A comprehensive taxonomy of security and privacy issues in RFID

Atul Kumar¹ · Ankit Kumar Jain¹ · Mohit Dua¹

Received: 15 September 2020 / Accepted: 18 January 2021 / Published online: 12 February 2021
© The Author(s) 2021

Abstract

Internet of things (IoT) is made up of many devices like sensors, tags, actuators, mobile devices, and many more. These devices interact with each other without human interaction. Radio-frequency identification (RFID) devices are used to track people, assets, objects, etc. Along with the small memory capacity and low-power battery issues, these devices suffer from various security-related issues. These security threats include attacks such as replay, disclosure, tracking, offline guessing, denial of service attacks, and many more. In the last few decades, the researchers have suggested various security approaches to overcome these vulnerabilities. Hence, this paper discusses various possible attacks that can occur on an RFID system, and several security schemes that have been proposed to handle these attacks. First, the works presents the architecture of IoT in detail. Second, all possible attacks are described by categorizing them into confidentiality, integrity, and availability. Then, taxonomy of various security schemes, to deal with these attacks, is discussed under the criteria cryptography approaches, privacy, authentication, authorization, and availability. Finally, the paper describes various issues and challenges to have a better understanding of scope of the future research in the field of RFID security.

Keywords IoT · RFID · Security · Confidentiality · Integrity · Availability · Authorization

Introduction

Internet of things (IoT) refers to the various types of heterogeneous devices connected to the Internet. In IoT, “things” refer to physical devices like sensors, actuators, and mobile devices that can communicate without human interaction. Gartner [1] reported approximately 8.4 billion “things” connected to the Internet in 2017. The report also expected the same to be increased by 20.4 billion, and the total spending to reach almost 3 trillion dollars in 2020 [1]. This much massive numbers of devices create a tremendous amount of communication data and power, throughout the network. Moreover, these huge numbers of devices cannot be handled by the IPv4 protocol. Therefore, the IPv6 protocol is used to handle these devices. IoT devices contain limited memory capacity and battery. However, the traditional IPv6 requires much power and necessitates high communication overhead. Thus, lightweight protocols such as 6LoWPAN and ZigBee are employed. IEEE 802.15.4 standard is used by most sensors that require low power and low rate of communication

overhead over the network. IoT can be applied in many domains such as smart transportation [2], smart grid [3], smart city [4, 5], smart house [6, 7], and logistics [8].

RFID is used to identify the object in the network. It uses three operating bands, namely low-frequency band (i.e., 125–134 kHz), high-frequency band (i.e., 13.56 MHz), and ultrahigh-frequency band (i.e., 860–930 MHz) [9, 10]. The RFID scheme consists of several classes of tags and a reader. These tags include an inadequate amount of memory and low-power capacity. However, there are numerous other issues in terms of privacy, forward security, and authentication. Due to these security issues, there are several attacks possible on RFID systems such as tag cloning, disclosure, spoofing, and replay attack to name a few. Table 1 shows the various threats on the IoT applications. This paper discusses various attacks on the RFID system. It also discusses different authentication schemes, hash function, block cipher, and stream cipher for the RFID system.

Along with efficient power and communication characteristics, RFID devices also require appropriate solutions to provide security. The security issues can be handled by different cryptographic, authentication, authorization, and privacy solutions [11–18]. The cryptographic solutions apply in various IoT applications, including smart

✉ Ankit Kumar Jain
ankitjain@nitkkr.ac.in

¹ National Institute of Technology, Kurukshetra, India

Table 1 Various threats in IoT applications

Application	IoT devices	Communication	Threads
Health care	Sensor, smart wearable devices	ZigBee, Bluetooth	Authorization, privacy, authentication
Smart grid	Smart readers, smart meters	ZigBee, Wifi	Eavesdropping, tampering, physical attack, privacy
Smart environment	Building	ZigBee, LTE, Wifi, Bluetooth	Eavesdropping, authentication, authorization, privacy
Transportation	RSU, EFC, OBU	DSRC	Spectrum sharing, congestion, jamming

cards, wireless body area networks (WBAN), wireless sensor networks (WSN), and radio frequency identification (RFID). There are various cryptographic security schemes suggested by the researcher, and these schemes are divided into two parts: public-key cryptography and symmetric-key cryptography. Public-key cryptography schemes include RSA, Diffie–Hellman key exchange, Elgamal, etc. However, these schemes require lots of bandwidth and power. An elliptic curve is introduced that provides less energy and fewer computational steps than RSA, Diffie–Hellman like schemes. The symmetric schemes use the simple bitwise operation (XOR, OR, AND, Rotate), cyclic redundancy checksum, and symmetric encryption. Thus, these schemes need less power and low communication overhead than public-key cryptography. The other classifications that can be used for these security solutions are privacy, authentication, authorization, and availability.

As RFID devices have become an essential part of computing and communication devices that we use for our research, scientific evaluation and even in our daily life. Various types of threats that can attack these devices, and the security solutions proposed by various researchers to handle these attacks become a piece of important technical discussion in the current scenario. This paper focuses on various attacks and security schemes on the RFID system. The contribution of this paper can be described in the following points:

- The work starts with presentation of the architecture of IoT in detail.
- This paper discusses various attacks possible on the RFID system in terms of confidentiality, integrity, and availability.
- This paper analyses various existing lightweight block and stream ciphers. These ciphers require to implement using the private-key and public-key cryptography.
- This paper also analyzes the existing lightweight and ultra-lightweight authentication scheme for the RFID system, i.e., taxonomy of various security schemes, to deal with the security attacks, is analyzed under the criteria cryptography approaches, privacy, authentication, authorization, and availability.

The rest of the paper consists of six sections. The next section defines the general architecture of the IoT system. The section includes a general overview of the RFID system, wireless sensor network, and a smart card. “[Security issues in RFID system](#)” presents various attacks possible on RFID devices. This section includes the attacks based on the CIA (confidentiality, integrity, and availability) properties of the RFID system. “[Taxonomy of defence mechanisms of RFID system](#)” presents an analysis of various security schemes proposed to deal with security attacks. “[Open issues and challenges](#)” discusses various challenges that still exist in implementation of RFID systems, and the last section concludes the paper.

Architecture of IoT

Figure 1 presents the architecture of IoT. There are three layers in IoT: the perceptron layer (physical layer), middleware layer, and application layer [19].

Perceptron layer

Perceptron layer consists of objects like sensors, actuators, readers, tags, and smart cards. It receives data from the IoT objects and sends it to the middle layer of the IoT layer. The remaining of this section describes the general overview of the Smart Card, Wireless Sensor Network, and RFID.

RFID

RFID [20] is used to identify objects in the network. It contains two components: Tag and Reader. The Tag is a small circuit that communicates with the Reader. Tag is divided into three types: passive Tag, semi-passive Tag, and active Tag. The passive Tag receives power from the Reader and performs simple operations like XOR, OR, AND. Furthermore, the passive Tag consists of low storage capacity, i.e., 1 KB, and comprises a short working range from 4 to 15 feet. A semi-passive tag contains battery power and uses it only, when the Tag is not in the range of the Reader. When a semi-passive tag enters the Reader’s communication range,

Fig. 1 IoT architecture

it takes power from the Reader, similar to a passive tag. The semi-passive has a long lifespan than active tag [14].

The active Tag consists of a small battery that supplies power to the tag [21]. The active Tag can be efficient to compute massive computational operation, as it has larger storage capacity than other types of Tag. It can operate in a more extended range up to 300 ft. In the Reader's case, the Reader reads information from the Tag and processes these pieces of information. The Reader comprises of various stored information, including tag identification number, security key, and other related information. Hitachi developed an ultrahigh-frequency tag of size $2.5 \text{ mm} \times 2.5 \text{ mm} \times 0.4 \text{ mm}$. These tags have Electronic Product Code (EPC) memory of size 128 bit (16 Byte) and Tag identifier (TID) memory of size 96 bit. Figure 2 represents the general interaction of tag with the RFID system.

According to RFID security, RFID tags are categorized into four classes: full-fledged class, simple class, light-weight class, and ultra-lightweight class. In full-fledged,

Tag requires a classical cryptographic operation. However, these tags require massive power and massive computational overhead. In simple class, RFID schemes need an elliptic curve, hash function, and random number generator to compute mutual authentication between Tag and Reader. These schemes require less power and computational overhead than full-fledged schemes. Lightweight schemes require hash function, checksum, and the random number for authentication. Ultra-lightweight class only uses simple bitwise operations like XOR, OR, AND, and Rotate operation. Hence, the ultra-lightweight class requires the lowest amount of power and computation. Figure 3 represent the general architecture of the RFID system.

Smart card

A Smart Card is a card that contains an embedded chip in it, and this chip acts as a token. The smart card receives power from the Reader like a passive tag. Smart cards

Fig. 2 Interaction of tag with the RFID system

Fig. 3 General architecture of RFID system

can be used in various real-time applications like banking system, credit card, computer security system, and government identification number. However, there are various attacks possible on Smart Card, including the power analysis, replay attacks. Smart Card comprises of skimming's or counterfeits fault. In this fault, the adversary can copy the magnetic stripe information to another card to use the information for performing false transactions [22].

Sensor node

Wireless sensor network (WSN) consists of a large number of sensor nodes and base stations [23]. The sensor node consists of the chip that comprises a battery, memory, transceiver, and transducer. The sensor node contains a short-communication range capacity, limited storage, small processing capacity, and low bandwidth. Thus, the sensor node collects data and takes action through the actuator. The wireless sensor network is used in many domains like military application, health monitoring, and environment exploration. Due to power constraints, the node sleeps at a particular interval of time. It cannot communicate with another node at that time. There are two types of deployments of sensor nodes, namely regular deployment, and random deployment. In regular deployment, the minimum sensor nodes are placed at the pre-determined location to cover all the desired areas. In random deployment, the sensor nodes are placed randomly in the network [24–26].

Middle-ware layer

This layer collects data from the Perceptron layer and sends it through Wi-Fi or Bluetooth to the application layer. This layer is divided into two parts: the first part consists of a gateway and networking layer. The second part consists of the management layer [21]. The gateway and networking layer is used to connect the sensor node and mobile node through the WAN (GSM, LTE) [27].

Application layer

The application layer is the topmost layer of IoT. It is connected to the middleware layer and used to collect information from the middleware and analyze these pieces of information. This application provides the IoT system available to the end-user. The application layer supports the various services for logistics, pollution monitoring, smart home, and smart transportation [6–8].

Security issues in RFID system

The RFID scheme consists of several classes of tags and reader. These tags include an inadequate amount of memory and low-power capacity. However, there are numerous other issues in terms of privacy, forward security, and authentication. Due to these security issues, there are several attacks possible on RFID systems like tag cloning, disclosure, spoofing, replay attack, etc. Figure 4 shows various attacks possible on the RFID system. This section discusses all possible attacks on RFID systems by categorizing them into three categories: confidentiality, integrity, and availability.

Confidentiality

In a computer network, confidentiality is defined as accessing sensitive information and protected data by an authorized user only. In confidentiality, privacy is the primary concern for a legitimate user. However, there are various threats such as side-channel, tracking, eavesdropping, key compromise, and privacy violation that can affect this primary concern.

Side channel attack

In this type of attack, the adversary can extract stored information from the RFID system by exploiting electromagnetic

Fig. 4 Possible attacks on RFID system

fields. This attack can be performed using the power analysis method that comprises extracting information using a variety of power supply. Differential power analysis can also perform a side-channel attack.

Tracking attack

In the tracking attack, the attacker is able to guess the correct tag ID, various tag IDs are already known to him. This attack targets the confidentiality of the data [28, 29].

Juels–Weis challenge-response model [30] Juels–Weis challenge-response model is a un-traceability model, which comprises a single reader and “ n ” number of the tags. The tag stores a pseudo-random number, and private key is reset after the execution of the challenge-response model. There are various messages used by the attacker such as SetKey, TagInit, and ReaderInit. The SetKey message is used to assign a new private key to the tag. The tag receives the SetKey packet, and changes the previous key value to an arbitrary private key. The TagInit message is used to initialize the current session, and to discard the previous session of the tag. Figure 5 shows functionality of the tag. The ReaderInit messages are used to initialize a current session to a reader R. An adversary can issue the queries, namely execute, send, corrupt, and test.

- **Execute (R, T, j):** In the execution phase, the adversary A eavesdrops actual packet of the protocol between the tag (T) and reader (R) in session “ j ”.
- **Send (P_1, P_2, j, m):** In the send phase, the adversary can impersonate party A which may be the tag or a reader in session “ j ”, and sends the message “ m ” to another party B.
- **Corrupt (T, K):** It is a SetKey query, in which adversary changes the key “ k ” of the tag ($T \in \text{Tag}$).
- **Test (T_1, T_2, j):** The test query randomly chooses bit $b_1 \in \{0, 1\}$ for session “ j ” and then adversary is given ID_{b_1} from $\{ID_1, ID_2\}$, and if adversary guess bit “ b_1 ”, then the adversary succeeds.

Un-traceability is defined as game between the adversary and party. The primary goal of the adversary is to find correct ID of the tag. There are three phases of this game to compute identity of the tag for strong authentication and strong integrity (SASI) scheme [28, 31], namely learning phase, challenges phase, and guessing phase.

- **Learning phase:** In this phase, the adversary executes query to eavesdrop the messages between the reader and tag to obtain C and D.
- **Challenges phase:** The adversary chooses two tags T_0 and T_1 with identifier ID_1 and ID_2 where $ID_1 = 0 \bmod 2$, and $ID_2 = 1 \bmod 2$.

- **Guessing phase:** In this adversary guess b' , such that $b' = S_{\text{LSB}} \oplus R_{\text{LSB}}$.

Eavesdropping attack

The Eavesdropping attack is a passive attack. The tag comes in a range of the reader. Then, the communication takes place between tag and reader. During the exchange of information, the attacker steals information or message packets communicating between tags and the reader. Figure 6 represents the general overview of eavesdropping attack on the RFID system.

Disclosure attack

In a disclosure attack [32–34], the attacker would be able to guess secret information like shared key, ID, and other secret information from the RFID system. There are two types of disclosure attacks possible on the RFID system, such as identity disclosure attack and full disclosure attack. In an identity disclosure attack, the attacker steals the identity of the tag. In full disclosure attack, the attacker retrieves all the information stored in the tag [35]. Masoumeh et al. [36] proposed disclosure attack on ultra-lightweight authentication protocol [37]. In this attack, there are two phases, namely the learning phase and passive secret disclosure attack. In learning phase, the adversary eavesdrops one session of the protocol. It collects the messages including IDS_{old} , IDS_{new} , P , Q , R , and S , where IDS_{old} represents old pseudo-random ID of tag, and IDS_{new} represents new pseudo-random ID of tag. In passive secret disclosure phase, the adversary uses these eavesdropping values to compute IDS_{old} , K_{old} , IDS_{new} , K_{new}

Fig. 6 Eavesdropping attack

Fig. 5 Tag functionality of the Juels–Weis challenge-response model

n , and m . The disclosure attack can be performed using two methods: recursive linear attack and recursive differential attack. The recursive linear cryptanalysis is a passive attack, and it requires only one authentication session to perform a disclosure attack. This attack exploits the T-functionality of the protocol. In this attack, the adversary first finds all the unknown parameters within the protocol. Then, it creates a linear equation for all its hidden variables. Recursive differential cryptanalysis (RDC) attack consists of a probabilistic attack. It requires more than one authentication session to perform this attack [38].

Impersonation attack

In these type of attacks, the adversary targets the security measure used for authentication of the RFID reader. The probability of these type of attacks may rise from “very easy” to “practically impossible”. For example, it may happen that the adversary steals the reader that has been used to store all the credentials, which, in turn, provides him/her access to the back-end systems along with the RFID tags.

Integrity

Integrity ensures consistency, the trustworthiness of data, while transmission through communication channels may get modified by unauthorized people. There are various threats to attack the integrity of RFID systems are: tag cloning, spoofing attack, replay attack, and relay attack.

Tag cloning

In the cloning attack, the attacker establishes a duplicate tag node similar to the existing tag node [39]. Thus, the reader is not be able to validate the attacker tag node, and the attacker becomes able to have unauthorized access to the reader [40]. By snooping the reader-tag communication,

the cybercriminals can extract tag data and write them into another tag. Tag cloning deceives the reader from getting authorized access, incurs financial losses, and damages company’s brand value.

Replay attack

In this attack, the attacker eavesdrops packet between the tag and reader [41]. Then, the attacker transmits an old genuine packet many times to the reader. The reader verifies these genuine packets and gives credentials to the attacker node.

Spoofing attack

This attack is an impersonation type of attack, in which the adversary establishes malicious devices in the communication channel. The adversary impersonates a genuine tag node, and gets all its privileges and information stored from the genuine tag node. After that, the adversary stored these pieces of information in the malicious node.

Man-in middle attack

This attack consists of modification of eavesdrop message packets. This attack is an active attack. In this attack, the adversary places malicious devices in a communication channel between legitimate tag and the reader. Then, the adversary believes that this tag/reader is a legitimate reader/tag. Hence, a genuine tag/reader interacts with this malicious device. Figure 7 describes the diagram of the Man-in middle attack.

Malicious code injection

As the name describes, in this type of attack, the RFID network entities such as readers, communicating networks, or devices, etc. are affected by spreading hostile code by an

Fig. 7 General diagram of man-in the middle attack

attacker. The available memory of RFID tags is used to propagate and store the malicious code or viruses in the back-end system. Although such type of vulnerabilities is rare, however, existence of these cannot be denied. The adversary may attack the middleware systems using this attack, as various scripting languages like XML, PHP, etc. are used by various middleware applications.

Availability

In a computer system, the availability refers to the genuine user's access resources or information at different specified locations. Data availability defines the consistency of data that must be available to a legitimate user. There are various threats to availability in RFID systems such as disabling tag, denial of service (DoS) attack, and desynchronization attack.

Jamming attack

In a jamming attack, the adversary stops communication between a genuine tag and the reader, such that the tag node cannot interact with the reader. The adversary creates a signal equivalent to the reader that makes the tag non-communicable with the Reader.

Denial of service attack

In this attack, the adversary blocks the RFID tag. RFID devices have limited storage capacity and low-power battery. Hence, the adversary takes advantage of this, and it transmits many packets to the communication channel. Due to this, there will be increase in bandwidth of the communication channel. Much power of the Tag is used in receiving these huge packets. Due to the power constraints, the RFID tag will get removed from the RFID system when the DoS attacks are performed in the RFID based systems. Distributed denial of service attacks (DDoS) are much powerful than the denial of service attack. There are various solutions for defending the DDoS attack using machine learning such as the honeypot intrusion detection system and many more [42, 43].

Desynchronization attack

In this attack, the adversary can break synchronization between the tag and reader [38, 44–46]. Paolo et al. [35] propose de-synchronization attack on SASI [31] scheme. The adversary eavesdrops message packets in the RFID system. After that, it transmits these message packets to tag. The tag validates these message packets. The adversary succeeds if the tag sends an authenticate packet to the adversary. After the successful authentication, the tag updates its shared key

and IDS. Hence, the adversary develops desynchronization between the tag and the reader.

In another way, the reader and tag contain old and new keys ($K1$, $K2$) and ids ($IDS1$, $IDS2$). When the tag comes in the range of a reader, it transmits IDS to the reader. The reader computes the authentication message and transmits it to the tag. The tag validates these packets and transmits authentication packets to the reader. After, the tag updates its key and IDS as $K2$, $IDS2$, and $K3$, $IDS3$, the adversary blocks these authentication message packets between the tag and the reader. Hence, the genuine reader cannot receive a reply from the tag. After that, the reader computes the authentication value from $K2$, $IDS2$, and transmits it to the tag. The tag authenticates message packet using $K2$, $IDS2$ and updates its key as $K3$, $IDS3$, and $K4$, $IDS4$. Hence, both the tag and reader contain different shared keys and IDS messages. Thus, the desynchronization occurs between tags and readers [47].

Covert channel attack

In these types of attacks, the adversary creates unwarranted communication mediums to transmit data secretly. The attacker secretly transfers the information by exploiting the unutilized memory space of different RFID tags, which makes it hard to recognize. For example, data related to daily activities or medical history of a human being can be stolen using a set of RFID tags that were otherwise installed for purpose of human identification, only.

Taxonomy of defence mechanisms of RFID system

As described in the previous section, confidentiality, integrity, availability, and authorization are essential properties of a secure RFID system. Therefore, this section describes the various security schemes proposed by different researchers to maintain such properties. The classification of these schemes has been done under the criteria cryptography approaches, privacy, authentication, authorization, and availability. In cryptography, key is an important aspect to defend the attack. There are two types of key in cryptography, i.e., public-key cryptography and private-key cryptography. The next two subsection describe about the public-key cryptography and private-key cryptography. After that, the remaining section describes the security schemes in terms of the privacy, authentication, authorizations, and availability.

Public-key cryptography

Asymmetric key cryptography or public-key cryptography consists of two different keys, i.e., a public key and private key.

The public key is used to encrypt data to form the cipher text. In contrast, the private key is used to decrypt the cipher text. In cryptography, there are various existing public-key cryptography schemes, i.e., RSA, Diffie–Hellman key exchange, etc. However, these schemes provide substantial computational overhead. Due to this, the elliptic curve cryptography was introduced, which requires a lessor computational overhead. The hash function is also used by the researchers to implement the public-key cryptography. There exist various traditional secure hash functions like SHA-2, SHA-256, etc. However, these hash functions also require massive computation. Therefore, there are various types of lightweight hash function proposed by the researchers [48, 49].

Lightweight hash function

A one-way hash function maps a string of arbitrary length to fixed length string. Hash function is defined as $\{h: A \rightarrow B\}$, where $A = \{0, 1\}^*$ and $B = \{0, 1\}^n$ for n -bit of an output length. There are various lightweight hash functions are available for RFID system like Quark [50], SQUASH [51], SPONGENT [48], Hash-One [49], and L-CAHASH [52]. Quark is a lightweight Hash function developed by Aumasson et al. in 2013. In this, there are three types of Quark, such as U-Quark, D-Quark, and T-Quark. U-Quark consists of 64 bit security, and requires 1379 gate equivalents (GE). D-Quark consists of 80 bits security, and T-Quark consists of 112 bits security, which requires 2296 GE [53].

Elliptic curve cryptography (ECC)

ECC is based on the algebraic structure over a finite field. It can be combined with a symmetric scheme to perform encryption. However, the ECC-based scheme may suffer from fault attack on the smart card [54].

Let A and B are points on elliptic curve over a finite field P and (x_A, y_A) , (x_B, y_B) represent points (A, B) on this curve. Then, equation represents elliptic curve as:

$$y^2 \equiv x^3 - X^3 + aX + b, \quad (1)$$

where a and b are constant, and then, λ represents slope of the lines and calculates as:

$$\lambda = \frac{y_B - y_A}{x_B - x_A}, \quad \text{if } A \neq B \quad (2)$$

$$\lambda = \frac{3x_A^2 - a}{2y_A}, \quad \text{if } A = B. \quad (3)$$

Private-key cryptography

Private-key cryptography (symmetric-key cryptography) employs a unique key for encryption and decryption. In the private-key cryptography, the unique key is shared between the sender and the receiver, and this process is called key-exchange. The private-key cryptography supports two types of ciphers, namely: block cipher and stream cipher. The block cipher contains a pre-determined collection of bits of plaintext for encrypting the block. The size of the block composes of 64 bits or can be smaller/larger according to the algorithm used by the researcher. There are various modes of operations for a block cipher including cipher feedback mode (CFB), electronic code-book mode (ECB), output feedback mode (OFB), and cipher block chaining mode (CBC). In CFB cipher, feedback provides the next block during encryption and decryption. This cipher uses the initialization vector (IV) to initialize the cipher. In the ECB mode of a cipher, the plaintext is divided into smaller blocks and then directly encrypts them using the key. The OFB mode contains the block cipher to generate the synchronous stream cipher. It generates the same using the XOR operation between the keystream block and the data block. The CBC involves the XOR operation between the data and previous cipher block to generate the cipher data. A stream cipher is generated using the combination of data and the pseudo-random keystream.

Privacy

Privacy is an essential concern for the RFID system. Generally, privacy is ensured using encryption. There are various encryption schemes for the power constrained devices in terms of block ciphers and stream ciphers.

Lightweight block cipher

A block cipher consists of encrypting a complete block of plaintext rather than a single bit like the stream cipher. According to the block cipher structure, there are various types of structures defined by the researchers like Substitution Permutation network (SPN), Feistel network, Generalized Feistel network (GFN), etc. The Feistel network divides block into two equal parts: left and right section, and function “ f ” applies on Feistel cipher. However, the SPN network consists of substitution and permutation layer along with the pseudo-random key. Figure 8 shows the general architecture of the block cipher in terms of the Feistel network and SPN network. There are various attacks possible on block cipher such as integral, fault [55], linear/differential cryptography,

Fig. 8 General architecture of SPN and Feistel network **Table 2** Detailed analysis of various lightweight block cipher

Scheme	Block size	Key size	Throughput	Cycle	Round	Type	Area (GE)	Operation	Vulnerability
RECHANGLE 80/128 [60]	64-bit/ 64-bit	80 bit/ 128-bit	246	26	25	SPN	1599.5/2063.5	–	side-channel attack [62]
LILLIPUT [68]	64-bit	80-bit	213	510	30	EGFN	1545	–	–
QTL-64/QTL-128 [69]	64-bit	64-bit	200	16/20	16/20	Feistel, SPN	1026/1206.52	Sboxes (4 * 4), ll, XOR, P, Round	Standard statistical [70]
LICI [71]	64-bit	128-bit	305	2518	16	Feistel	1153	–	–
BORON [72]	64-bit	128-bit/80-bit	96.02	7997.53	18	SPN	1939/ 1626	Shift, round, permutation, xor	Differential Power Attack [73]
SPN [118]	64-bit	96-bit	200	4736	32	SPN, Feistel	1876.4	Permutation, XOR, Round, Sbox	–
μ^2 [119]	80-bit	64-bit	148.28 Mb/s	–	16	Feistel	–	–	–
LRBC [120]	16-bit	16-bit	–	–	24	Feistel, SPN	258.9	–	Known attack [121]

etc. Table 2 presents the detailed analysis of various light-weight block ciphers for the RFID system.

Bogdanov et al. [56] proposed a block cipher and named this block cipher as “PRESENT”. The PRESENT is an ultra-light weight cipher for the low computational devices. This

cipher consists of 64-bit block length and supports two different key lengths, i.e., 80 bits and 128 bits.

The author suggested that the PRESENT cipher is used in those applications that require a moderate level of security. Space and power are another essential consideration for the implementation of the PRESENT cipher. However, the

algebraic, statistical saturation, linear, and invasive attacks are possible on the PRESENT cipher [57, 58]. In 2011, the author proposed a lightweight cipher and named it as TWINE [59]. This cipher consists of 64-bit of block size and supports two 128-bit and 80-bit keys. This scheme uses a 4-bit XOR operation and 4-bit S-box. RECTANGLE [60] is a lightweight block cipher, and it uses the SPN network. It consists of 16 S-boxes of size 4×4 in parallel. RECTANGLE scheme supports an 80-bit key as well as a 128-bit key. It requires 1600 gate on the 80-bit key size at 246 Kbit per second throughput in the 100-kHz clock cycle. For the 128-bit key, it requires 2063.5 gate equivalent. RECTANGLE scheme also consists of 26 cycles and requires 25 rounds for computing the cipher. However, Selvam et al. [62] revealed a related key and side-channel attacks on the RECTANGLE scheme.

The SIMECK block cipher [63] consists of a modified SIMON round function for designing the block cipher. It contains SIMECK block cipher that uses a round function, key schedule, and key constant for designing the block cipher. The word size for the SIMECK cipher is 16 bit, 24 bit, and 32 bits. SIMECK consist of $n + 1$, $n - 1$, and n combinational circuits for XOR, XNOR, and AND gates, respectively. The SIMECK block cipher is designed to provide a smaller area than the SIMON block cipher, but it has the same security level. Bagheri et al. [64] performed cryptanalysis of SIMECK block cipher, and found that the block cipher is vulnerable to reduced round attack [65–67].

Berger et al. [68] proposed another lightweight block cipher using the EGFN network and named this cipher as LILLIPUT. This cipher worked on 80-bit key size and 64-bit block size. LILLIPUT cipher requires a 65-nm logic process and 1545 GE for computing encryption. Also, LiLIPUT cipher performs 213 Kbit per second throughput for encryption and decryption. The authors suggested that the LILLIPUT cipher is secure against various classical attacks

like impossible differential, integral attack, and linear or differential cryptanalysis.

Li et al. [69] proposed an ultra-lightweight cipher QTL using the generalized Feistel network structure for resource constraint devices. This cipher supports 64-bit and a 128-bit key. QTL scheme supports the S-boxes of size 4×4 , concatenation operation, XOR, and permutation operation. QTL supports 1026 and 1206.52 gate operations for computing QTL-64 and QTL-128, respectively. However, QTL cannot resist from standard statistical attack [70].

Jagdish et al. [71] developed a lightweight cipher and named as LiCi. It consists of 31 consecutive rounds with lightweight S-boxes of size 4×4 . Also, this algorithm supports 64-bit plaintext along with a 128-bit key size. The LiCi algorithm consists of 1153 GE, 30-mW power, and 1944 bytes of memory. The author suggested that the LiCi cipher resists from Zero correlation, Biclique, and linear/differential attack.

Bansod et al. [72] proposed an SPN-based lightweight cipher and called as BORON. BORON cipher supports two key sizes of length 80-bit and 128-bit along with 64-bit block size. This scheme uses XOR, shift operation, permutation, and S-boxes to design a block cipher. BORON cipher provides a throughput of 96.02 Kbit per second. It consists of 18 rounds and 7997.53 cycles for designing the cipher. BORON cipher design consists of hardware and software along with 1626 gate equivalent for the 80-bit key, and 1939 gate equivalent for 128-bit key size. The authors suggested that the BORON cipher is resistant to linear/differential cryptanalysis and zero correlation attack. Sutar et al. [73] found a vulnerability in BORON cipher, and claimed that the BORON cipher cannot resist differential power attack.

Lightweight stream cipher

A light stream cipher requires low computational complexity, but achieves high level of security, while creating cipher

Table 3 Detail study of various lightweight stream cipher

Stream cipher	Key size	Initialization vector (IV)	Type	Gate equivalent (GE)	Vulnerability
WG-8 [78]	80-bit	80-bit	LFSR, WG	–	Key recovery attack [79]
ALE [80]	128-bit	128-bit	SNP	–	Leaked state forgery [81], LOCAL attack [82]
ACORN [86]	128-bit	128-bit	6LFSR	–	Differential fault attack [122]
SVH [83]	64-bit	64-bit	Dual pseudo-random transformation and output feedback	1171	–
Fruit [84]	80-bit	70-bit	LFSR, NFSR	990	Full round attack [123], correlation attack, and divide and conquer attack
Lizard [85]	120-bit	64-bit	LFSR, NFSR, feedback shift registers (FSRs)	1161	Differential fault [86]
Fruit-80 [124]	80-bit	70-bit	LFSR, NFSR	960	Fast correlation attacks [125]

text for a given plaintext. It combines pseudo-random shared key with the plaintext to perform the encryption of plaintext. There are various types of stream ciphers with regard to its structure such as linear-feedback shift register (LFSR), nonlinear feedback shift register (NFSR), shift register with carry feedback (FCSR), PANAMA, random shuffled, addition/rotation/XOR (ARX) [74]. Table 3 presents an analysis of various existing lightweight stream ciphers. The analysis has been done in terms of key size, initialization vector (IV), type, gate equivalent (GE), and vulnerability of the stream cipher. There are various vulnerabilities that affect a stream cipher, which mainly include side-channel, time memory trade-off, linear masking, and related key attack.

Nawaz et al. [75] used Welch Gong (WG) transformations to propose a novel synchronous stream cipher. The family of Welch Gong (WG) stream cipher consists of excellent property of randomness, and this stream cipher efficiently executes on resource-constrained devices. Fan et al. [76] optimized the WG-16 cipher using composite field arithmetic. Later on, Zidaric et al. [77] proposed hardware optimization of WG-16 stream cipher with tower field arithmetic.

In 2013, Fan et al. [78] proposed a stream cipher and named as WG-8. This cipher also belongs family of Welch Gong (WG)-based cipher, and consists of randomness and cryptographic property. The authors used an 80-bit key

size for the stream cipher. However, this scheme does not provide resistance from a key recovery attack [79].

Bogdanov et al. [80] proposed AES-based stream cipher and named as AES-Based Lightweight Authenticated Encryption (ALE). This stream cipher consists of a 128-bit key size. However, Wu et al. and Khovratovich et al. [81, 82] claimed that the ALE cipher cannot resist from leaked state forgery attack and LOCAL attack. The scheme proposed by Dai et al. [83] uses the 64-bit initialization vector and 64-bit key. This scheme uses 1171 GE operations during the process. Fruit [84], a light weight stream cipher, was proposed by Ghafari et al. The scheme is based on the LFSR and NFSR shift cipher. It uses the 80-bit key size, and also provides 990 GE operation for computing encryption. However, there are various vulnerabilities from which the Fruit-based cipher scheme suffers from, such as full round, divide and conquer, full round attacks, etc.

In 2017, Hamann et al. [85] proposed a lightweight cipher for RFID devices and named it LIZARD. The authors claimed the cipher to be hardware efficient as it combined FP(1) mode and Grain-like structure. The scheme consists of a 64-bit initialization vector and a 120-bit security key. However, Wu et al. [86] proved vulnerability of LIZARD security scheme toward the differential fault attack.

Table 4 Notation used for RFID authentication schemes

Symbol	Description
SetKey	To assign new secret key to the Tag
TagInit	Initialize session key by the Tag
ReaderInit	Initialize session key by the Reader
R	RFID Reader
T	RFID Tag
$A, B, C, D, S, R, X, X_1, A'', B''$	96-bit numbers generated by the Tag and Reader to compute mutual authentication
A', B', C'	96-bit numbers modify by the attacker to unauthorized to the system
IDS	Pseudo-random id of the Tag
ID	Unique Id of the Tag
A_{win}	Success of the adversary
K_c	Pseudo-Kasami code
ID_1, ID_2	Two different IDs of the Tag given to adversary
K, K_1, K_2	96-bit shared key between Tag and Reader
r	Random number
s	Private key of the Reader
m	Message
$x \gg y$	Right rotation of x in y times
$\oplus$	Xor operator
K_x, K_y	Points on elliptic curve
TK_{t1}, TK_{t2}	Intermediate value generated by the Tag to compute authentication
$C_1, C_2, S_n, T_s, Auth_s$	Server transmits messages to the Tag to compute mutual authentication
$Auth_t, R_t, R_1, T_1, T_2, v$	Tag transmits messages to the server to compute mutual authentication
Z_T	Tag public key

Authentication

Authentication is an important concern for RFID devices. This section describes various types of lightweight authentication schemes as well as ultra-lightweight authentication scheme. Table 4 describes notations used in this paper. A lightweight authentication scheme consists of public-key cryptography, i.e., elliptic curve, hash function. The ultra-lightweight scheme consists of symmetric-key cryptography that uses simple operations such as OR, AND, XOR, and ROT. Table 5 consists of various existing authentication schemes for RFID.

Lightweight schemes

Lee et al. [87] proposed a lightweight authentication scheme using the elliptic curve implementation. In this protocol, the server selects a pseudo-random number, and forwards it to the tag. After receiving a random number from the server, the tag selects a random number and computes the values T_1 , T_2 , and v . The tag transmits T_1 , T_2 , and v to the server. The server computes the value X_2 and validates the Tag. This scheme provides unilateral authentication in which the server only verifies the genuineness of the tag. In this scheme, the system's memory requirement for storing private-key and public-key is 652 bits, and communication overhead between networks is 82 bytes. However, Bringer et al. [88] found security issues such as tag impersonation attack and tracking attack in this scheme.

Liao et al. [41] modified the scheme proposed by Lee et al.'s scheme to propose a lightweight mutual authentication scheme. The scheme provides mutual authentication between the tag and server. This scheme also implements elliptic curves to compute the value T_s from a random number, and forwards it to the Tag. The tag evaluates the values $Auth_t$, R_t , and sends the same to the server. The server validates the tag, and sends $Auth_s$ to the Tag. The tag validates the server, and mutual authentication takes place between the tag and the server. This scheme consists of 1280 bits of communication overhead, and uses five multiplications during authentication. The author claimed that this scheme provides anonymity, forward security, availability, and resistance from the impersonation attack.

However, Zhao et al. [89] discovered a security flaw in the scheme proposed by Liao et al., i.e., key compromise. To eliminate its problems, Zhao et al. proposed a scheme that uses values K_x and K_y to generate TK_{t1} , TK_{t2} . It computes $Auth_T$ from the value Z_T , TK_{t1} and TK_{t2} . The tag forwards the values $Auth_T$ and R_1 to the Server. After receiving $Auth_T$ and R_1 , the server validates the tag and sends a message to the tag. In this scheme, the total memory required for private key and public key is 652 bits, and communication overhead between tag and Server is 82 bytes. The tag also validates server, and mutual authentication takes place between tag and server. The authors claimed that this scheme provides security against various security issues such as key compromise, mutual

Table 5 Detail study of existing authentication schemes for RFID environment

Scheme	Operation	Storage	Communication	Vulnerability
LMAP [96]	$+$, OR, $\oplus$	6L ^a	2L ^a	Desynchronization, disclosure attack and tracking attack
SASI [31]	$\oplus$, OR, ROT	7L ^a	2L ^a	Desynchronization, disclosure, and tracking attack
Gossamer [99]	ROT, $\oplus$, MIXBITS	7L ^a	5L ^a	Desynchronization attack
Yeh et al. [100]	NOT, XOR, OR, ROT	3L ^a	2L ^a	Desynchronization attack, full disclosure attack, traceability attack, and formal security attack
RAPP [44]	ROT, $\oplus$, Per operation	5L ^a	2L ^a	Desynchronization attack
R ² AP[101]	XOR, ROT, and Rec(A, B)	5L ^a	7L ^a	Desynchronization attack, disclosure, tracking, and security of diffusion function
Zhao et al. [89]	Ecliptic curve cryptography	652 bits	82 bytes	Key comprises problem, replay attack, cloning attack, impersonation attack, spoofing attack, tracking attack
Shen et al. [94]	Elliptic curve cryptography, hash function	—	1440 bits	Server spoof attack and a replay attack
Ryu et al. [93]	Hash, elliptic curve	—	960 bits	Mutual authentication
Tewari et al. [37]	$\oplus$, Rot	7L ^a	3L ^a	Disclosure attack
KMAP [47]	$\oplus$, Rot	7L ^a	4L ^a	—
SLAP [102]	$\oplus$, Rot, Con(A, B)	7L ^a	4L ^a	—
Kumar et al. [127]	Hash, elliptic curve	—	800 bits	—

^aWhere L is equal to 96 bits

authentication, tracking, cloning attack, DoS attack, server spoofing attack, forward security, and replay attack.

He et al. [90] proposed an authentication scheme for the RFID system with an ID verifier transfer protocol. This scheme consists of 1440 bits + 480w bits of storage capacity for the server, and 1760 bits of storage capacity for the tag. Hence, the total storage requirement of the RFID system is 3200 and 480w bits. The elliptic curve's running time for multiplication operation on 5 MHz tag is 0.064 s, and PIV 3 GHz server is 0.83 ms [91, 92]. The authors found that the running time for server and tag to compute elliptic multiplication is 2.49 ms and 0.192 s. The communication cost of this scheme for server and tag is 640 bits each. Hence, the total communication cost between the tag and the server is 1280 bits. This scheme comprises of mutual authentication between the tag and the reader, and has the properties of confidentiality, anonymity, availability, and forward security. It also provides resistance from various attacks like DoS attack, replay attack, and tracking attack.

Ryu et al. [93] proposed another authentication scheme for the RFID system. This scheme requires $2 \times T_H$ and $2 \times T_M$, where T_H is the time required to compute hash function, and T_M is defined as the time required to compute elliptic multiplication. This scheme consists of 960 bits of communications cost for the RFID system. This scheme provides resistance from various attacks like traceability, forward security, server spoofing, and cloning. However, this scheme does not provide mutual authentication between RFID devices.

Shen et al. [94] introduced an RFID authentication scheme that uses a hash function and elliptic curve. The author reviewed the scheme proposed by Chen et al.'s scheme [95], and claimed that the scheme does not resist various attacks such as spoofing attacks and replaying attack. In the scheme proposed by Shen et al., the server selects a random number. It calculates values C_1 and C_2 , then a value s_n is calculated from C_1 , C_2 , r , and s , where r represents a random number, and s represents the private key of the server. The server sends C_1 , C_2 , and s_n to the tag. The tag validates C_1 , C_2 , and s_n . If the message is from the valid server, then it computes the values C_3 , c , and d . The tag forwards it to the server; otherwise, it rejects the packet. After receiving the packet from the tag, the server validates the ID of the tag using a hash function. If the validation is successful, then mutual authentication takes place between the server and the tag. This scheme requires 1440 bits of communication overhead, and uses three hash functions and four multiplications during mutual authentication. The scheme provides un-traceability, forward security, and resistance from a cloning attack. However, this scheme is not resistant to a server spoof attack and a replay attack.

Ultra-lightweight schemes

LMAP [96] is a lightweight mutual authentication protocol. It uses four shared keys between the reader and the tag. This protocol uses one pseudo-random number to create values A , B , C , and forwards these values to the Tag. After receiving the message, the tag computes the value B' and checks whether B' is equal to B or not. After successful authentication, the reader generates the value D and forwards it to the tag. After receiving the message, the tag also computes D' and verifies the reader. After successful mutual authentication, tag and reader modify the value of IDS key. This protocol provides security against the man-in-middle attack, data confidentiality, and forward security. However, this protocol cannot protect the system against the desynchronization, disclosure, and tracking attacks.

In 2006, Peris et al. [97] proposed an Efficient Mutual-Authentication Protocol (EMAP), lightweight authentication scheme for RFID system. The scheme uses various bitwise operations like OR, XOR, AND, etc. This scheme requires 6L-bits storage cost for authentication, and communication cost between tag and reader is 5L-bits. This scheme provides data integrity, mutual authentication, forward security, user data confidentiality, and tag anonymity. This scheme also provides resistance from various attacks like man-in-the-middle attack and replay attack. However, this scheme cannot provide resistance from various attacks such as desynchronization attacks, disclosure attacks, and tracking attacks.

In 2006, Peris et al. [98] proposed a lightweight authentication scheme for the RFID system and named as minimalist mutual-authentication protocol (M2AP). The scheme uses various bitwise operations OR, AND, XOR, and +.

SASI [31] algorithm is an ultra-lightweight scheme, which uses XOR, OR, and Rot function to perform the authentication. The scheme contains three phases, namely, tag identification, mutual authentication, and key updating. In the first phase, the tag enters the range of the reader. Then, the tag receives “hello” packet from the reader. After receiving the “hello” packet, the tag sends old IDS (pseudo-random ID) to the reader for verification. The reader computes A , B , C values and forwards these values to the tag. The tag computes C' from A and B , and verifies C' is equal to C or not. Then, the tag validates the reader. It computes D and forwards it to the reader. The reader computes D' from the ID and Key, and validates the tag. After successful authentication, the reader and tag update their key and IDS value. This algorithm provides security against mutual authentication, data integrity, replay attack, forward security, and man-in-middle attack. However, this algorithm cannot protect the desynchronization attack, disclosure attack, and tracking attack.

Gossamer scheme [99] is an ultra-lightweight protocol, which uses XOR, +, AND, Rotate, and MixBits operations.

The MixBits operation is used to provide security against the desynchronization and disclosure attacks. The author claimed that it is difficult for the attacker to perform the desynchronization attack in the Gossamer protocol.

Yeh et al. [100] proposed a process-oriented ultra-lightweight RFID authentication protocol that required 3L bits memory space for the tag. The authors claimed their scheme to have better tag memory utilization, and to be more secure with less computation overhead. However, this scheme also suffered from various security issues such as desynchronization, full disclosure, traceability, and formal security attack [47].

Zhuang et al. [101] proposed an ultra-lightweight authentication scheme in 2014 and named this scheme as R^2AP . This scheme uses a bitwise operation such as XOR, ROT, and $Rec(A, B)$. As per the presented scheme, the total memory requirement on tag to compute mutual authentication between tag and reader is 5L, and communication cost for transmitting and receiving messages is 7L. The scheme provides mutual authentication, forward security, and also, is resistant from various attacks such as man-in-the-middle attacks. However, this scheme cannot provide resistance from various attacks such as desynchronization attack, disclosure attacks, tracking attack, and security of diffusion function [102].

Mujahid et al. [103] proposed an ultra-lightweight authentication scheme named RCIA for RFID system using a recursive hash function. In this scheme, the total memory requirement on tag to compute mutual authentication between the tag and the reader is 7L, and the communication cost for transmitted messages and receiving messages is 6L. In these total messages, the communication messages cost generated by the tag is 2L. This scheme provides resistance from various attacks like desynchronization, disclosure, tracking, mutual authentication, and replay attacks. However, this scheme cannot provide resistance from the diffusion function.

The protocol proposed by Tewari et al. [37] implements the double rotate function used to generate the authentication credential. The author claimed that this scheme provides much better security in the desynchronization attack than SASI protocol. This protocol additionally uses two random values to implement the scheme. The author also claimed that this scheme provides security against the replay attack, man-in-middle attack, data confidentiality, and forward security. Still, this algorithm cannot provide security against the disclosure attack.

KMAP [47] is an ultra-lightweight mutual authentication protocol in which it implements bitwise operation such as XOR and left circular rotate. It uses pseudo-Kasami code to provide security against the desynchronization attack. The pseudo-Kasami code (K_c) consists of three phases. The first phase consists of bit selection in which it selects bits

according to the seed value. The second phase contains the left rotate value of X , and the last phase involves XOR for the value X and X' . The memory requirement on tag is 7L, and also, communication messages generated by tag are 2L. In this scheme, the total number of messages for mutual authentication is 4L. This scheme provides security against the man-in-the-middle attack, replay attack, tracking, and forward security.

SLAP [102] is Succinct and Lightweight Authentication Protocol, which implements left rotate, $\oplus$ and $con(A, B)$ function. The author uses $con(A, B)$ to provide resistance from a desynchronization attack. The $con(A, B)$ consists of three phases: grouping, rearrange, and composition.

- Grouping phase splits the value of A and B according to the threshold value.
- Rearrange phase consists of exchange bit of A' and B' , and then rotating bit according to the hamming distance to form A'' and B'' .
- Composition phase performs XOR of values A'' and B'' and calculate the value of $con(A, B)$.

SLAP provides security against mutual authentication, resistance to man-in-middle attack, resistance from replay attack, resistance from the forward security, disclosure, and tracking attack. Table 5 shows various authentication schemes for RFID environment.

Availability

Another important security issue that an RFID system has to deal with is availability of the data for its legitimate users. Attacks such as DDoS affect an RFID system to a great extent. The RFID tags easily get separated from the RFID system due to the DDoS attack. Therefore, it is essential to mitigate the DDoS attack from the RFID system. There are various defence mechanisms which are available to handle the DDoS attack in IoT system like learning automata-based defence [104], blockchain-based defence [105], software-defined networking base defence model [106], machine learning-based defence mechanism [107–109], and IoT middleware-based DDoS defence mechanism [110]. The Learning automata-based defence mechanism uses service-oriented architecture (SOA) and cross-layer model. The blockchain contains the self-executable computer program, and the machine learning-based defence model uses the supervised and unsupervised learning models [42].

Authorization

It is essential to trust the validity of the data to solve the challenges of the economic or environment problems using the IoT system. This can be done using access control

mechanism. In the access control mechanism, the information is prevented from unauthorized users. There are various models to implement access control mechanisms like role-based access control model (RBAC), credential-based access control model (CBAC), and trust-based access control model (TBAC).

The role-based access control model defines the authority and management rights of the users. This model authorizes the different types of users to access the information. It allows the user to read, write, and modify the data. Hence, this model also provides privacy to the user [111, 112].

The user requires a digital credential by the trusted third-party certificate to access the resource data in case of credential-based access control model. The credential-based access is divided into two types of accessing models, i.e., attribute-based access control model (ABAC) and capability-based access control model (Cap-BAC). The ABAC model comprises of the rights that are assigned to the user to access the information using the defined policies. The attribute-based access control model also named as the policy-based access control model. The policies defined in the model involves many different type of attributes like user attributes, object attributes, resource attributes, contextual attribute, etc. The user attribute contains the information (e.g., age, department, and role) about the user. The object attribute defines the resources that are accessed by the users. The action attribute involves the activities that can be performed by the users like read, view, delete, and modify. The contextual attributes contain information about the location or time, such that the user can access the data at a particular interval of time or location [113]. The capability-based access control model requires an authorization certificate to be generated for the requestor. These certificate is given by the data owner to the requestor to access the data [114].

The trust-based model for the IoT involves the trustworthiness of the IoT device. The trust-based access model uses multi-dimensions in terms of the categories and subcategories [115, 116].

Open issues and challenges

In the last few decades, the scientists and researchers have developed several security schemes to make RFID systems resistant toward different threats and attacks. However, there is no full-proof mechanism available to secure RFID system against all types of attacks. Whenever a new security scheme is proposed by some researcher, the attackers modify their strategy to attack the system. Hence, there is always room for improvement in the existing security schemes, i.e., there are many issues that are still open. This keeps the researchers always motivated to work in this important area of designing complete solutions for RFID system. This

section presents several issues and challenges presented in the existing mechanisms.

Challenge to develop ultra-lightweight scheme

As IoT devices have small battery size and low memory capacity. Hence, there exists always a challenge to develop ultra-lightweight security schemes that overcome these constraints and provide security against all types of RFID attacks, as well. The discussion above has presented many ultra-lightweight schemes for security techniques for the RFID devices that use XOR, Rotate, OR, and AND operations. However, these schemes do not provide security against various types of attacks such as desynchronization, disclosure, and racking attacks [28, 47]. Therefore, to develop a scheme that provides resistance against all types of attacks is still an open challenge. Moreover, the researchers can always work in the area of reducing requirements of battery and memory capacity for IoT devices.

Challenge to develop secure authentication mechanism

To verify the identity of communication device in RFID system is an important and essential concern. As described in the above sections, researchers have exploited various techniques such as symmetric-key cryptography, elliptic curve cryptography, etc., to provide authentication for RFID systems [89, 92, 93]. However, to develop a single scheme that deal with all types of authentication issues is still open challenge for researchers.

Challenge to develop a lightweight secure hash function

In the various RFID schemes proposed by the researchers, hash function has been used as an important tool to implement authentication and integrity criteria of RFID system. However, the hash functions have massive computation overhead. Opposite to it, the RFID devices have limited computation power. Due to the limitation of computational capacity, it is difficult to provide security against various security threats [28]. That is, the hash function should provide a smaller output size and secure communication at low computational cost. Hence, developing hash functions with less computation overhead is another challenge for the researchers.

Challenge to develop efficient block cipher

It is essential to consider the key size and block size for developing a lightweight cipher. The key size and block size increase the overall computational power requirement

of RFID devices. However, decreasing key size or block size helps the adversary in breaking the cipher easily, as he/she can quickly guess the cipher's security key [9]. Hence, it is crucial to develop a block cipher of optimized size, such that the adversary cannot easily break the cipher. The new scheme should be hardware efficient, required low computational power, and must be resistant to all types of security attacks.

Challenge to develop to efficient shift cipher

In the current scenario, the stream cipher designs are based on the operations, round functions, components, structures. The structure of the stream ciphers is a fixed permutation of the hash function. There are various existing stream ciphers presented by the various researchers [76, 78, 79]. However, these suffer from various limitations such as exhaustive key search attack, related key attack, and algebraic attack [74, 117]. Hence, to construct a stream cipher that can deal with all such limitations is a challenge for the researchers working in the area of developing secure and efficient RFID systems. The various matrices, such as area, throughput, bits per cycle, power consumption, interface, etc., may be considered along with different security issues while designing a new solution.

Conclusion

In the last few years, IoT devices are being used for performing our day-to-day activities. These devices not only have constraints of less memory, low power, and low computational capacity, but also, are suffer from various security issues. These devices can easily be targeted by the attackers to steal vital information that can be related to a personal, a business organization, medical firm, etc. Hence, securing such constrained devices is an important issue. The objective of this paper was to discuss various security threats and issues that have been faced during the years by the researchers during implementations of such systems. It also discussed various solutions provided by the scientists to deal with such attacks. The work also gave a detailed overview of the IoT architecture. The paper focused on all possible attacks by classifying them into confidentiality, integrity, and availability criteria. The taxonomy of various security schemes was discussed under the categories of cryptography, privacy, authentication, authorization, and availability. Undoubtedly, researchers have put tremendous efforts to develop efficient and secure RFID systems. However, there is still a scope of improvement in various areas. Therefore, this paper also provided the various open issues and challenge that need to be addressed in the future by researchers working in this important area.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Gartner (2015) Gartner says 6.4 billion connected 'Things' will be in use in 2016, up 30 percent from 2015. Gartner, Inc., p 1 [Online]. <http://www.gartner.com/newsroom/id/3165317>
2. Greengard S (2015) Smart transportation networks drive gains. *Commun ACM* 58(1):25–27. <https://doi.org/10.1145/2686742>
3. Fang X, Misra S, Xue G, Yang D (2012) Smart grid—the new and improved power grid: a survey. *IEEE Commun Surv Tutor* 14(4):944–980. <https://doi.org/10.1109/SURV.2011.101911.00087>
4. Pan G, Qi G, Zhang W, Li S, Wu Z, Yang L (2013) Trace analysis and mining for smart cities: issues, methods, and applications. *IEEE Commun Mag* 51(6):120–126. <https://doi.org/10.1109/MCOM.2013.6525604>
5. Cocchia A (2014) Smart and digital city: a systematic literature review. In: *Smart city*. Springer, Berlin, pp 13–43
6. GhaffarianHoseini AH, Dahlan ND, Berardi U, GhaffarianHoseini A, Makaremi N (2013) The essence of future smart houses: from embedding ICT to adapting to sustainability principles. *Renew Sustain Energy Rev* 24:593–607. <https://doi.org/10.1016/j.rser.2013.02.032>
7. Ge M, Hong JB, Guttman W, Kim DS (2017) A framework for automating security analysis of the internet of things. *J Netw Comput Appl* 83:12–27. <https://doi.org/10.1016/j.jnca.2017.01.033>
8. Sha K, Wei W, Andrew Yang T, Wang Z, Shi W (2018) On security challenges and open issues in Internet of Things. *Future Gener Comput Syst* 83:326–337. <https://doi.org/10.1016/j.future.2018.01.059>
9. Singh S, Sharma PK, Moon SY, Park JH (2017) Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *J Ambient Intell Humaniz Comput*. <https://doi.org/10.1007/s12652-017-0494-4>
10. Anjum SS et al (2019) Energy management in RFID-sensor networks: taxonomy and challenges. *IEEE Internet Things J* 6(1):250–266. <https://doi.org/10.1109/JIOT.2017.2728000>
11. Conti M, Dehghantanha A, Franke K, Watson S (2018) Internet of Things security and forensics: challenges and opportunities. *Future Gener Comput Syst* 78:544–546. <https://doi.org/10.1016/j.future.2017.07.060>
12. Alazab M, Huda S, Abawajy J, Islam RL, Yearwood J, Venkatraman S, Broadhurst R (2014) A hybrid wrapper-filter approach for malware detection. *J Netw* 9(11):2878–2891
13. Jhaveri RH, Desai A, Patel A, Zhong Y (2018) A sequence number prediction based bait detection scheme to mitigate sequence number attacks in MANETs. *Security and*

- Communication Networks, Wiley-Hindawi, pp 1–13. <https://doi.org/10.1155/2018/3210207>
14. Riahi Sfar A, Natalizio E, Challal Y, Chtourou Z (2018) A roadmap for security challenges in the Internet of Things. *Digit Commun Netw* 4(2):118–137. <https://doi.org/10.1016/j.dcan.2017.04.003>
 15. Borrego C, Amadeo M, Molinaro A, Jhaveri RH (2019) Privacy-preserving forwarding using homomorphic encryption for information-centric wireless ad hoc networks. *IEEE Commun Lett* 23(10):1708–1711. <https://doi.org/10.1109/LCOMM.2019.2927913>, IEEE, July
 16. Adat V, Gupta BB (2018) Security in Internet of Things: issues, challenges, taxonomy, and architecture. *Telecommun Syst* 67(3):423–441. <https://doi.org/10.1007/s11235-017-0345-9>
 17. Fan K, Jiang W, Li H, Yang Y (2018) Lightweight RFID protocol for medical privacy protection in IoT. *IEEE Trans Ind Inform* 14(4):1656–1665. <https://doi.org/10.1109/TII.2018.2794996>
 18. Swarna Priya RM, Maddikunta PKR, Parimala M, Koppu S, Reddy T, Chowdhary CL, Alazab M (2020) An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. *Comput Commun* 160:139–149. <https://doi.org/10.1016/j.comcom.2020.05.048>
 19. Tewari A, Gupta BB (2020) Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Futur Gener Comput Syst* 108:909–920. <https://doi.org/10.1016/j.future.2018.04.027>
 20. Finkenzeller K (2010) RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication. Wiley, New York
 21. Sadeeq MAM, Zeebaree SRM, Qashi R, Ahmed SH, Jacksi K (2018) Internet of Things security: a survey. *ICOASE 2018 Int Conf Adv Sci Eng* 88:162–166. <https://doi.org/10.1109/ICOASE.2018.8548785>
 22. Mayes KE, Markantonakis K (2008) Smart cards, tokens, security and applications. Springer, New York
 23. Yick J, Mukherjee B, Ghosal D (2008) Wireless sensor network survey. *Comput Netw* 52(12):2292–2330. <https://doi.org/10.1016/j.comnet.2008.04.002>
 24. Bai X, Yun Z, Xuan D, Lai T, Jia W (2008) Deploying four-connectivity and full-coverage wireless sensor networks. In: *IEEE INFOCOM 2008—the 27th conference on computer communications*, pp 296–300
 25. Tian H, Shen H, Matsuzawa T (2006) Random walk routing in WSNs with regular topologies. *J Comput Sci Technol* 21(4):496–502. <https://doi.org/10.1007/s11390-006-0496-8>
 26. Bai X, Kumar S, Xuan D, Yun Z, Lai TH (2006) Deploying wireless sensors to achieve both coverage and connectivity. In: *Proceedings of the international symposium on mobile ad hoc networking and computing (MobiHoc)*, vol 2006, pp 131–142. <https://doi.org/10.1145/1132905.1132921>
 27. Razzaque MA, Milojevic-Jevric M, Palade A, Cla S (2016) Middleware for internet of things: a survey. *IEEE Internet Things J* 3(1):70–95. <https://doi.org/10.1109/JIOT.2015.2498900>
 28. Phan RCW (2009) Cryptanalysis of a new ultralightweight RFID authentication protocol—SASI. *IEEE Trans Dependable Secur Comput* 6(4):316–320. <https://doi.org/10.1109/TDSC.2008.33>
 29. Ouafi K, Phan RCW (2008) Traceable privacy of recent provably-secure RFID protocols. In: *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)*, 2008, vol 5037. LNCS, pp 479–489. https://doi.org/10.1007/978-3-540-68914-0_29
 30. Juels A., Weis SA (2009) Defining strong privacy for RFID. *ACM Trans Inform Syst Secur* 13(1):7. <https://doi.org/10.1145/1609956.1609963>
 31. Chien HY (2007) SASI: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. *IEEE Trans Dependable Secur Comput* 4(4):337–340. <https://doi.org/10.1109/TDSC.2007.70226>
 32. Saffkhani M, Shariat M (2018) Implementation of secret disclosure attack against two IoT lightweight authentication protocols. *J Supercomput* 74(11):6220–6235. <https://doi.org/10.1007/s11227-018-2538-8>
 33. Zhuang X, Zhu Y, Chang CC, Peng Q (2018) Security issues in ultralightweight RFID authentication protocols. *Wirel Pers Commun* 98(11):779–814. <https://doi.org/10.1007/s11277-017-4895-7>
 34. Bagheri N, Saffkhani M, Peris-Lopez P, Tapiador JME (2012) Cryptanalysis of RAPP, an RFID authentication protocol. *ePrint Arch*, pp 1–4
 35. D'Arco P, De Santis A (2011) On ultralightweight RFID authentication protocols. *IEEE Trans Dependable Secur Comput* 8(4):548–563. <https://doi.org/10.1109/TDSC.2010.75>
 36. Saffkhani M, Bagheri N (2017) Passive secret disclosure attack on an ultralightweight authentication protocol for Internet of Things. *J Supercomput* 73(8):3579–3585. <https://doi.org/10.1007/s11227-017-1959-0>
 37. Tewari A, Gupta BB (2017) Cryptanalysis of a novel ultralightweight mutual authentication protocol for IoT devices using RFID tags. *J Supercomput* 73(3):1085–1102
 38. Ahmadian Z, Salmasizadeh M, Aref MR (2013) Recursive linear and differential cryptanalysis of ultralightweight authentication protocols. *IEEE Trans Inf Forensics Secur* 8(7):1140–1151. <https://doi.org/10.1109/TIFS.2013.2263499>
 39. Numan M, Subhan F, Khan WZ, Hakak S, Haider S, Reddy GT, Jolfaei A, Alazab M (2020) A systematic review on clone node detection in static wireless sensor networks. *IEEE Access* 8:65450–65461
 40. Mosenia A, Jha NK (2017) A comprehensive study of security of internet-of-things. *IEEE Trans Emerg Top Comput* 5(4):586–602. <https://doi.org/10.1109/TETC.2016.2606384>
 41. Liao YP, Hsiao CM (2014) A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. *Ad Hoc Netw* 18:133–146. <https://doi.org/10.1016/j.adhoc.2013.02.004>
 42. Vishwakarma R, Jain AK (2020) A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommun Syst* 73(1):3–25. <https://doi.org/10.1007/s11235-019-00599-z>
 43. Vishwakarma R, Jain AK (2019) A honeypot with machine learning based detection framework for defending IoT based Botnet DDoS attacks. In: *2019 3rd International conference on trends in electronics and informatics (ICOEI)*. IEEE, New York, pp 1019–1024
 44. Ahmadian Z, Salmasizadeh M, Aref MR (2013) Desynchronization attack on RAPP ultralightweight authentication protocol. *Inf Process Lett* 113(7):205–209. <https://doi.org/10.1016/j.ipl.2013.01.003>
 45. Sun HM, Ting WC, Wang KH (2011) On the security of Chien's ultralightweight RFID authentication protocol. *IEEE Trans Dependable Secur Comput* 8(2):315–317. <https://doi.org/10.1109/TDSC.2009.26>
 46. Wang S, Han Z, Liu S, Chen D (2012) Security analysis of RAPP an RFID authentication protocol based on permutation. *IACR Cryptology*. ePrint Arch, vol 2012, p 327 [Online]. <http://dblp.uni-trier.de/db/journals/iacr/iacr2012.html#WangHLC12>
 47. Mujahid U, Najam-ul-Islam M, Sarwar S (2017) A new ultralightweight RFID authentication protocol for passive low cost

- tags: KMAP. *Wirel Pers Commun* 94(3):725–744. <https://doi.org/10.1007/s11277-016-3647-4>
48. Bogdanov A, Knežević M, Leander G, Toz D, Varici K, Verbauwhede I (2011) Spongent: a lightweight hash function. In: *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)*, 2011, vol 6917. LNCS, pp 312–325. https://doi.org/10.1007/978-3-642-23951-9_21
 49. Mukundan PM, Manayankath S, Srinivasan C, Sethumadhavan M (2016) Hash-one: a lightweight cryptographic hash function. *IET Inf Secur* 10(5):225–231. <https://doi.org/10.1049/iet-ifs.2015.0385>
 50. Aumasson JP, Henzen L, Meier W, Naya-Plasencia M (2013) Quark: a lightweight hash. *J Cryptol* 26(2):313–339. <https://doi.org/10.1007/s00145-012-9125-6>
 51. Shamir A (2008) SQUASH—a new MAC with provable security properties for highly constrained devices such as RFID tags. In: *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)*, 2008, vol 5086. LNCS, pp 144–157. https://doi.org/10.1007/978-3-540-71039-4_9
 52. Hanin C, Echandouri B, Omary F, El Bernoussi S (2017) L-CAHASH: a novel lightweight hash function based on cellular automata for RFID. In: *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)*, 2017, vol 10542. LNCS, pp 287–298. https://doi.org/10.1007/978-3-319-68179-5_25
 53. Hammad BT, Jamil N, Rusli ME, Z'aba MR (2017) A survey of lightweight cryptographic hash function. *Int J Sci Eng Res* 8(7):806–814 [Online]. <https://www.ijser.org/researchpaper/A-survey-of-Lightweight-Cryptographic-Hash-Function.pdf>
 54. Biehl I, Meyer B, Müller V (2000) Differential fault attacks on elliptic curve cryptosystems. In: *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)*, 2000, vol 1880, pp 131–146. https://doi.org/10.1007/3-540-44598-6_8
 55. Roy I, Rebeiro C, Hazra A, Bhunia S (2020) SAFARI: automatic synthesis of fault-attack resistant block cipher implementations. *Comput Des Integr Circuits Syst* 39(4):752–765. <https://doi.org/10.1109/TCAD.2019.2897629>
 56. Bogdanov A et al (2007) PRESENT: an ultra-lightweight block cipher. In: *International workshop on cryptographic hardware and embedded systems*, 2007, pp 450–466
 57. Nakahara J, Sepehrdad P, Zhang B, Wang M (2009) Linear (hull) and algebraic cryptanalysis of the block cipher PRESENT. In: *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)*, 2009, vol 5888. LNCS, pp 58–75. https://doi.org/10.1007/978-3-642-10433-6_5
 58. Collard B, Standaert FX (2009) A statistical saturation attack against the block cipher present. In: *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)*, 2009, vol 5473, pp 195–210. https://doi.org/10.1007/978-3-642-00862-7_13
 59. Suzaki T, Minematsu K, Morioka S, Kobayashi E (2011) Twine: a lightweight, versatile block cipher. In: *ECRYPT Work. pn Light. Cryptogr. LC11*, pp 146–169 [Online]. http://www.nec.co.jp/rd/media/code/research/images/twine_LC11.pdf
 60. Zhang W, Bao Z, Lin D, Rijmen V, Yang B, Verbauwhede I (2015) RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. *Sci China Inf Sci* 58(12):1–15. <https://doi.org/10.1007/s11432-015-5459-7>
 61. Biham E, Dunkelman O, Keller N (2005) A related-key rectangle attack on the full KASUMI. In: *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)*, 2005, vol 3788. LNCS, pp 442–461. https://doi.org/10.1007/11593447_24
 62. Selvam R, Shanmugam D, Annadurai S (2014) Side channel attacks: vulnerability analysis of PRINCE and RECTANGLE using DPA. In: *IACR Cryptol. ePrint Arch.*, vol 2014, p 644 [Online]. <http://dblp.uni-trier.de/db/journals/iacr/iacr2014.html#SelvamSA14a>
 63. Beaulieu R, Treatman-Clark S, Shors D, Weeks B, Smith J, Wingers L (2015) The SIMON and SPECK lightweight block ciphers. In: *Proceedings—design automation conference*, vol 2015. <https://doi.org/10.1145/2744769.2747946>
 64. Bagheri N (2015) Linear cryptanalysis of reduced-round SIMECK variants. In: *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)*, 2015, vol 9462, pp 140–152. https://doi.org/10.1007/978-3-319-26617-6_8
 65. Zhang K, Guan J, Hu B, Lin D (2018) Security evaluation on Simeck against zero-correlation linear cryptanalysis. *IET Inf Secur* 12(1):87–93. <https://doi.org/10.1049/iet-ifs.2016.0503>
 66. Qiao K, Hu L, Sun S (2017) Differential analysis on Simeck and SIMON with dynamic key-guessing techniques. *Commun Comput Inf Sci* 691:64–85. https://doi.org/10.1007/978-3-319-54433-5_5
 67. Zhang K, Guan J, Hu B, Lin D (2016) Integral cryptanalysis on Simeck. In: *6th International conference on information science and technology, ICIST 2016*, pp 216–222. <https://doi.org/10.1109/ICIST.2016.7483413>
 68. Berger TP, Francq J, Minier M, Thomas G (2016) Extended generalized Feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput. *IEEE Trans Comput* 65(7):2074–2089. <https://doi.org/10.1109/TC.2015.2468218>
 69. Li L, Liu B, Wang H (2016) QTL: a new ultra-lightweight block cipher. *Microprocess Microsyst* 45:45–55. <https://doi.org/10.1016/j.micpro.2016.03.011>
 70. Sadeghi S, Bagheri N, Abdelraheem MA (2017) Cryptanalysis of reduced QTL block cipher. *Microprocess Microsyst* 52:34–48. <https://doi.org/10.1016/j.micpro.2017.05.007>
 71. Patil J, Bansod G, Kant KS (2017) LiCi: a new ultra-lightweight block cipher. In: *2017 International conference on emerging trends and innovation in ICT, ICEI 2017*, pp 40–45. <https://doi.org/10.1109/ETIICT.2017.7977007>
 72. Bansod G, Pisharoty N, Patil A (2017) BORON: an ultra-lightweight and low power encryption design for pervasive computing. *Front Inf Technol Electron Eng* 18(3):317–331. <https://doi.org/10.1631/FITEE.1500415>
 73. Sutar SA (2018) Differential power attack analysis of ultra-lightweight block cipher BORON. In: *Proceedings of the 2nd international conference on electronics, communication and aerospace technology, ICECA 2018*, pp 365–370. <https://doi.org/10.1109/ICECA.2018.8474902>
 74. Jiao L, Hao Y, Feng D (2020) Stream cipher designs: a review. *Sci China Inf Sci* 63(3):1–25. <https://doi.org/10.1007/s11432-018-9929-x>
 75. Nawaz Y, Gong G (2005) The WG stream cipher. *ECRYPT Stream Cipher Project Report* 2005, 33
 76. Fan X, Zidaric N, Aagaard M, Gong G (2013) Efficient hardware implementation of the stream cipher WG-16 with composite field arithmetic. In: *Proceedings of the ACM conference on computer and communications security*, 2013, pp 21–33. <https://doi.org/10.1145/2517300.2517305>
 77. Zidaric N, Aagaard M, Gong G (2019) Hardware optimizations and analysis for the WG-16 cipher with tower field arithmetic. *IEEE Trans Comput* 68(1):67–82. <https://doi.org/10.1109/TC.2018.2854757>

78. Fan X, Mandal K, Gong G (2013) WG-8: a lightweight stream cipher for resource-constrained smart devices. In: Lecture notes of the institute for computer sciences, social-informatics and telecommunications engineering, LNICST, 2013, vol 115, pp 617–632. https://doi.org/10.1007/978-3-642-37949-9_54
79. Ding L, Jin C, Guan J, Wang Q (2014) Cryptanalysis of lightweight WG-8 stream cipher. *IEEE Trans Inf Forensics Secur* 9(4):645–652. <https://doi.org/10.1109/TIFS.2014.2307202>
80. Bogdanov A, Mendel F, Regazzoni F, Rijmen V, Tischhauser E (2014) ALE: AES-based lightweight authenticated encryption. In: Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), 2014, vol 8424. LNCS, pp 447–466. https://doi.org/10.1007/978-3-662-43933-3_23
81. Wu S, Wu H, Huang T, Wang M, Wu W (2013) Leaked-state-forgery attack against the authenticated encryption algorithm ALE. In: Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), 2013, vol 8269. LNCS, no PART 1, pp 377–404. https://doi.org/10.1007/978-3-642-42033-7_20
82. Khovratovich D, Rechberger C (2014) The LOCAL attack: cryptanalysis of the authenticated encryption scheme ALE. In: Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), 2014, vol 8282. LNCS, pp 174–184. https://doi.org/10.1007/978-3-662-43414-7_9
83. Dai X, Huang Y, Chen L, Lu T, Zhao S (2015) SVH: a lightweight stream cipher based on dual pseudo-random transformation and OFB. In: 2015 4th International conference on mechatronics, materials, chemistry and computer engineering, 2015. <https://doi.org/10.2991/icmmcce-15.2015.136>
84. Aminghafari V, Hu H (2016) Fruit: ultra-lightweight stream cipher with shorter internal state. *IACR Cryptology. ePrint Arch*, vol 2016, p 355 [Online]. <http://dblp.uni-trier.de/db/journals/iacr/iacr2016.html#AminghafariH16>
85. Costa E, Silva S, Tavaría F, Pintado M (2014) Antimicrobial and antibiofilm activity of chitosan on the oral pathogen *Candida albicans*. *Pathogens* 3(4):908–919. <https://doi.org/10.3390/pathogens3040908>
86. Wu H (2014) ACORN: a lightweight authenticated cipher (v1). In: CAESAR first round submissions. CAESAR Comm. CAESAR competition for authenticated encryption security, applicability and robustness
87. Lee YK, Batina L, Verbaauwhede I (2008) EC-RAC (ECDLP based randomized access control): provably secure RFID authentication protocol. In: 2008 IEEE international conference on RFID (frequency identification), IEEE RFID 2008, 2008, pp 97–104. <https://doi.org/10.1109/RFID.2008.4519370>
88. Hamann M, Krause M, Meier W (2017) LIZARD – A lightweight stream cipher for powerconstrained devices. *IACR Trans Symmetric Cryptol*. <https://doi.org/10.46586/tosc.v2017.i1.45-79>
89. Zhao Z (2014) A secure RFID authentication protocol for health-care environments using elliptic curve cryptosystem. *J Med Syst* 38(5):269–273. <https://doi.org/10.1007/s10916-014-0046-9>
90. He D, Kumar N, Chilamkurti N, Lee JH (2014) Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. *J Med Syst*. <https://doi.org/10.1007/s10916-014-0116-z>
91. Cao X, Kou W, Du X (2010) A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. *Inf Sci (NY)* 180(15):2895–2903. <https://doi.org/10.1016/j.ins.2010.04.002>
92. Gódor G, Imre S (2011) Elliptic curve cryptography based authentication protocol for low-cost RFID tags. In: 2011 IEEE international conference on RFID-technologies and applications, RFID-TA 2011, pp 386–393. <https://doi.org/10.1109/RFID-TA.2011.6068667>
93. Ryu EK, Kim DS, Yoo KY (2015) On elliptic curve based untraceable RFID authentication protocols. In: IH and MMSEC 2015—proceedings of the 2015 ACM workshop on information hiding and multimedia security, 2015, pp 147–153. <https://doi.org/10.1145/2756601.2756610>
94. Shen H, Shen J, Khan MK, Lee JH (2017) Efficient RFID authentication using elliptic curve cryptography for the Internet of Things. *Wirel Pers Commun* 96(4):5253–5266. <https://doi.org/10.1007/s11277-016-3739-1>
95. Chen Y, Chou JS (2015) ECC-based untraceable authentication for large-scale active-tag RFID systems. *Electron Commer Res* 15(1):97–120. <https://doi.org/10.1007/s10660-014-9165-0>
96. Peris-Lopez P, Hernandez-Castro JC, Estévez-Tapiador JM, Ribagorda A (2006) LMAP: a real lightweight mutual authentication protocol for low-cost RFID tags. In: Workshop on RFID security, 2006, vol 6, p 6
97. Peris-Lopez P, Hernandez-Castro JC, Estevez-Tapiador JM, Ribagorda A (2006) EMAP: an efficient mutual-authentication protocol for low-cost RFID tags. In: Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), vol 4277. LNCS-I, pp 352–361. https://doi.org/10.1007/11915034_59
98. Peris-Lopez P, Hernandez-Castro JC, Estevez-Tapiador JM, Ribagorda A (2006) M2AP: a minimalist mutual-authentication protocol for low-cost RFID tags. In: Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), 2006, vol 4159. LNCS, pp 912–923. https://doi.org/10.1007/11833529_93
99. Peris-Lopez P, Hernandez-Castro JC, Tapiador JME, Ribagorda A (2009) Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol. In: Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), 2009, vol 5379. LNCS, pp 56–68. https://doi.org/10.1007/978-3-642-00306-6_5
100. Yeh KH, Lo NW, Winata E (2010) An efficient ultralightweight authentication protocol for RFID systems. *Cryptol Inf Secur Ser* 4:49–60. <https://doi.org/10.3233/978-1-60750-485-6-49>
101. Zhuang X, Zhu Y, Chang CC (2014) A new ultralightweight RFID protocol for low-cost tags: R(formula presented)AP. *Wirel Pers Commun* 79(3):1787–1802. <https://doi.org/10.1007/s11277-014-1958-x>
102. Luo H, Wen G, Su J, Huang Z (2018) SLAP: succinct and lightweight authentication protocol for low-cost RFID system. *Wirel Netw* 24(1):69–78. <https://doi.org/10.1007/s11276-016-1323-y>
103. Mujahid U, Najam-UL-Islam M, Shami MA (2015) RCIA: a new ultralightweight RFID authentication protocol using recursive hash. *Int J Distrib Sens Netw* 4:2015. <https://doi.org/10.1155/2015/642180>
104. Misra S, Venkata Krishna P, Agarwal H, Saxena A, Obaidat MS (2011) A learning automata based solution for preventing distributed denial of service in internet of things. In: Proceedings—2011 IEEE international conferences on internet of things and cyber, physical and social computing, iThings/CPSCo 2011, pp 114–122. <https://doi.org/10.1109/iThings/CPSCo.2011.84>
105. Javaid U, Siang AK, Aman MN, Sikdar B (2018) Mitigating IoT device based DDoS attacks using blockchain. In: CRYBLOCK 2018—proceedings of the 1st workshop on cryptocurrencies and blockchains for distributed systems, part of MobiSys 2018, pp 71–76. <https://doi.org/10.1145/3211933.3211946>
106. Ejaz Ahmed M, Kim H (2017) DDoS attack mitigation in internet of things using software defined networking. In: Proceedings—3rd IEEE international conference on big data computing service and applications, BigDataService 2017, pp 271–276. <https://doi.org/10.1109/BigDataService.2017.41>

107. Su J, Danilo Vasconcellos V, Prasad S, Daniele S, Feng Y, Sakurai K (2018) Lightweight classification of IoT malware based on image recognition. In: Proceedings—international computer software and applications conference, 2018, vol 2, pp 664–669. <https://doi.org/10.1109/COMPSAC.2018.10315>
108. HaddadPajouh H, Dehghantanha A, Khayami R, Choo KKR (2018) A deep recurrent neural network based approach for Internet of Things malware threat hunting. *Future Gener Comput Syst* 85:88–96. <https://doi.org/10.1016/j.future.2018.03.007>
109. Meidan Y et al (2018) N-BaIoT-network-based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Comput* 17(3):12–22. <https://doi.org/10.1109/MPRV.2018.03367731>
110. Sicari S, Rizzardi A, Miorandi D, Coen-Porisini A (2018) REATO: REActing to denial of service attacks in the Internet of Things. *Comput Netw* 137:37–48. <https://doi.org/10.1016/j.comnet.2018.03.020>
111. Amoon M, Altameem T, Altameem A (2020) RRAC: role based reputed access control method for mitigating malicious impact in intelligent IoT platforms. *Comput Commun* 151:238–246
112. Thakare A, Lee E, Kumar A, Nikam VB, Kim YG (2020) PAR-BAC: priority-attribute-based RBAC model for azure IoT cloud. *IEEE Internet Things J* 7(4):2890–2900. <https://doi.org/10.1109/JIOT.2019.2963794>
113. Omolola O, More S, Faslija E, Wagner G, Alber L (2019) Policy-based access control for the IoT and Smart Cities. In: Open identity summit 2019
114. Ahamed J, Khan F (2019) An enhanced context-aware capability-based access control model for the internet of things in healthcare. In: ITT 2019—information technology trends: emerging technologies blockchain and IoT, 2019, vol 2019, pp 126–131. <https://doi.org/10.1109/ITT48889.2019.9075073>
115. Bernal Bernabe J, Hernandez Ramos JL, Skarmeta Gomez AF (2016) TACIoT: multidimensional trust-aware access control system for the Internet of Things. *Soft Comput* 20(5):1763–1779. <https://doi.org/10.1007/s00500-015-1705-6>
116. Putra GD, Dedeoglu V, Kanhere SS, Jurdak R (2020) Trust management in decentralized IoT access control system. In: 2020 IEEE international conference on blockchain and cryptocurrency (ICBC), 2020, pp 1–9
117. Bokhari MU, Alam S, Syeed Masoodi F (2012) Cryptanalysis techniques for stream cipher: a survey. *Int J Comput Appl* 60(9):29–33. <https://doi.org/10.5120/9721-4187>
118. Li L, Liu B, Zhou Y, Zou Y (2018) SFN: a new lightweight block cipher. *Microprocess Microsyst* 60(September 2016):138–150. <https://doi.org/10.1016/j.micpro.2018.04.009>
119. Yeoh WZ, Sen Teh J, Sazali MISBM (2020) $\mu 2$: a lightweight block cipher. In: Lecture notes in electrical engineering, vol 603, no. September 2019, pp 281–290. https://doi.org/10.1007/978-981-15-0058-9_27
120. Biswas A, Majumdar A, Nath S, Dutta A, Baishnab KL (2020) LRBC: a lightweight block cipher design for resource constrained IoT devices. *J Ambient Intell Humaniz Comput*. <https://doi.org/10.1007/s12652-020-01694-9>
121. Sadeghi S, Bagheri N (2020) An argument on the security of LRBC, a recently proposed lightweight block cipher. *IACR Cryptology. ePrint Arch*, vol 2020, p 392
122. Siddhanti A, Sarkar S, Maitra S, Chattopadhyay A (2017) Differential fault attack on grain v1, ACORN v3 and lizard. In: Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), 2017, vol 10662. LNCS, pp 247–263. https://doi.org/10.1007/978-3-319-71501-8_14
123. Dey S, Sarkar S (2017) Cryptanalysis of full round Fruit. *IACR Cryptology. ePrint Arch*, vol 2017, p 87 [Online]. <http://dblp.uni-trier.de/db/journals/iacr/iacr2017.html#DeyS17>
124. Ghafari VA, Hu H (2018) Fruit-80: a secure ultra-lightweight stream cipher for constrained environments. *Entropy* 20(3):180. <https://doi.org/10.3390/e20030180>
125. Zhang C, Dong L (2020) An improved fast correlation attack on Fruit-80. In: Advances in intelligent systems and computing, 2020, vol 1151. AISC, pp 1426–1436. https://doi.org/10.1007/978-3-030-44041-1_120
126. Gao L, Ma M, Shu Y, Wei Y (2014) An ultralightweight RFID authentication protocol with CRC and permutation. *J Netw Comput Appl* 41(1):37–46. <https://doi.org/10.1016/j.jnca.2013.10.014>
127. Kumar A, Jain AK (2020) A lightweight authentication scheme for RFID using ECC. *Adv Intell Syst Comput* 1122:177–183. https://doi.org/10.1007/978-3-030-39875-0_19
128. Safkhani M (2018) Cryptanalysis of r2ap an ultralightweight authentication protocol for rfid. *J Electr Comput Eng Innov* 6(1):107–114

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations