security transmission system. In *2015 international conference on cyber-enabled distributed computing and knowledge discovery*.
108. Yao, X., Chen, Z., & Tian, Y. (2015). A lightweight attribute-based encryption scheme for the internet of things. *Future Generation Computer Systems, 49,* 104–112. https://doi.org/10.1016/j.future.2014.10.010.
109. Guo, R., Wen, Q., Shi, H., Jin, Z., & Zhang, H. (2014). Certificateless public key encryption scheme with hybrid problems and its application to internet of things. Hindawi Publishing Corporation, Mathematical Problems in Engineering (pp. 1–9).
110. Weber, R. H., & Studer, E. (2016). Cybersecurity in the internet of things: Legal aspects. *Computer Law and Security Review, 32*(5), 715–728. https://doi.org/10.1016/j.clsr.2016.07.002.
111. Han, G., Zhou, L., Wang, H., Zhang, W., & Chan, S. (2018). A source location protection protocol based on dynamic routing in WSNs for the social internet of things. *Future Generation Computer Systems, 82,* 689–697. https://doi.org/10.1016/j.future.2017.08.044.
112. Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A. K., & Choo, K.-K.R. (2018). A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. *Journal of Network and Computer Applications, 103,* 194–204. https://doi.org/10.1016/j.jnca.2017.07.001.
113. Tewari, A., & Gupta, B. B. (2018). Security, privacy and trust of different layers in internet-of-things (IoTs) framework. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2018.04.027.
114. Alavi, A. H., Jiao, P., Buttlar, W. G., & Lajnef, N. (2018). Internet of things-enabled smart cities: State-of-the-art and future trends. *Measurement, 129,* 589–606. https://doi.org/10.1016/j.measurement.2018.07.067.
115. Yang, N., Wang, L., Geraci, G., Elkashlan, M., Yuan, J., & Renzo, M. D. (2015). Safeguarding 5G wireless communication networks using physical layer security. *IEEE Communications Magazine, 53*(4), 20–27. https://doi.org/10.1109/MCOM.2015.7081071.
116. Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE, 104*(9), 1727–1765. https://doi.org/10.1109/JPROC.2016.2558521.

117. Pandey, A., & Yadav, S. (2018). Physical layer security in cooperative AF relaying networks with direct links over mixed Rayleigh and double-Rayleigh fading channels. *IEEE Transactions on Vehicular Technology, 67*(11), 10615–10630. https://doi.org/10.1109/TVT.2018.2866590.
118. Pandey, A., & Yadav, S. (2020). Secrecy analysis of cooperative vehicular relaying networks over double-Rayleigh fading channels. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-020-07500-1.
119. Chu, S. (2019). Secrecy analysis of modify-and-forward relaying with relay selection. *IEEE Transactions on Vehicular Technology, 68*(2), 1796–1809. https://doi.org/10.1109/TVT.2018.2885807.
120. Zhang, C., Jia, F., Zhang, Z., Ge, J., & Gong, F. (2020). Physical layer security designs for 5G NOMA systems with a stronger near-end internal eavesdropper. *IEEE Transactions on Vehicular Technology*, 1–1. https://doi.org/10.1109/TVT.2020.3018234.
121. Osorio, D. P. M., Olivo, E. E. B., Alves, H., & Latva-Aho, M. (2020). Safeguarding MTC at the physical layer: Potentials and challenges. *IEEE Access, 8,* 101437–101447. https://doi.org/10.1109/ACCESS.2020.2996383.

Seyyed Keyvan Mousavi received the B.Sc. degree in Software Engineering from the Payam Noor University, Miandoab, Iran, in 2012, and the M.Sc. degree in Software Engineering from the Islamic Azad University, Miandoab branch, in 2017. He is currently a Ph.D. Student at the Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran. His research interests include Internet of things, Information security, and Cryptography. Currently his research work is based on Security and Privacy in IoT networks.

Ali Ghaffari received his B.Sc., M.Sc. and Ph.D. degrees in computer engineering from the University of Tehran and IAU (Islamic Azad University), TEHRAN, IRAN in 1994, 2002 and 2011 respectively. He has served as a reviewer for Applied Soft Computing, Ad Hoc networks, Future Generation Computer System (FGCS), Elsevier, International Communication System (IJCS), Journal of Ambient Intelligent and Humanized Computing (AIHC), Wireless Networks, Wireless Personal Communication. As an associate professor of computer engineering at Islamic Azad University, Tabriz branch, IRAN, his research interests are mainly in the field of software defined network(SDN), Wireless Sensor Networks (WSNs), Mobile Ad Hoc Networks (MANETs),Vehicular Ad Hoc Networks(VANETs), networks security and Quality of Service (QoS). He has published more than 100 international conference and reviewed journal papers.

Sina Besharat received his B.Sc., M.Sc. and Ph.D. degrees in waster engineering from the University of Urmia, Tarbiat modarres and Tabriz University in 2000, 2002 and 2010 respectively. As an associate professor of water engineering at Urmia University, Urmia, IRAN, his research interests are mainly in the field of Numerical solution, Numerical Modeling of water flow and solute transport and Soil Water and Plant Relationship. He has published more than 100 international conference and reviewed journal papers.

Hamed Afshari received his B.Sc., M.Sc. and Ph.D. degrees in mechanical engineering from the University of Urmia and Zahedan University in 2006, 2009 and 2016 respectively. As an assistant professor of mechanical engineering at Islamic azad University, Urmia branch, Urmia, IRAN, his research interests are mainly in the field of biomechanical engineering. He has published more than 20 international conference and reviewed journal papers.