Wireless Personal Communications
https://doi.org/10.1007/s11277-024-11382-y

A Survey on 6LoWPAN Security for IoT: Taxonomy, Architecture, and Future Directions

Leki Chom Thungon[1] · Nurzaman Ahmed[2] · Debashis De[3] · Md. Iftekhar Hussain[4]

Accepted: 19 June 2024

Abstract
Provisioning security to the communications, data, and partaking *things* in resource-constrained IoT is a huge challenge. Due to the scalability and interoperability among low power-consuming networks, 6LoWPAN is used widely in IoT. However, security schemes used by traditional Internet are proven to be very heavy and power-consuming for resource-constrained devices in 6loWPAN. This paper describes various existing security schemes used in different layers of 6LoWPAN based IoT networks in detail and highlights their pros and cons. We pointed out the issues and challenges of lightweight security mechanisms for IoT to enable the researchers to easily and quickly get into the problem domain. Compared to other relevant works, we emphasize open issues and future directions.

Keywords 6LoWPAN · Attacks · Internet of things · Security · Privacy

Abbreviations

ABE	Attribute-based encryption
ACL	Access control List
AES	Advanced encryption standard
AKE	Authenticated key establishment
APKES	Adaptable pairwise key establishment scheme

✉ Leki Chom Thungon
lekichom.thungon@vit.ac.in

Nurzaman Ahmed
nur.zaman@live.com

Debashis De
dr.debashis.de@gmail.com

Md. Iftekhar Hussain
ihuusain@nehu.ac.in

[1] School of Computer Science and Engineering, VIT, Chennai, Tamil Nadu 600127, India

[2] Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur 721302, India

[3] Department of Computer Science and Engineering, Maulana Abul Kalam Azad University of Technology, Kolkata, West Bengal 700064, India

[4] Department of Information Technology, North-Eastern Hill University, Shillong 793022, India

Published online: 06 July 2024

BLE	Bluetooth low energy
CAP	Contention access period
CBC	Cipher block chaining
CCM	Counter with CBC-MAC mode of operation
CFP	Contention free Period
CNN	Convolutional neural network
CoAP	Constrained application protocol
CoAPs	Constrained application protocol security
CTR	Counter
DoS	Denial-of-service
DODAGs	Destination oriented directed acyclic graphs
DIS	DODAG information solicitation
DTLS	Datagram transport layer security
ECC	Elliptic curve cryptography
E2E	End-to-end
ECDHE	Elliptic-curve Diffie-Hellman ephemeral
ECDSA	Elliptic-curve digital signature algorithm
EBEAP	Easy broadcast encryption and authentication protocol
ETX	Expected transmission count
FFD	Full function device
FPGA	Field programmable gate array
GCM	Galois/counter mode
HMAC-SHA1	Hash-based message authentication code with secure hash algorithm
IoT	Internet of things
ICV	Integrity check value
IPv4/v6	Internet protocol version 4/version 6
IPSec	Internet protocol security
IDS	Intrusion detection system
IPSec-AH	IPSec authentication header
IPSec-ESP	IPSec encapsulating security payload
IKE	Internet key exchange
LTK	Long term key
MAC	Message authentication code
MAG	Mobile access gateways
MITM	Man-in-the-middle
MIC	Message integrity code
MTU	Maximum transmission unit
M2M	Machine-to-machine
MIC-CCM	Message integrity code with cipher block chaining
NETLMM	Network-based localized mobility management
PKI	Public key infrastructure
PKC	Public key cryptography
PMIPv6	Proxy mobile IPv6
PUF	Physical unclonable function
QoS	Quality-of-service
RFD	Reduced function device
RF	Radio frequency
RPL	IPv6 routing protocol for link layer networks (LLNs)
ROR	Real-or-random model-based formal security analysis

RSA	Rivest–Shamir–Adleman cryptograhy
RSSI	Received signal strength indicator
STK	Short term key
SMQTT	Secure message queuing telemetry transport
TCP/IP	Transmission control protocol/ internet protocol
TLS-PSK	Transport layer security pre-shared key ciphersuites
TLS/SSL	Transport layer security/ secure sockets layer
TTP	Trusted third party
UDP	User datagram protocol
WSNs	Wireless sensor networks
6LoWPAN	IPv6 over low-power wireless personal area networks
6Hs	6LoWPAN host
6BR	6LoWPAN edge/border router

1 Introduction

In today's era, homes, offices, industries, and hospitals have own wireless networks and contain multiple devices with their IP addresses. Anything connected to the network ranging from tiny light bulbs to complex systems, with its unique IP address, so the concept of the Internet of Things (IoT) becomes vital in such an environment. IoT is a computing concept where all physical objects are interconnected to the Internet and can identify themselves to others with their IP addresses [77]. These physical objects, such as devices, vehicles, buildings, etc., collect and exchange their data over the Internet [104, 121]. These devices are constraints in terms of power, computation, and memory.

While developing IPv4-based Internet is private, but in today's scenario, there is more public rather than private networks [92]. Due to its private network and small address space, IPv4 addresses started running out. So, IPv6 was addresses these problems. To support IPv6 and IEEE 802.15.4 devices, a layer that provides an adaptation between IPv6 network layer capabilities and 802.15.4 link layer capabilities is develop. This layer is called 6LoWPAN. It employs IPv6 connectivity, which allows devices to communicate with each other, accesses each other's services, and interact with the Internet [126]. Due to its address space and its openness, 6LoWPAN was formally established by IETF and released in September 2007 and is still gaining massive popularity in IoT [60, 73]. Such short-range, low-rate, and low-power 6LoWPAN commonly deals with tiny packets, low bandwidth, and, most importantly, low resources. Therefore, security has always been a challenge for such a network. Furthermore, the device makers and developers hardly considered this issue. In such a case, the attacker can quickly get access to any IoT application. The devices embedded with small silicon form factor low power consumption characteristics provide limited connectivity. For example, embedded devices are kept in the human body to read health-related real-time, and sensitive data must protect from unauthorized usage. Similarly, in an smart meter or real-time power grid application, a third party should not access energy usage data.

The security schemes designed for the Internet require massive computation and uses too many disk spaces. As human beings do not operate these devices, authentication and trust in the application must take from own judgments and decisions whether to accept a command or execute a task. With increased public awareness towards data security, people may not consider an application that offers no protection against threats while confidential

data traverse. Security and privacy become essential to provide smooth service on the public Internet. In the literature, various survey papers discussed security and privacy in 6LoWPAN networks as shown in Table 1 with security mechanisms used and security issues addressed. In this paper, we highlight various 6LoWPAN technologies with their existing security mechanisms, possible threats and open issues. A detailed survey focusing on communication security in different layers of 6LoWPAN based IoT networks was provided. We analyze the possible threats and available solutions in various communication technologies and those proposed in the literature. Security vulnerabilities in various 6LoWPAN communication technologies were also explained and lastly, we highlight the existing open challenges and issues and its possible future research work.

The remainder of this paper is organized as follows: Sect. 2 presents the overview of security and the most frequent attacks in a 6LoWPAN network. In Sect. 3, we explain about different 6LoWPAN technologies with their existing security features and their vulnerabilities. Various issues and existing security solutions in different layers of a 6LoWPAN network were identified in Sect. 4. Moreover, Sect. 4 also describes the possible attacks which can occur in different layers of 6LoWPAN. Section 5 highlights about various open issues, challenges and future research scope in 6LoWPAN-based IoT networks. The Sect. 6 with some of the existing and future applications of the IoT-centric concepts. Finally, the paper concludes with Sect. 7.

2 Security Overview of 6LoWPAN-Based Network

Security and privacy become important when personal information transfers over the more untrusted wireless networks. Applications like e-health and smart home transmit personal and sensitive information continuously, so protecting such information remains critical. An intruder can detect when the house is occupied and people's daily schedule inside the house using traffic analysis attacks. It allows an attacker to steal at will. In the healthcare scenario, a denial of service attack at the cloud or fog devices could even lead to a person's death. Ordinarily, security mechanisms require additional processing and bandwidth resources. Designing security schemes for resource-constrained devices and networks becomes a challenging task. The 6LoWPAN security schemes could be very important in various domains especially like industrial monitoring, intelligent transportation system, home management, environmental monitoring, healthcare, etc., as shown in Table 2:

- *Industrial Process Monitoring and Automation:* Operations like remote monitoring of machines for energy efficiency, production quality, and machine supervision are essential and expensive in industrial monitoring. Using easy and inexpensive 6LoWPAN devices that can be accessed remotely via the Internet makes it a more viable solution. The traffic type is primarily event-driven. Security features to be addressed here are product authentication, confidentiality, track, and trace (privacy), etc.
- *Intelligent Transportation System:* 6LoWPAN technology in intelligent transportation systems like roads, vehicles, parking garages, and traffic signals, monitoring them to make transport possible anytime. Such an application has a continuous traffic type. Physical security of devices is necessary for such systems. The authenticated user or device should be allowed to access the required data.

Table 1 Surveys on 6LoWPAN-based network security

Survey	Year	6LoWPAN vision	Security issues addressed	Limitations
[99]	2009	3-Layer Architecture	Key management, End-to-end security, Malicious Node Detection mechanism	No research and future directions
[34]	2014	5-Layer Architecture	Key management, Privacy, End-to-end security	Lack of attack analysis and open research issues and future directions
[117]	2015	Adaptation Layer	Confidentiality, Integrity, Intrusion detection system	Lack of attack analysis and open research directions and future scope
[85]	2015	Routing protocol	Intrusion detection system	Focused only on RPL and IDS. No study on 6LoWPAN security schemes, open research issues, challenges, and future directions
[98]	2013	6-Layer Architecture	Key management, Intrusion detection system	Lack of attack analysis, open research issues, challenges, and future directions
[16]	2016	Mobility	Secure mobility	No layer-wise overview of the current protocols, No identification of security challenges related to the mobility
[101]	2017	Adaptation layer	Authentication, Data Integrity, Confidentiality, Access control, Data security	No layer-wise attack analysis, open research issues, challenges, and future directions
[78]	2020	5-Layer Architecture	Attacks analysis, Privacy	Lack of attack analysis of well-known attacks and open research directions and future scope
[13]	2023	5-Layer Architecture	M2M and E2E communications security, Authentication and key exchange mechanisms	Lack of security analysis in existing 6LoWPAN tehnologies, no highlights on future application on 6LoWPAN technologies

Table 2 Comparison of 6LoWPAN network applications [9, 17, 47, 98, 99]

Applications	Traffic-type	Authentication	Confidentiality	Integrity	Privacy
Smart home	ED, QD	Y	Y	Y	–
Patient monitoring	C	Y	Y	Y	Y
Environ-ment monitoring	ED	Y	Y	–	Y
Intelligent transportation system	C	Y	–	Y	–
Structural monitoring	QD, ED	Y	Y	–	–
Industrial monitoring	ED	Y	Y	–	Y

ED Event-driven, *QD* Query-driven, *C* Continuous, *Y* Yes, – Undefined

- *Home Management and Monitoring:* 6LoWPAN technology can offer a smart home using intelligent tools manipulated through the Internet for home safety, elderly care, and intelligent energy control to control it from away. These devices have constrained resources with restricted protocols. The data obtained can be event-driven or query-driven. Device authentication is necessary to prevent the access of these 6LoWPAN devices by an authorized user. Confidentiality for sensitive information also should be maintained.
- *Environment Monitoring:* In the same way, 6LoWPAN technologies are applicable in gathering and monitoring specific environment information which can prevent natural disasters. The traffic type in such an application is event-driven. Authentication of data is necessary here.
- *Healthcare:* 6LoWPAN devices can monitor the current health conditions of the patient and generate an alarm to trigger the medical devices remotely. The traffic generated in such applications is continuous. The privacy and security of data are mandatory since sensitive information is transmitted continuously. Also, authentication of the person who can control those devices is necessary.

LoWPAN enables devices with IEEE 802.15.4 standard to use IPv6. Due to the growth in IoT devices, supports for IPv6 with auto-configuration is critical for larger address spaces. Figure 1 shows a typical architecture of such networks with resource-constrained 6LoWPAN Host (6Hs), 6LoWPAN Border Router (6BR), and IPv6 network connected to the remote server over the Internet. The protocol stack of 6LoWPAN comprises of 5-Layer architecture as shown in Fig. 2. The layer between the network layer and link layer is a 6LoWPAN layer. The adjustment between these two layers is challenging due to their different packet sizes. The adaptation layer is responsible for fragmenting the IPv6 packets (i.e., 1280 bytes) and reassembling them in the 802.15.4 layer (i.e., 127 bytes). As the wireless links used by these tiny devices can easily be eavesdropped on and are susceptible to many attacks, protecting sensitive information traversing in such links becomes essential and challenging. Different characteristics of the 6LoWPAN-based network are summarized as follows:

- *Wireless Link*: Devices in WSN are susceptible to eavesdropping, DoS attack, man-in-the-middle attacks, etc.
- *Unattended Devices*: Most of the 6LoWPAN devices are not updated for a long time and are kept unattended.

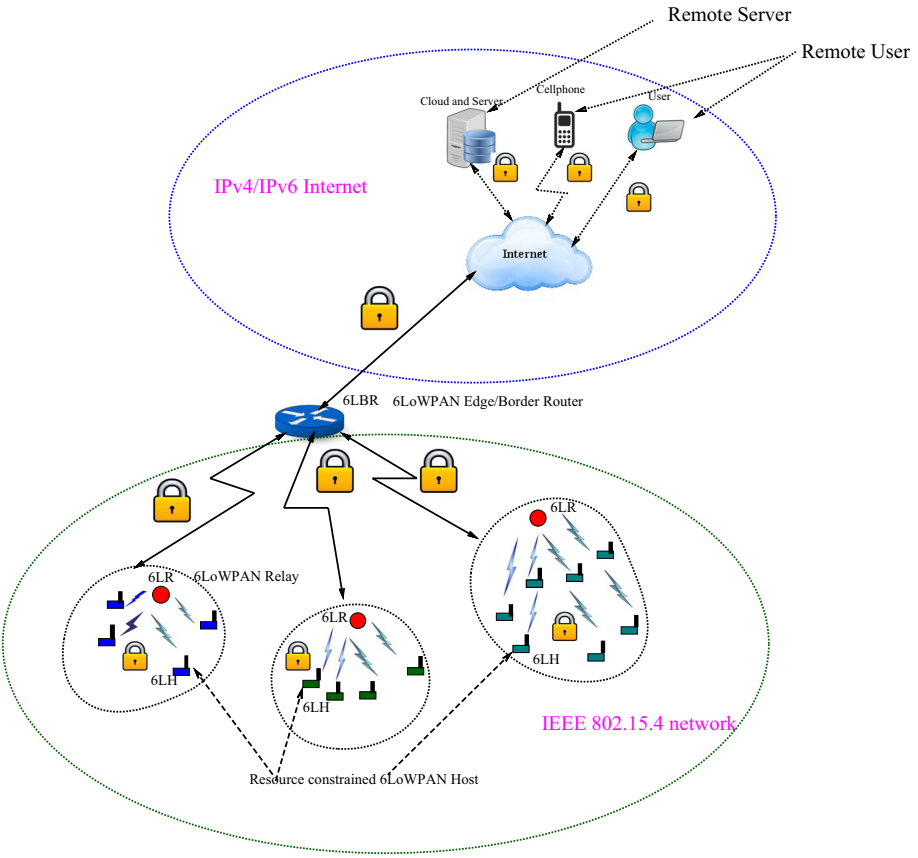

Fig. 1 A 6LoWPAN architecture

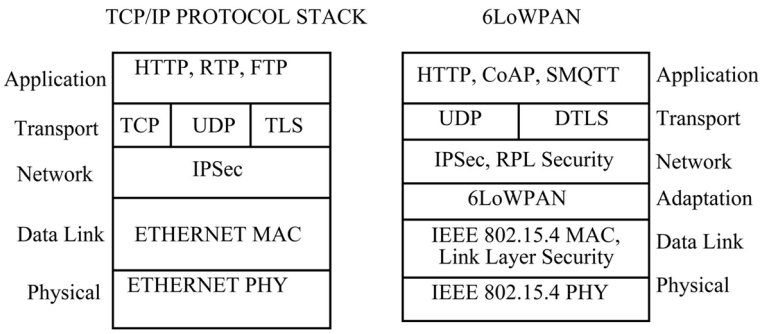

Fig. 2 Comparison of TCP/IP protocol stack with 6LoWPAN

- *Mesh management*: Managing mesh network creates overhead. Adding a security feature to it further creates additional overhead.
- *Low Rate*: IEEE 802.15.4 supports an over-the-air rate of 250 kbps and low data rates of 20 kbps, 40 kbps, 100 kbps, respectively.
- *Low Power*: Small batteries run for months or even years.

2.1 Security Requirements in 6LoWPAN

Security is essential in 6LoWPAN devices as they are always connected and accessible over the untrusted network. 6LoWPAN devices may carry sensitive information, and thus, availability, integrity, and confidentiality of the data are crucial. When collecting data from multiple fragments, collated, analyzed, ensuring security to IoT devices becomes a significant problem. IoT security protocols are different from traditional security protocols. Conventional security protocols need more processing power and hence, cannot be used in battery-operated devices. With the constraints of wireless sensor networks like limited energy, limited capacity, unreliable communication, high communication latency, and unattended node, the security mechanism must be designed to find a balance between the node constraints and also ensuring security [76, 125]. Security in 6LoWPAN devices have three configurations, i.e., i) between devices, ii) between border router, and devices and iii) between server and border router as shown in Fig. 1. Essential security services in 6LoWPAN based IoT network can be listed as follows:

- *Confidentiality:* Confidentiality is to prohibit sensitive information from unauthorized people by granting access to the authorized user only. For example, an unauthorized person can steal valuable information in an intelligent home. Unlike traditional Wireless Sensor Networks (WSNs), IoT devices are always accessible, so End-to-End (E2E) secrecy is essential in IoT [67]. Methods used to ensure confidentiality is data encryption, biometric verification, and secure tokens.
- *Data Integrity:* In broadcasting IoT communications, an adversary can continuously sense the medium for tampering or eavesdropping on the message sent by the user. Data integrity helps the receiver to identify whether the data alter or not. The IoT devices could end up communicating and controlling the faulty appliances. In the patient monitoring systems, which provide continuous remote monitoring of patients, data integrity must be provided [49, 63]. Data integrity is obtain using Message Integrity Codes (MIC).
- *Data Authentication:* Data authentication allows a receiver to verify whether the claimed sender sends the data or not. For example, an authorized user inside or outside the house can obtain sensitive information like changing the dose of a diabetic patient, which can endanger his life. Hence, the authentication of such devices is necessary for critical IoT applications. Data authentication can be achieved by calculating the Message Authentication Code (MAC) [49, 67], hash functions [97], password mechanisms [11, 94], Digital signatures [33] etc.
- *Privacy:* Privacy becomes important in IoT as connected things generate an enormous amount of sensitive data like personal data. Privacy is the right of the user to act on its behalf to determine the degree to interact with its environment [52]. In the absence of any user interface or any adequate tool, it becomes difficult to regulate the data flow. For example, IoT objects like health monitoring devices,

wearable devices generate sensitive information. A patient's body attached to a smart device can periodically monitor his health condition by forwarding the resultant data to the remote physician through the Internet. For emergency cases, the physician can prescribe medicine or trigger instant injection. So protecting such sensitive information becomes essential [34]. Data control techniques like anonymization, encryption, aggregation, integration, and synchronization safeguard the data.

2.2 Possible Security Threats in 6LoWPAN Networks

The 6LoWPAN network suffers from various threats within its network and also from outside its network. Some of the most common security threats [81] in the network are as below :

- *Man-In-The-Middle attack* is an attack by which an attacker can modify or introduce the data or information in the network to manipulate the legitimate data or information [47].
- *Eavesdropping Attack* allows an adversary to view, listen, sniff the data transmitted without the knowledge of nodes involved and thus, hampering the privacy of the communicating nodes [9, 41]
- *Replay Attack* is when the adversary spies on the valid data transmitted between the sender and receiver and prudently replay or delays the data to one of them [41, 45, 115].
- *Packet Injection/ node reprogramming* makes clone or duplicate packet. A compromised node can inject a message over the network to force the end-point to request re-transmission [81].
- *Denial-of-Service Attack* floods the device or gateway with spurious messages or excessive querying, leading to dysfunctional or inefficient performance [26, 45, 47].
- *Flooding Attack* floods the network with large packets until it occupies the entire bandwidth [14, 45].
- *Fragmentation Attack*- In the 6LoWPAN packet fragmentation mechanism, packets are transmitted in fragments. When many fragmented packets are sent, the receiver cannot identify whether a legitimate fragment or a legitimate source increasing the risk of duplication and buffer overflow. Therefore, there can be attacks, i.e., fragment duplication attack or exhaust buffer, i.e., buffer reservation attack [35, 79].
- *Command Injection Attacks* are where an adversary uses the broadcast session credentials to bypass the authentication phase and inject false commands in the network [14].
- *Wormhole Attack* is an out-of- band connection between the nodes, where packets are forwarded faster than the normal packet [118]. The attacker eavesdrop a packet of one location and tunnels it to another location or by dropping data [81].
- In *Sybil Attack*, a node pretends to be more than one node using the identities of others. Sybil attacks launch against distributed storage, routing mechanism, data aggregation, misbehavior detection, etc. The usage of radio resources can detect Sybil attacks [118].
- *Physical Attack* makes node's resources inaccessible. Node destruction, relocation, and masking are some of the physical attacks which make the node's resource inaccessible [81].

- *Sinkhole aka Black-hole Attack* happens if a malicious node generates a special routing graph to transmit all network traffic to a single or several targets proceeding to a falsification attack [81, 118].
- *Redirect Attack* is where an adversary redirects packets to another legitimate receiver legitimate receiver in another link [45].
- *Neighbor Discovery Attack*, an attacker spoof the neighbor advertisement or neighbor solicitation [45, 46]. Neighbor advertisement and solicitation messages bind the IP addresses and MAC addresses.
- *Traffic Analysis Attack*, IEEE 802.15.4 does not protect an acknowledgment frame. An adversary can forge the acknowledgment of each data frame and create jamming to prevent the delivery of the specific packet [46].
- *Replication attack*, the attacker, inserts the replicated nodes in the network to test the reliability and response of the nodes in the network. [66].

3 Security Analysis in Existing 6LoWPAN Technologies

The advancement of 6LoWPAN has motivated different latest technologies to consider resource-constrained and scalable network implementation. Trending 6LoWPAN technologies are Bluetooth LoW Energy (BLE), Thread, ISA100.11a, and WirelessHART. A brief description of the various 6LoWPAN technologies with their security mechanisms used and possible threats in these technologies is shown in Table 3.

3.1 WirelessHART

WirelessHART [14, 75] is the first open standard for Wireless Sensor Networks (WSNs) designed for industrial automation and manufacturing. WirelessHART network architecture consists of HART devices, routers, gateways, and a high-resource network manager. WirelessHART provides confidentiality and integrity at the network layer and link layer with the help of CBC-MAC with AES128 bits and MIC, respectively. A network manager does the authentication of the link layer and MIC of the network layer. Some of the possible threats are *communication scheme attack*, where an attacker bypasses the authentication scheme using its credentials and inject false command in the network. *Direct Command injection attack* occurs where a fake broadcast packet is being forwarded to its neighbor by an attacker and when a phony broadcast packet is forwarded to the parent node. It is *bounced command injection attack*. Simultaneously, in *on-the-fly Command injection attack*, after receiving a broadcast packet, the malicious node forwards a modified version of the received packet to its neighbors, *flooding attack*, in which an adversary overloads the communication channel by transmitting various packets simultaneously. In the paper, [14], proposed an attack validation countermeasure to solve broadcast injection attacks. They did not address the problem of *command injection attacks* are where an adversary uses the broadcast session credentials to bypass the authentication phase and inject false commands in the network. Designing an IDS system for command injection attacks can be an open issue, and solutions for external attacks are also to be considered yet. Moreover, WirelessHART offers various mechanisms to increase the sensors lifetime but does not provide any mechanism to update security credentials which is again a drawback.

Table 3 Comparison of 6LoWPAN technologies

Technologies	Applications	Network type	Security mechanisms used	Possible attacks
Thread [64, 105]	Home	Mesh/star	AES encryption and authentication	Load alter attack, Jamming attack, Eavesdropping, Traffic analysis attack, sybil attack, physical attack
WirelessHART [14, 75]	Automation and Manufacturing	Mesh	Integrity with MIC (4bytes), encryption with AES-128, authentication with AES-128 CCM, key management with Symmetric AES 128 keys	Node-compromise attack, communication scheme attack, direct command injection attack, bounced command injection attack, on-the-fly Command injection attack, sybil attack, sniffing attack, flooding attack, Sinkhole Attack, DoS attack
ANSI/-ISA100.11a [10, 75]	Industrial	Star/Mesh	Integrity with MIC (4-16bytes), encryption and authentication with AES-128, Key management with Symmetric and asymmetric AES 128 keys	Deliberate exposure attack, physical attack, sniffing attack, routing falsification attack, jamming attack, flooding attack, Sinkhole Attack
Bluetooth Low energy (Bluetooth 4.0) [53, 72, 96]	Home management and monitoring	Star	Confidentiality with 128bit AES CCM cryptography, key management with Elliptic Curve Cryptography (ECC), authentication with MAC	Eavesdropping, Man-in-the-Middle (MITM) attack, packet injection attack, eavesdropping, password attacks, firmware attacks, rogue device attacks

3.2 ISA100.11a

ISA100.11a [10, 75] is a 6LoWPAN technology designed for automation and control systems with mesh or star network topology. ISA100.11a offers similar services as WirelessHART but provides additional services like frequent key updates, firmware updates, etc. The network components of ISA100.11a are sensors, routers, gateways, system manager, which offers resource allocation and communications, and security manager for providing security services. ISA100.11a provides security at the link layer and transport layer. Link-layer integrity provides MAC MIC (MMIC) in payload and encryption using the AES algorithm. The MIC offers the integrity of the header and payload with nonce and timestamp and secures symmetric and asymmetric 128-bit keys at the transport layer. Authentication and confidentiality are provided with a network key and session key, respectively. Threats possible in such networks are deliberate *exposure attack* (adversary obtains the join key and ID of a session manager and deceives the authentication mechanism that it is the legitimate node), *physical attack*, *sniffing attack* (an attacker compromise link key to obtain network key to read the content of any message), *routing falsification attack* (adversary gives false information about the connectivity and the quality of network links of the network to the system manager), *jamming attack* (transmitting channels are blocked by generating noise in RF channels by an attacker), *flooding attack* (communication channel overloaded by sending various packets simultaneously). Multiple countermeasures resolve these threats; still, lightweight security solutions remain a challenge. One of the significant drawbacks is all Internet-based applications must support ISA100.11a, i.e., ISA100.11a is not an open standard.

3.3 Thread

The existing wireless mesh protocol does not meet the requirements of the new era of connected devices. There was a need for a new wireless mesh protocol with resilient mesh characteristics such as reliability, self-healing and extending, avoids single point failure, and interference robustness for critical infrastructure. Therefore, Thread was developed [64, 105] for secure wireless mesh networks with a large number of connected devices. The Thread was designed for low power and low bandwidth home devices with critical infrastructure. It is built on 6LoWPAN technology, which runs over IPv6 and IEEE 802.15.4. The Thread can support up to 250 devices per network and appliances like climate control, energy management, lightening, security, access control features. It can support various applications such as CoAP and smart Objects, Zigbee Smart Energy 2.0, ECHONET Lite.

It is vulnerable to attacks [41] like (i) *DoS attack:* an intelligent home network with constrained devices, an attacker with an excellent computational resource like PC overloads tiny devices with messages, making the device unable to respond to the legitimate device. (ii) *Frequency jamming:* Adversary adds noise in the radio frequency of the communicating nodes, thus affecting the communication mean and thus, disrupts the network. This attack is considered a sub-type of a DoS attack. (iii) *Eavesdropping:* In an intelligent home, an eavesdropper attempt to listen to the conversation between smart home devices and could break the privacy of the consumers. Thus, the attacker can launch various types of attacks by extracting consumer information. (iv) *Traffic Analysis Attack:* Attacker identifies the traffic flow patterns and the behavior of the user and launches an attack.

3.4 Bluetooth Low Energy (BLE)

Bluetooth Low Energy [53, 72, 96] is a standardized short-range communication technology developed for low-power and loosely coupled mechanisms for sensor data collection with easy integration with smart handheld devices. To support 6LoWPAN compressed BLE communication, both the smart device and remote user sides support 6LoWPAN header compression mechanisms. BLE has fewer security features than traditional Bluetooth. BLE provides link layer security with end-to-end security between two neighboring nodes providing protection from *eavesdropping* (i.e., an attacker listens to the pairing process and obtains the packets transmitted to obtain keys) and *man-in-the-middle attack* (i.e., an attacker gains access to the network with malicious association and can monitor network traffic or provide false information). Some other possible attacks are *password attacks*, *firmware attacks* (i.e., attacker use high-level firmware update service to change the firmware), *rogue device attacks* (i.e., adversary device begins to advertise as legitimate). Therefore, developing lightweight IDS for BLE is an issue. BLE security with keys consists of three phases; in the first phase, communicating devices agree on the second phase. The second phase generates Short Term Key (STK) and distributes a 128-bits Long Term Key (LTK); the third phase computes link-layer encryption and authentication. BLE security is not scalable for dynamic mesh topology, and managing BLE mesh with security is challenging. Group communication is an essential feature of the 6LoWPAN network; providing secure group communication in BLE and is another vital issue.

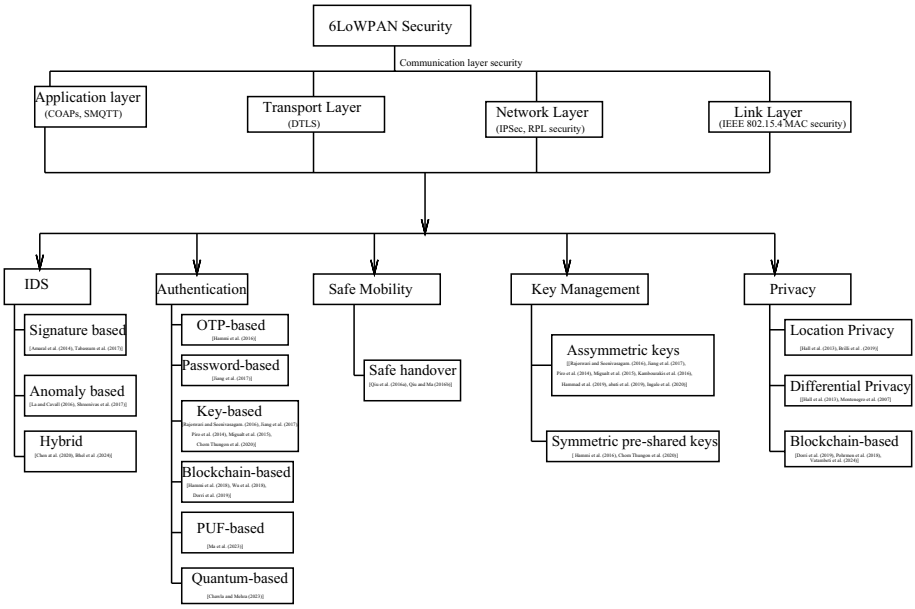

Fig. 3 Taxonomy of security in 6LoWPAN-based IoT networks

4 Existing Security Protocols for 6LoWPAN-Based Networks

This section gives an overview of possible vulnerabilities across different layers of 6LoWPAN networks. Different solutions to the existing problems are discussed below. A classification framework can be seen in Fig. 3. The solutions are classified based on the supports for authentication, safe mobility, key management, Intrusion Detection System (IDS), and privacy over different layers of the protocol stack.

4.1 Application Layer

Data aggregation and encryption operations are done in the application layer. Constrained Application Protocol (CoAP) satisfies the requirements of the tiny device with a low rate and light protocols.

Constrained Application Protocol security (CoAPs) [27, 36, 41, 90] and Secure Message Queuing Telemetry Transport (SMQTT) [111] are the security protocols which serves the purpose. Datagram Transport Layer Security (DTLS) protocol is used in CoAP to provide security is COAPs. Traditional protocols like TLS are not suitable for 6LoWPAN, TLS connection setup consumes more resources and TLS/SSL session, and key management requires many message exchanges. DTLS is an extension of TLS suitable for UDP connection. DTLS allows client/server communications in a way that prevents eavesdropping, tampering, and message forgery.

Traditionally used symmetric key-based authenticationfor obtaining security. Due to its limitations, certificate-based authentication was proposed in the literature to solve these problems. Hummen et al. [36] proposed a DTLS certificate-based authentication for tiny IoT devices. However, resource-constrained challenges like limited CPU, ROM, RAM, and energy resources made it infeasible. A DTLS header compression scheme developed for a 6LoWPAN standard called Lithe [93] proves to reduce the energy consumption using DTLS header compression in 6LoWPAN standard. It also reduced transmitted bytes without compromising the security properties of DTLS. Security features in the MQTT protocol called SMQTT [111] provide security with Attribute-based Encryption (ABE) using Elliptic Curve Cryptography (ECC). Still, their security features do not consider any protocol adaptability.

Also, Machine-to-Machine communication integrates heterogeneous devices with constrained nature and sensitive information. In paper [27], the author explored the recent security threats in communication provided in devices with the help of CoAPs, and analyzed these threats with the help of threat analysis and countermeasures in Contiki OS V.3.0. In paper [41] De Jesus et al. identified security threats in CoAP-based communication protocol in 6LoWPAN smart-home network. However, only the computational overhead of Eavesdropping and DoS attacks was computed and analyzed, and no mechanisms were performed to prevent these attacks.

In paper [29], Granjal et al. proposed an authentication mechanism with mobility for the applications running on Internet clients and sensor devices. Author considered mobility with end-to-end communication with the Internet host and the CoAP devices. Authentication using the public key and CoAP certificate for high security and pre-shared key CoAP security for light security mode, but transparent to the communicating parties.

The biggest challenge is to keep high performance while maintaining the balance between security and protection and hence, performance. There are still areas where DTLS is lacking and can be considered a potential threat.

4.2 Transport Layer

With increasing connected devices, a massive number of confidential data generated traverse through the Internet. A secure and able connection is required in various applications to protect confidential data. TLS provides security in the Transport layer, but the resource-constrained nature of devices enhanced TLS called Datagram Transport Layer Security (DTLS) enhances security. DTLS provides security in UDP-based applications as same as TLS protects TCP-based applications where its records are 8 bytes longer than TLS [79]. DTLS also provides security for CoAP and is the default security scheme for CoAP applications called CoAPs for resource-constrained devices. Like IPSec, it also provides end-to-end security. DTLS consists of a handshake phase and a data transmission phase. The handshake phase consists of a cipher suite list for agreement between client and server and key agreement between client and server. IANA registers 301 cipher suites by 2015. So, heterogeneous devices may use various cipher suites with different cryptographic primitives, creating a burden to tiny IoT devices. The certificate-based cipher suite used in DTLS uses Public Key Infrastructure (PSK), which creates overhead to constrained devices. DTLS protocol supports peer authentication in its handshake phase.

Identifying the limitations of the existing security mechanism in DTLS, a paper for lightweight security mechanism [56] provided virtual things as remote intelligent physical devices in secure IoT cloud for the worst-case scenario. Lakkundi et al. evaluated the proposed system in tiny devices with 48 KB ROM, 10 KB RAM, and an msp430 CPU, unlike most existing studies with Class 2 devices with 250 KB ROM, 50KB RAM. Instead of using a complete handshake mechanism, only DTLS record layer protocol is used. But its limitations were that there was no security support for mobile devices, and the proposed scheme uses a pre-shared key for the secure bootstrapping phase. Although using a pre-shared key is efficient for tiny IoT devices, the whole network gets compromised if one device gets compromised. Moreover, the DTLS handshake suffers two significant problems. The server suffers from a DoS attack where an adversary repeatedly sends ClientHello messages making it resource exhausted and unable to respond to the legitimate nodes. Other is the key management issue; the server maintains the key and distributes it in a pre-shared key manner. The scenario is suitable for static scenarios but in a dynamic environment supporting many keys by server becomes tedious and inefficient. So, lightweight security architecture was proposed in [114] solving these issues, and the key establishment and management were shifted to a trusted third party rather than server thus, decreasing overhead.

Marco et al. [114] instead of generating a stateless cookie value, after receiving the first ClientHello message, the server replies with a Helloverify request with a local cookie generated by the server. The client replies with the cookie generated by the server after successful reception. This process will make the attacker challenging to launch an attack even after receiving the cookie from the server since the attacker uses a spoofed IP address. However, the proposed scheme relies on a Trust Anchor entity which is the drawback of the proposed method.

4.3 Network Layer

Network layer security is provided basically with the help of IPSec and RPL. The details of both the security protocol are discussed below.

4.3.1 IPSec

The network layer provides E2E security. Some existing network layer protocols are IPv6 and RPL. IPSec and RPL security provide security in 6LoWPAN based network. IPSec provides end-to-end security in the network layer. IPSec protects data transferred in the IP layer. IPSec uses AH, and ESP for traffic security and IKE for key management [40, 92]. IPSec AH performs authentication using a cryptographic hash function with the available key for sender and receiver. The hash value is calculated in source and placed in Integrity Check Value (ICV) is then recalculated and verified at the receiver side. Field Programmable Gate Array (FPGA), a reconfigurable hardware platform for applying cryptographic security, was proposed by Muzaffar et al. [40]. Also, in [92] which proves to be efficient than software programmable processor. FPGA implemented for IPSec AH protocol supports both tunnel and transport mode in IPSec and uses the AES cryptography algorithm. But due to its overhead and extra memory for coupling makes it difficult to implement in tiny 6LoWPAN devices. Mobility is an important characteristic in the dynamic environment of resource-constrained devices. Mobility-aware solutions increase connectivity and enhance adaptability with a change in location and its infrastructure. 6LoWPAN technology requires a dynamic environment with seamless handover, flexible roaming, and an inter-operable mobility protocol. HMAC-SHA1-96 provides authentication in IPSec [40].

The need for security in a smart home environment and the effect of the security settings like encrypted communication on the Quality of Service (QoS) by CPU time and elapsed time were measured [68]. Migault et al. [68] tested security with different IPSec configurations and platforms. The authors explain CTR and CBC authenticates the whole payload using HMAC-SHA1-96 while GCM and CCM authenticate block by block. Thus, their performances were dependent on CPU and were more sensitive to MTU. Therefore, variations on MTU create variations in cryptographic blocks. The effect of different IPSec parameters in the communication network was identified, and also, overhead caused by using security and various authentication-encryption schemes in the network were identified. It was observed using IPSec in transport mode, and using IPSec over TLS seems more efficient.

4.3.2 RPL

RPL is the routing protocol in IoT and supports mesh networking [115]. RPL is a network layer distance-vector Routing Protocol for Low power and Lossy networks using IPv6. It uses the concept of *rank* to know the position of the node from its root and neighbors [110]. RPL supports message confidentiality and integrity and uses a link-layer security mechanism when necessary and appropriate. It has three basic modes of security, i.e., authenticated, pre-installed and unsecured mode as discussed in [115]. In unsecured mode, RPL messages are sent in clear without any security mechanisms; the pre-installed mode has pre-installed keys, which help nodes joining RPL instances to communicate securely, and in authenticated mode, nodes to join an authenticated RPL Instance. Wallgren et al., [118] analyzed various possible threats in routing protocol for the 6LoWPAN network and demonstrated various possible attacks using the Cooja simulator. A lightweight hear-beat protocol was developed to counter-measure these attacks [118], and also, IDS [85] to detect such attacks. A

trust-based strategy for detection and prevention of replication attacks was proposed by Bacem et al. [66]. The author identifies and counteracts compromised nodes by deploying the tested replica nodes. These tested replica nodes are deployed in the network to identify the compromised nodes by the reaction of the tested witness nodes. Also, Abhinaya et al. [6] propose an appropriate load balancing and malicious node detection mechanism in RPL. A secure RPL routing protocol efficiently distributes the load in different nodes and mitigates the DODAG Information Solicitation (DIS) flooding attack.

4.4 Adaptation Layer

The Maximum Transmission Unit (MTU) size for IPv6 packets is 1280 octets, whereas MTU for IEEE 802.15.4 is 127 octets with a MAC MTU of 102 octets. However, due to the maximum frame overhead, the IPv6 packet cannot fit in an IEEE 802.15.4 frame. To resolve it, a fragmentation and reassembly layer between network and link layer called the *adaptation layer*. No fragmentation is required if the IPv6 packet fits in a single IEEE 802.15.4 frame. Otherwise, the datagram is broken into 8 bytes of multiple fragments [69]. Address auto-configuration feature of IPv6 does not provide any security features. Therefore, the problem of duplicate addresses by accident or forgery can happen. Packet fragmentation is vulnerable unidirectional or bidirectional fragment replays called *packet fragmentation attack*. Some of the existing solutions to such attacks are adding a new field in the fragmentation header to support security. DTLS is used as a protection in CoAP, but its heavy computation and handshake in messages cause message fragmentation. Therefore, avoiding fragmentation whenever possible becomes important to avoid fragmentation attack [93].

4.5 Link Layer Security

For low data-rate and short-range communication, IEEE 802.15.4 has been most widely used [102]. It defines the physical and link layer for low-power devices. At the link layer, all the frames are to be secured with encryption or other mechanisms defined. Adding security procedures integrated to tiny devices further induces computational overhead.

Link layer provides security features like access control, message integrity, message confidentiality, and replay protection [28, 60, 102].

IEEE 802.15.4 MAC provides security to both packet header as well as data in paper [60]. IEEE 802.15.4 devices has a choice of its security suite like authentication only, encryption only, and authentication and encryption, and IEEE 802.15.4 radio chips have Access Control List (ACL), which can support up to 255 entries. ACL consists of 802.15.4 address, security suite, cryptographic key, and nonce for replay protection. There are two ways of sending the packets: (i) sends packets without any security credentials, (ii) if security is requested, then the destination address Media Access Control (MAC) finds the appropriate entry in the ACL table. If there is a match in the ACL entry, encryption, or authentication to the outgoing packets and the flag value sets. When no entry matches the destination address, the default ACL entry sets. If there is no entry in a default ACL entry, then MAC returns with an error code. Similarly, if security is not requested for packet reception, the packet is sent; else, MAC finds the appropriate entry in the ACL table based

on the sender's address. Then, appropriate required security is applied and if no entry matches in the ACL table error message is sent.

In paper [102], the author analyzed IEEE 802.15.4 MAC security capability to know its limitations in the IoT. Attacks occurring in frame structures like Contention Free Period (CFP) and Contention Access Period (CAP) are identified and explored. In a CFP attack, attackers choose low back-off time by observing relevant slot information from the beacon, making the channel permanently busy. An explicit Auxiliary Security Control field is inserted in the MAC header to handle security features in IEEE 802.15.4. But they did not specify how to securely add a new node in the 802.15.4 network, the authentication protocols, and the keying mechanism required by a new node to join the network. Moreover, the safe handover of the signaling information is also to be considered.

Sciancalepore et al. [107] discussed securing MAC packets using symmetric-key cryptography techniques with upper layer support to create and exchange encryption keys. Sciancalepore et al. proposed simple, secure framework architecture for providing security features IEEE 802.15.4 link layer and described key management protocol to negotiate link keys among devices. Security was provided for five different security levels addressing the heterogeneous IoT devices: (i) *confidentiality and Integrity of all packets*, (ii) *No security*, (iii) *only message integrity* and (iv) *Hybrid secured*.

Node compromise becomes a major problem in IEEE 802.15.4 nodes since the nodes support pairwise keys. Therefore, Konrad et.al [51] proposed a new pairwise key establishment scheme adaptable in various 6LoWPAN applications. Pairwise key proves to be feasible for unicast frames, but it is not efficient for broadcast frames. So Public Key Cryptography (PKC) remains inappropriate due to time and energy-consuming on nodes. Resolving, using Elliptic Curve Cryptography Digital Signature Algorithm (ECDSA), but its high energy consumption of ECDSA signature generations made it infeasible. So Adaptable Pairwise Key Establishment Scheme (APKES) authenticates and encrypt a uni-cast message, Easy Broadcast Encryption and Authentication Protocol (EBEAP) used to authenticate and encrypt broadcast which does not use PKC. APKES can prevent unauthorized nodes from joining the network, EBEAP can authenticate broadcast frames using broadcast keys. However, RAM overhead increases with increasing nodes, and if a node is compromised, then the attacker can still inject malicious nodes.

In paper [50], they solved the issues of APKES. Krentz et al. proposed a secure system for resource-constrained mobile nodes using a session key which helps to avoid swapping and survive reboots. To handle mobility, when a node gets out of range and a new node comes into the field, authentic UPDATE, UPDATEACKs are used to delete the permanent disappearing neighbor and Tickling HELLOs to discover a new neighbor. But the proposed scheme is not suitable for the dynamic nature of IEEE 802.15.4 networks and does not support mobility. Moreover, key revocation and rekeying are yet to be considered again.

Yang et al. [124] studied various security suites, encryption schemes, and various security vulnerabilities in IEEE 802.15.4 networks. Moreover, the authors analyzed security overhead using security for AES encryption, processing cycles per block, different acknowledgment schemes, etc., in the IEEE 802.15.4 MAC. AES adopts 128-bit block size and 128-bit key size. Some of the significant problems in replay attacks were solved using a sequential frame counter. A timestamp is a frame counter, and the sender compares the current time with the timestamp after receiving the frame to solve the problem. If the timestamp is lesser than the timestamp, it rejects the frame considering an attack. After waking up, the sender contacts its coordinator and updates the timestamp with the current time, thus preventing DoS Attack. But using timestamps increases the field length.

Some of the crucial security issues identified were initialization security, how a new node joins securely in the IEEE 802.15.4 network, how the generation and exchange of keys take place, how mackeytable has been build etc., ([80], and [34]). A security framework was proposed in [82] to resolve the problem, with an efficient mechanism for initializing security in different security architectures of IEEE 802.15.4 domain. Also, the authors proposed a lightweight mechanism describing negotiating keys. For providing security in the initialization phase, secure communication was provided at the setting-up stage, creating a bootstrap phase for FFD and RFD of 6LoWPAN and a key negotiation phase to solve the problem of using a pre-shared key. Implementation of the security framework is yet to be considered.

Various available security mechanisms in different 6LoWPAN layers were discussed and evaluated in Table 4. A comparison of possible attacks and security solutions in different layers of 6LoWPAN is shown in Tables 5 and 6 respectively.

5 Open Issues and Challenges

6LoWPAN is a promising IoT technology, and it has specified the essential issues of Machine-to-Machine (M2M) communication. It has various security issues to be addressed and unspecified, with many vulnerabilities existing and its development. Some of these issues are as follows:

5.1 Key Management

Key management remains an important issue in security. The key used for cryptographic security should remain secret throughout the lifespan of the network, i.e., from the deployment to revocation [51, 90]. Therefore, key management is also a concept of authorization because these keys are with devices that prove legitimate [21]. The traditional key management schemes for 6LoWPAN are of three types: trusted-server scheme, pre-distribution scheme, and public-key cryptography scheme [81]. Kerberos [71] is an example of the trusted-server key management scheme, where the server manages the key agreement between the nodes. In the pre-distribution scheme, the secret key is distributed to all the 6lowpan nodes in the network before network deployment. The intruder node before the node deployment can easily breach the network. Due to the usage of a single key, the whole network gets compromised if the key is compromised. Public-key cryptography or asymmetric cryptography is the use of public-key certificates for key management mechanisms. The typical examples of such key management schemes are Diffie-Hellman key agreement, RSA, ECC key exchange mechanisms [61]. Using asymmetric keys for resource-constraint 6lowpan devices is still challenging due to heavy certificates. The link-layer provides security features like authentication, confidentiality, frame integrity, and data freshness by making the frames cryptographically protected. But there is no mechanism to add a node securely and to manage these cryptographic keys. To resolve the problem, 6iTSCH introduced a security framework with a master key distributed at the initialization phase, network key shared by nodes after authentication, and authorization by authorized nodes and link keys between the neighbor nodes. However, if the master key is not secured cryptographically, an adversary can access the key and the whole IEEE 802.15.4 network. Link keys use asymmetric cryptography using public/private key and certificate which is heavy for resource-constrained devices [27, 36, 40–42, 70, 114]. Lightweight mechanisms for

Table 4 Various security mechanisms for 6LoWPAN-based IoT based on literature

Layers	Existing solutions	Security features	Security mechanisms used	Issues
Application layer	CoAPs [36]	Authentication	Header compression	Resource-constrained challenges makes it infeasible
	Lithe [93]	End-to-End security	Header compression	Only header compression done
	CoAPs [27]	Integrity, Confidentiality, DoS Protection	MIC, TLS-RSA with AES-128-CBC-SHA, Cookie	EPOCH time used for configuring cookies always starts with zero, therefore, cookies can be predicted easily, keys are not generated randomly or distributed in a safe way
	CoAPs [41]	Confidentiality, DoS Protection	AES encryption, Firewall	Identified overhead of only Eavesdropping and DoS attack
	SMQTT [111]	Confidentiality	Attribute Based Encryption (ABE)	No protocol adaptability
	CoAPs [29]	Authentication, Confidentiality, Replay attack, DoS Attack	ECC public key mutual authentication, AES/CCM encryption, ticket	Trust model is considered in the integration scenario and solves external attacks only
	CoAPs [90]	Authentication, Confidentiality, Replay attack, Integrity	TLS-PSK-WITH-AES-128-CCM-8, ECDHE-ECDSA-WITH-AES-128-CCM-8	DTLS does not support multicast messages
Transport layer	DTLS [79]	Integrity, Confidentiality, Authentication, fragmentation attack protection	Hash function, ECDHE, AES-128-CCM-8, decreasing key block size	No security support for mobile device, use pre-shared key for secure bootstrapping
	Lightweight DTLS [56]	Confidentiality, Authentication	AES CCM, Secure Hash using SHA-2, keyed-hash message authentication code	Session based security features in different layers is to be considered
	DTLS handshake [114]	Integrity, Replay Protection of old ClientHello message, lightweight Key management	Message Authentication Code (MAC), Sequence Number, Pre-Shared Key (PSK)scheme	Proposed security architecture relies on a Trust Anchor entity

Table 4 (continued)

Layers	Existing solutions	Security features	Security mechanisms used	Issues
Network layer	IPSec [68]	Integrity, Confidentiality, Authentication	AES-256-CTR-SHA1, AES-256-GCM16, AES-256-GCM16	AES is not lightweight and may have overhead
	IPSec [92]	Replay Protection, integrity, end-to-end security	FGPA-based IPSEC-AH in both transport and tunnel mode operation, 256 bit SHA-3 , ICV	Key configuration and distribution is not considered, confidentiality is not provided etc
	RPL [118]	Confidentiality, Integrity, Authentication, Replay protection	AES-128 bit MAC, one way hash chains and signatures, Consistency Check (CC) control message	No protection against active attack like DoS attack, replay attack and spoofing attack, provides only hop-to-hop security

Table 4 (continued)

Layers	Existing solutions	Security features	Security mechanisms used	Issues
Link layer	IEEE 802.15.4 MAC [60]	Integrity, Confidentiality,Replay attack, access control	AES-CTR, AES-CBC-MAC, AES-CCM	AES security mechanism is relatively loose and not suitable for LR-WPAN
	IEEE 802.15.4 [102]	Replay Protection, Confidentiality, integrity	MIC, ENC-MIC	No mechanism to securely add a new node, considered only for static environment
	IEEE 802.15.4 [107]	Confidentiality, Message Integrity, Dos protection	AES CCM, MIC, using cookie	Proposed scheme considered single hop senario and dynamic key management scheme requires extra computational effort
	IEEE 802.15.4 MAC [51]	Authentication, Message Integrity, Replay protection	Easy Broadcast Encryption and Authentication Protocol (EBEAP), Message Integrity Code with Cipher Block Chaining (MIC-CCM), frame counter	RAM overhead increases with increasing nodes, can inject malicious nodes if a node gets compromised
	IEEE 802.15.4 MAC [50]	Replay protection, Hidden wormhole protection	Anti-replay across reboot	No mobility support, proposed scheme consumes more energy in dynamic scenario, key revocation and re-keying to be considered yet
	IEEE 802.15.4 Node compromise [124]	Replay protection, DoS protection	Timestamp, randomly generating nonce	Timestamp increases field length, using additional overhead separating nonce and frame counter
	Key establishment scheme [82]	Authentication, Bootstrapping	RSA or Diffie-Hellman algorithm, 128 bit Hash	Practical implementation is yet to be considered
	IEEE 802.15.4 security suite [54]	Prevention from physical attack	IDS using machine learning	Security is considered only for static environment

Table 5 Possible attacks in 6LoWPAN based IoT network

Layers	Vulnerabilities	Description
Application layer	Eavesdropping [41, 81]	An eavesdropper listens to the conversation and launches various types of attacks by extracting the user information
	DoS attack [41, 81]	Attackers use a device overloading tiny devices with messages with superior computational resources, such as a laptop and launch attack
	Traffic analysis attack [41]	Attacker identifies the traffic flow patterns and identifies the behavior of the user and launch attack
Transport layer	Fragmentation attack [35, 79]	Due to fragmentation, a large number of packets are re-transmitted which increases the risk of duplication
	Denial of service attack [26, 114] and [29]	Attacker disrupts and gains information about data being transmitted. For example, repeatedly sending ClientHello message making server resource exhausted and unable to respond to the legitimate nodes
	Traffic analysis attack [26]	Finding out information about the data pattern of transmitted data
Network layer	DoS Attack [45]	The attacker node forbids node's communication which is under attack with others or the destination node in the network
	Redirect attack [45]	Attacker redirects the packet from last hop router or from legitimate receiver to another node in the network
	Sinkhole aka black-hole attack [81]	In this attack, a malicious node generates a special routing graph to transmit all network traffic to a single or several targets proceeding to a falsification attack
	Wormhole attack [118]	An attacker records the packet of a network and tunnels it into another network
	Replay attack [45]	Attacker captures valid messages and replays them later
	Sybil attack [118]	In such attacks, a node pretends to be another node, using the identities of others
	Duplicate address detection DoS attack [45]	In DoS attack, an attacker responds to all duplicate address detection attempts made by going through the host
	Neighbor discovery DoS attack [45]	A valid node who wants to join the network cannot join the neighbor discovery service because the router is busy in sending solicitations from the attacker
	Command injection attack [14]	An adversary uses the broadcast session credentials to bypass the authentication phase and inject false commands in the network
	Replication attacks [66]	The attacker inserts the replicated nodes in the network to test the reliability and response of the nodes in the network

Table 5 (continued)

Layers	Vulnerabilities	Description
Link layer	Node compromise attack [51]	Devices are in an unattended environment so attacker extracts cryptographic details and lead to a physical attack
	Frequency jamming attack [41]	Adversary adds noise in the radio frequency of the communicating nodes thus affecting the communication mean and thus, disrupts the network. This attack is considered sub-type of DoS attack
	Replay attack [50, 51] and [124]	Attackers can inject and replay IEEE 802.15.4 frames like HELLOACKs
	Node replication attacks [51]	Attacker uses the identity of the compromised node on an unauthorized node
	DoS attack ([51, 124] and [110])	flooding hello command DoS attack is launched
	Hidden wormhole attack [50]	In large IEEE 802.15.4 network, some anti-replay data must be swapped to non-volatile data. So, these invalid data are treated as neighbor's data and which are further stored forever
	Hello flood attack [50]	Attacker compromised node and broadcast fresh authentic message to expend energy and memory of receivers
	Same-nonce attack [124]	If the same nonce and same key is present in ACL entry, an attacker can obtain the useful information
	ACK attack [124]	Adversary doesn't wants receiver to receive data sent by the sender and sends an interference frame to the receiver when the sender sends data. Attacker sends forged ACK frame back to sender since ACK frame has no integrity
	Replay protection attack [124]	It is a DoS attack where adversary sends frames with a larger frame counter. The receiver upon receipt of the larger frame counter discards normal frame counter for replay protection and the normal service is denied
	Sinkhole attack [110]	An attacker illegally modify the ETX value and launch an attack
	Selective forwarding attack [110]	Attacker present in a routing path can advertise low ETX value and attract traffic towards itself

Table 6 Comparison of different security protocols based on the issues addressed in 6LoWPAN based network

Layer	Existing solutions	Authentication	Confidentiality	Integrity	Replay protection	DoS protection
Link layer	[60]	×	✓	✓	✓	×
	[102]	×	✓	✓	✓	×
	[107]	×	✓	✓	×	✓
	[51]	✓	×	✓	✓	×
	[124]	×	×	×	✓	✓
	[82]	✓	×	×	×	×
	[108]	×	✓	✓	×	×
	[51]	✓	✓	✓	×	✓
Network layer	[68]	✓	✓	✓	×	×
	[92]	×	✓	✓	✓	×
	[107]	×	✓	✓	×	✓
	[95]	✓	✓	✓	×	×
	[80]	×	×	✓	×	×
	[118]	✓	✓	✓	✓	×
	[127]	✓	✓	✓	✓	×
Transport layer	[79]	×	✓	✓	✓	×
	[114]	×	×	✓	✓	✓
Application layer	[93]	✓	✓	✓	×	×
	[36]	✓	×	×	×	×
	[27]	×	✓	✓	×	✓
	[41]	×	✓	×	×	✓
	[29]	✓	✓	✓	✓	✓
	[90]	✓	✓	✓	✓	×

resource-constrained devices are still an issue here. Moreover, both IPSec and DTLS support pre-shared keys. If the key is not secured cryptographically, an attacker who can get this key can control the whole network. Therefore, defining key management mechanisms considering the resource-constrained nature of devices becomes an important issue. Key management in CoAP is also an issue.

5.2 Intrusion Detection System

Message security provides E2E security; still, due to globally accessible, resource-constrained, and lossy links, devices in 6LoWPAN based networks are vulnerable to many attacks. IDS is a security approach that monitors network activity to detect any intrusion or anomaly [80]. It is also a security mechanism against both inside and outside attackers. IDS detection is machine learning and signature-based. A network-based IDS approach and machine learning approach are mainly used for IDS [113]. A network-based IDS for wireless sensor networks has selected nodes called watchdogs, deployed for network IDS for preventing eavesdropping by watching abnormal behavior of neighboring nodes [11]. However, the proposed IDS system does not provide confidentiality, integrity, and

authenticity. IDS system with signature-based detection [11] needs promiscuous listening, which consumes lots of power and all anomaly detection mechanisms need machine learning methods, which are expensive and difficult for 6LoWPAN networks. The simulation was carried out in TinyOS 2.1.2 and InteliJ IDEA 12.3.1. The tools used were PPPSniffer and Finger2IPv6 to detect the sniffing attacks.

In paper [54], the author identifies the importance of the IDS system from a misbehavior node in the network. La et al. [54] provided an intrusion detection mechanism for malicious node detection. The detection algorithm includes the learning phase to identify the most common normal status of a network and the monitoring phase for misbehavior node identification and malicious path detection. But the mobility of the node was not being considered by the proposed algorithm. Foren6 in FIT-IoT testbed were used for experimental result. It is an open-source tool that passively captures 6LoWPAN traffic and renders it in a graphical user interface. IDS with a geographical hint in RPL [110] secure inside nodes from any malicious node. 6LoWPAN mapper constructs RPL DODAG (6BR) by collecting necessary information from each node at regular time intervals.

In SVELTE, it defines a request packet using a rank value that identifies RPL DODAG, but Shreenivas et al. [110] complimented ETX value with 6LoWPAN mapper and sends it with each request packet. ETX value of the parent node (6BR) is lesser than the ETX values of its child, and it keeps on increasing with increasing hop. Lower ETX values state that there is a better path to the 6BR. The use of IDS in both IPv6 and IEEE 802.15.4 is not feasible since it consumes more energy. Therefore, hybrid IDS considering both IPv6 and IEEE 802.15.4 network characteristics is yet to be considered. The evaluations were performed using Contiki 2.6 and Cooja. The power consumption with duty cycling and without duty cycling were measure. Expected Transmission (ETX) is used as a metric to measures path reliability for lossy networks.

In recent researches, attack analysis models with machine learning approaches have gained popularity [19]. The attack analysis model uses the zeroth-based optimizing technique with score-based adversarial models via gradient estimation. Still, the concept is new and in need of exploration in this field. The experiments were carried out on a Tesla K80 GPU and python. CleverHans and Foolbox were used to make the averserial models. A hybrid intrusion detection system is proposed by [15] against sinkhole attacks using the Hidden Markov model. The proposed method was capable of distinguishing between normal and malicious nodes. Attack analysis with multiple mixed attacks analysis is still required.

5.3 Authentication

Most of the 6LoWPAN technologies consist of sensitive information transmission, so protecting these data frames from being modified/or accessed by unauthenticated/ unauthorized users becomes vital. Authentication ensures that the claimed sender sends data. Therefore, authentication becomes very important. Authentication schemes are of two types: symmetric (shared common private key) and asymmetric (private and public keys) authentication. The broadcast nature of 6LoWPAN networks sends accurate data to untrusted receivers, and using symmetric authentication becomes infeasible and insecure. One of the major problems in the shared key is key distribution, how the key is shared among devices in the network, and using two keys again creates a problem how to manage different keys generated. Some of the existing solutions are AES symmetric-key algorithm, RSA, and ECC public key algorithm. Authentication in the IEEE 802.15.4 is possible using

the Key Source and Key Index field in the Key Identifier field of IEEE 802.15.4 MAC [82]. Authentication in IPSec takes place using HMAC-SHA1-96, CBC-MAC, GMAC [68]. AES CTR authenticates using HMAC-SHA1-96 in the whole payload, and GMAC authenticates per block basis.

[32] propose an asynchronous One-time Password-based authentication mechanism for tiny devices. The author provides MAC sub-layer authentication using challenge/response mechanisms. OTP is valid only for one transaction; therefore, an attacker cannot use it to authenticate even if it receives the message. The gateway or device generates a random number called to challenge and Pre-Shared Key (PSK) and sends it to the device that wants to authenticate. After receiving the challenge, the device generates an OTP using HMAC-SHA 256 based OTP (HOTP) encryption algorithm. On the other side, the gateway or device also computes OTP using the same encryption algorithm. Authentication mechanism provides security to replay attacks, some DoS attacks, and brute force attacks. The delay of the association operation is increased to 10 times using an authentication mechanism and does not provide data confidentiality. Moreover, it offered no mutual authentication. Testing were done in the OCARI stack software with C Language. Delays of the association operation were compared with or without authentication as a metrics.

A proposed mutual authentication scheme based on smart card and password security with bio-hashing proved the identity of the user in [42]. A formal automatic security analysis tool for security protocols called ProVerif is used in the work. Efficiency and security features were computed with state-of-art literatures.The authentication scheme proves to be efficient and prevents both possible active and passive attacks. An OAuth 2.0-based Authentication and Authorization framework [70] was proposed especially for constrained devices and networks. The scheme used a nonce-based symmetric authentication with Authenticated Key Establishment (AKE) protocol and Trusted Third Party (TTP). The following operations are measured: (a) TX: sending data over the radio, (b) RX: receiving data over the radio, (c) generating a True Random Number with the TRNG module, (d) Normal operation CPU consumption. The operations are used to calculate the energy consumption. A lightweight authentication with asymmetry feature of Rabin cryptography, unlike heavy RSA and ECC cryptosystems, was discussed in [42]. The scheme proved to be resistant to passive and active attacks, thus, creating a balance between security and efficiency. Secure, lightweight user authentication scheme with multi-gateway based key agreement in WSNs proves to be a better solution [91]. Recently, a symmetric-key lightweight authentication scheme with hash and XOR operation provides a feasible solution [21]. Designing a secure, lightweight authentication scheme is still an open issue. Designing a secure, lightweight authentication scheme is still an open issue.

One of the recent technologies used for IoT security and privacy is Blockchain. Blockchain technology helps in managing, controlling, and also securing IoT devices. It provides decentralized authentication and data integrity. It consists of a block of records with timestamps and validated using cryptography [33]. Public Key Infrastructure (PKI) and Bitcoins (Elliptic Curve Digital Signature (ECDSA)) provide authentication in smart home applications. The integrated 2-factor out-of-band authentication scheme with blockchain infrastructure with the help of Eris blockchain and relevant IoT computing devices [123]. The authentication mechanism includes two steps. In primary authentication, the device registers itself with the Nest server and obtains a valid token. The out-of-band channel is for secondary authentication, which helps prevent the compromising of the legitimate node even after accessing the correct token. A recent paper [127] provides an efficient authentication mechanism that provides trust, security, and privacy for a LoWPAN network by monitoring power consumption and storage requirement while running RPL.

[13], gave an extensive study on Machine-to-machine (M2M) and end-to-end (E2E) communications security with Authentication and Key exchange mechanisms. The study lacks a security analysis of existing 6LoWPAN technologies and future applications of 6LoWPAN technologies.

Recently, machine learning approaches have gained popularity for providing authentication in resource-constrained devices [86]. With the advantage of adapting and improving the system without being programmed dynamically, machine learning approaches has advantage over the traditional approaches. The Biometric-based authentication with machine learning approaches helps in authenticating the user and device. The biometric features can be keystroke [44], ECG [31, 37, 55], and fingerprint [12, 43].Ingale et al. [37] had a detailed comparative analysis of ECG Biometric Authentication with various filtering types, segmentation, feature extraction, and health status on ECG. The paper collected on-set and off-set data to analyze accuracy, false accept rate (FAR), false reject rate (FRR), and equal error rate (EER). Some of the latest research on authentication is Quantum-based Authentication [18]. Mutual Identity authentication is achieved by using quantum signature and orthonormal entanglement. Still, the topic is new and yet to be explored. Additionally, ECC and physical unclonable function (PUF) can mutually authenticate and key exchange between the communicating device [59]. Some major disadvantages are that hardware devices or sensors with PUF chips are mandatorily required, and the research field is new and needs more exploration.

5.4 Secure Mobility

Many 6LoWPAN applications may consist of devices that by nature moves from one domain to another of the same administration block. An example is a patient monitoring system, where the patient equips with 6LoWPAN enabled sensors. When the patient moves around the house or the hospital with the equipped sensors, the sensors should adapt the security mechanisms with mobility. Support for end-to-end security in constrained devices is an open issue and challenging when the devices are mobile. [88] proposed a safe handover ticket generation method for the mobile device within a network to achieve fast, secure authentication while performing handover. A Proxy Mobile IPv6 (PMIPv6), a Network-based Localized Mobility Management (NETLMM) protocol [89] allows a 6LoWPAN device to roam in a LoWPAN network securely. Mobility management is provided in Mobile Access Gateways (MAG) attached to Mobile Nodes (MNs). PMIPv6-based authentication schemes traditionally provide security in vehicular networks. A hybrid cryptography scheme supports MNs roaming within the 6LoWPAN network, and a key chain generated between 6MNs and 6MAGs omits repeated authentication when 6MNs are roaming within 6LoWPAN networks. But the proposed authentication scheme increases the overall computational overhead.

5.5 Providing End-to-End Security

The resource-constrained nature of sensing 6LoWPAN devices, providing end-to-end security with such devices, makes it difficult. In real-time applications like patient monitoring systems, sensitive information exchanged enables end-to-end security in such applications. At the link layer, the frame providing a shared master key provides a minimum security level. Each node can secure the key; the whole network is compromised if this node is captured. The key should be updated frequently when the frame counter

expires to resolve the problem. But there is no mechanism explaining how to update these keys. Confidentiality is provided only for the outside network, not for the inside network. No authentication mechanism has been defined for IEEE 802.15.4 network yet. Similarly, the network layer or transport layer could provide hop to hop or end to end security. In real-time applications like patient monitoring system, sensitive information is being exchanged, so providing end-to-end security becomes very important in such applications. At the link layer, frame providing a shared master key provides minimum security level in the link layer. Each node can secure this key but if this node is captured then the whole network can be compromised. To resolve the problem, the key should be updated frequently when frame counter expires. But there is no mechanism explaining how to update these keys. IPSec is a network-level security protocol that provides authentication with IPSec AH and with or without authentication with confidentiality using IPSec ESP. DTLS does not support well in CoAP proxy mode. When an HTTP client needs to access data from the CoAP back-end server, then there exists an issue with CoAP end-to-end communication. [28] proposed a lightweight end-to-end security solution in the adaptation layer called 6LoWPSec. 6LoWPSec performs data integrity, authentication, and confidentiality at the edge, i.e., 6LBR. To embed link-layer security in the adaptation layer, mesh under routing is turned on. The hardware implementation provides the link-layer security functions. Thus, reducing the computational overhead in latency, energy consumption, and efficiency compared to lightweight IPSec. However, key-management techniques are further to be explored in the same scenarios.

5.6 Privacy

Personal privacy on the Internet has already dwindled in recent years. With the introduction of IoT, with everyday smart objects exchanging sensitive information, privacy is as important and challenging as other security features [77]. The need for easy accessibility of data anytime makes it essential to protect the privacy of personal information. One of the possible ways to maintain user privacy is by using Trust management (TM) policy, and prospects of preserving personal data [9]. Privacy protection in the device, during communication, storage, and processing as shown in Fig. 4 ([52, 129]) are essential. Privacy in the device should protect the device from leaking sensitive information; for example, an intruder can obtain sensitive information after compromising a surveillance camera. Encryption provides communication privacy, and pseudonymization and anonymization provide storage and processing privacy [30]. Another method for providing privacy and protecting user traceability in 6LoWPAN networks is by [17]. An extension of the 6LoWPAN neighbor discovery protocol in [69] could simultaneously refresh the node's addresses after every specific time. Every node needed to change its address after every timeout impacting the routing. Biometric template privacy in [42], where user biometric information is not stored rather than a hash value of user biometric information called biohashing algorithm protects user privacy. The concept of privacy can still be explored and remains an open issue. A lightweight, scalable blockchain was proposed in [24]. Blockchain decentralization is obtained with an overlay network and high-resource devices to provide end-to-end privacy. Blockchain-connected gateways protect individual privacy by protecting the access of the user-sensitive data without their concern [83]. A recent research by [116] explain a blockchain-based data broadcast strategy with oppositional-based harmony search (OHS) optimization key generation technique. The privacy of the patient's health records was preserved using digital ledgers with hash and encryption. The

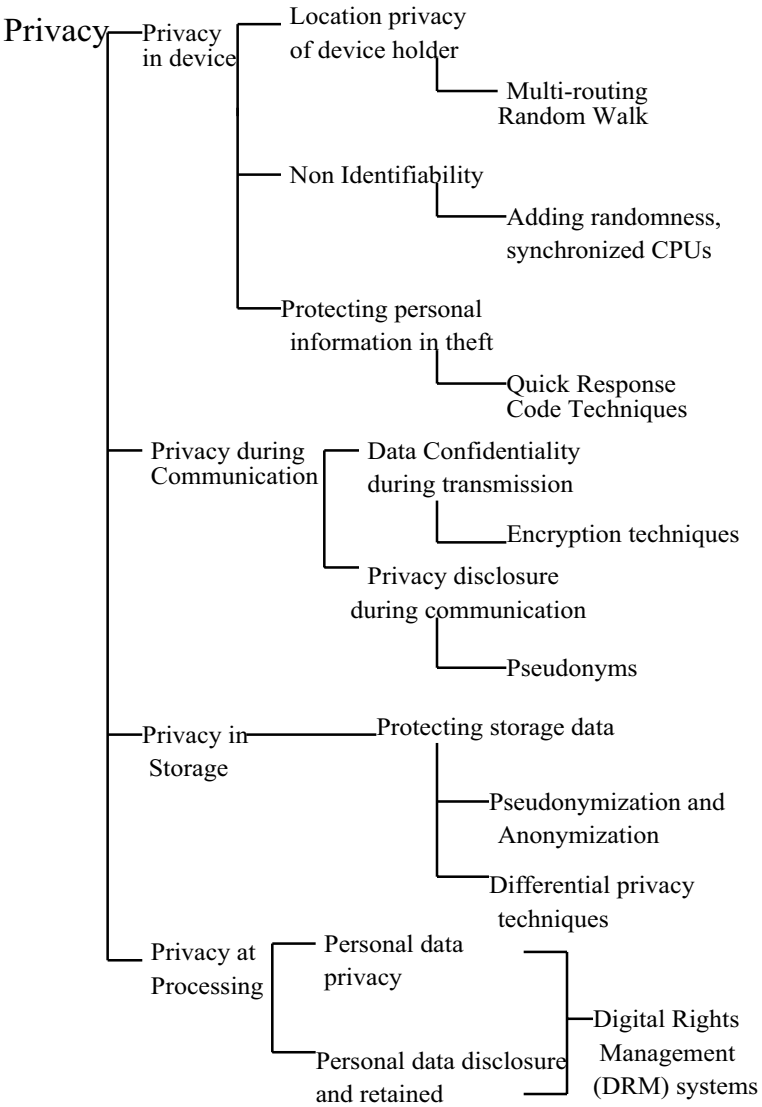

Fig. 4 Taxonomy of different types of privacy in 6LoWPAN-based IoT

attack analysis were not done. The summary on open issues of security in 6LoWPAN-based IoT is highlighted as shown in Tables 7 and 8. Additionally, an outline of the paper is given in Fig. 5.

5.7 Future Research Directions

Future research work may target the support of secured multi-hop scenarios for 6LoWPAN based IoT networks. Designing lightweight certificates, unlike heavy X.509 certificates, makes the computation overhead for tiny devices. Researchers can evaluate the

Table 7 Summary on taxonomy of security in 6LoWPAN-based IoT

References	6LoWPAN vision	Security types	Relevant attack	Placement strategy	Limitations	Validation	Tools	Performance
[11]	IDS	Signature	Traffic signatures and abnormal behaviors	Promiscuous listening for anomaly	Needs promiscuous listening, which consumes lots of power	Simulation	PPPSniffer, Finger2IPv6	FPR, Accuracy
[54]	IDS	Anomaly	Malicious attacks	Passively captures 6LoWPAN traffic and renders it in a graphical	No mobility of the node	Testbed	Foren6	Travel time, FPR, Accuracy
[110]	IDS	Anomaly	d ETX attacks	IDS with a geographical hint in RPL	he use of IDS in both IPv6 and IEEE 802.15.4 is not feasible since it consumes more energy	Simulation	Contiki OS	Power, Accuracy
[19]	IDS	ML	Hop-skipjump, Boundary attack	Optimizing technique with score-based adversarial models	New concept and in need of exploration in this field	Simulation	Tesla K80 GPU, python	Success rate
[32]	Authen-tication	One-time Password	Replay attacks	Challenge/-response mechanisms, Pre-Shared Key (PSK)	Delay, no mutual authentication	Simulation	OCARI stack software, Wireshark	Delay
[42]	Authen-tication	Lightweight	Imperso-nation, replay, insider attack	Asymmetry feature of Rabin cryptography	Computatio-nal overhead	Simulation	ProVerif	Efficiency, security features
[70]	Authen-tication	Nonce-based symmetric authentication	–	OAuth Authorization architecture	Attack analysis not done	Testbed	TX, RX, TRNG	Energy consumption

Table 7 (continued)

References	6LoWPAN vision	Security types	Relevant attack	Placement strategy	Limitations	Validation	Tools	Performance
[21]	Authen-tication	Lightweight	Replay, man-in-the middle attack	Xor and one-way hash, symmetric key	Lightweight authentication scheme is still an open issue	Simulation	AVISPA, BAN Logic	Commun-ication and computational overhead, computation time
[33]	Authen-tication	Lightweight	Spoofing, replay, DoS attack	Blockchain and ECC	Regulating and stabilizing amounts related to smart contracts, an optimization protocol for the miner distribution	Simulation	Ethereum, JSON	Energy, time -consumption, cost

Table 8 Summary on taxonomy of security in 6LoWPAN-based IoT

References	6LoWPAN vision	Security types	Relevant attack	Placement strategy	Limitations	Validation	Tools	Performance
[37]	Robust Authentication	Biometric	–	Kalman filter, feature extraction, and health status on ECG	Attack analysis not done	Simulation	FIR filter, Kalman filter	Accuracy, FAR, FRR, and EER
[88]	Secure mobility	Machine-to-machine communication	MITM, Impersonation, Sybil attack	Safe handover ticket generation method	Computation cost of the devices increases as the sensor device generate its own session key	Simulation	AVISPA, Protocol Composition Logic (PCL)	Computational, transmission overhead
[89]	Secure mobility	Lightweight	Replay, MITM, Impersonation	Network-based localized mobility management (NETLMM) protocol	Cannot withstand all well-known security attacks	Simualtion	AVISPA	Computational cost
[28]	End-to-End Security	Lightweight	Replay, DoS, Data loss attack	New security protocol called 6LowPSec	Key-management techniques are further to be explored in the same scenarios	Simulation	Contiki, Rime	Computational overhead, energy consumption
[17]	Privacy	Efficiency	–	An extension of the 6LoWPAN neighbor discovery protocol	Attack analysis not done	Simulation	Ns-3	Overhead analysis

Table 8 (continued)

References	6LoWPAN vision	Security types	Relevant attack	Placement strategy	Limitations	Validation	Tools	Performance
[42]	Authen-tication, Privacy	Biometric template privacy	Imperso-nation, modification, replay attack	Biohashing algorithm for biometric information	The concept of pri-vacy can still be explored and remains an open issue	Simulation	ProVerif, heuristic security analysis	Computational time
[116]	Privacy	Blockchain, Homomorphic encryption	–	Rectified linear unit (ReLU), pooling and a fully associated model	No attack analysis done	Simulation	Convolut-ional neural network	Accuracy, G-mean, Specificity
[59]	Authen-tication	PUF	Replay attack, impersonation attack, MITM attack	ECC and PUF	Hardware device with PUF chips mandatorily required, new field need more exploration	Simulation	Heuristic analysis, ROR model, proverif tool	Security, communication, computation overhead
[15]	IDS	Hybrid	Sinkhole attacks	Hidden Markov model	Attack analysis with multiple mixed attacks analysis is still required	Simulation-/ Testbed	Contiki , FIT IoT-LAB real testbed	Accuracy, precision, recall, F1 score

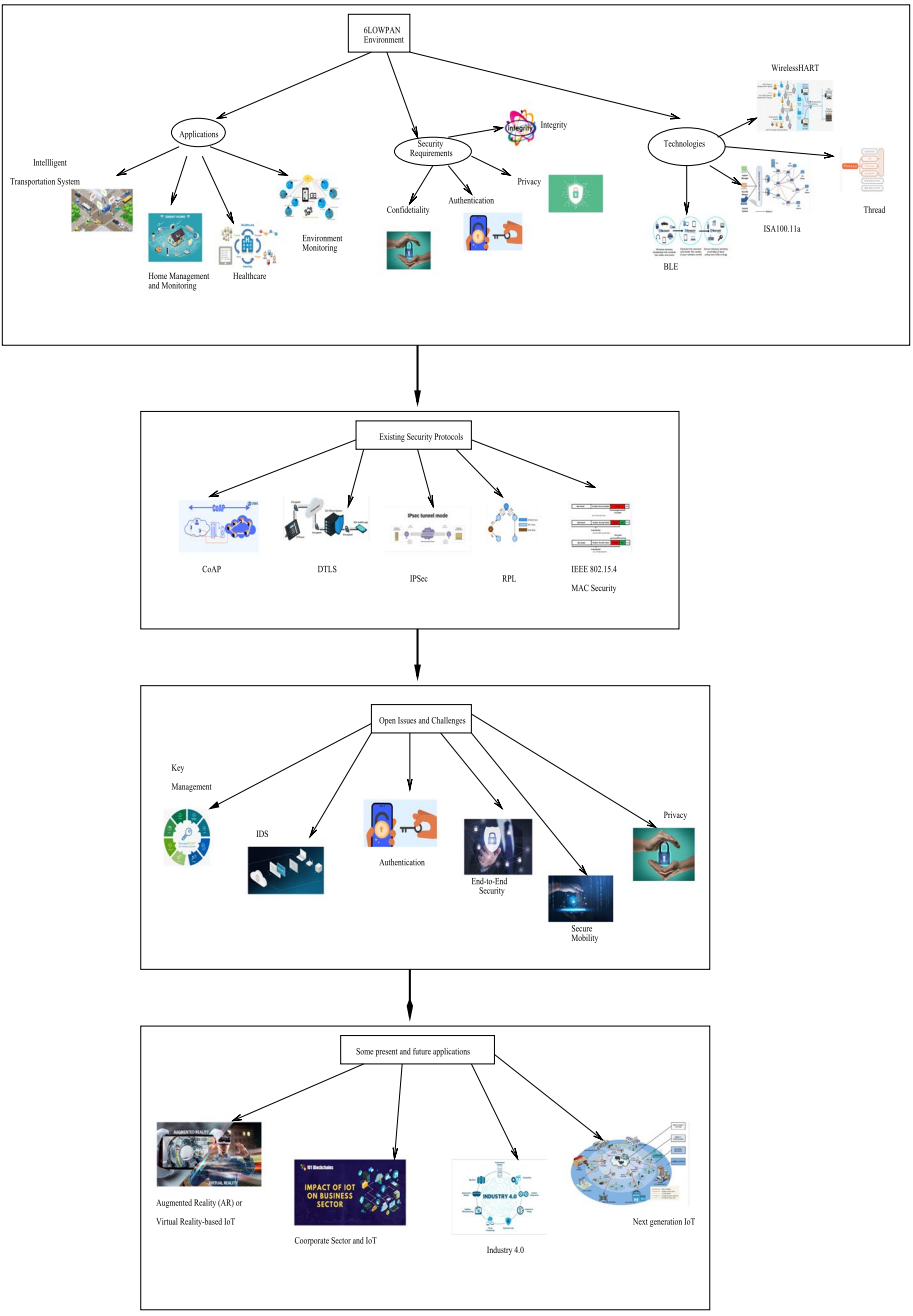

Fig. 5 An outline of the survey on 6LoWPAN security for IoT

computational overhead of using ECC and RSA encryption algorithms and instead use lightweight encryption algorithms like lightweight ciphers, which are more suitable for the constraint nature of devices [22]. Other important areas are designing lightweight IDS

systems considering the features of both IEEE 802.15.4 and IPv6 characteristics of such networks. Developing an intelligent IDS system independent of the network protocol and attacks can also be a feasible solution. Fog-based security solutions with edge computing can be evaluated and explored. The various advantages and disadvantages of such solutions are still unexplored in LoWPAN based IoT [87]. Blockchain-based authentication and privacy schemes can also be explored and incorporated in 6LoWPAN-based lightweight, and scalable network [24, 119]. Recent references like post-quantum [18], PUF-based [59] methods for authentication, key exchange, signature generator, etc., which solve both integer factorization problems (RSA, Diffie-Hellman) and discrete logarithm problems (Elliptic curve), can provide feasible security solutions [20, 103]. Incorporating machine learning and authentication can also create an opportunity to explore the advantages of artificial intelligence and authentication techniques for resource-constrained IoT. The experimental results are preliminary and do not fulfill the security requirements of a 6LoWPAN.

6 Some Present and Future Applications

We discuss some of the existing and the future applications of IoT-centric concepts are as described in the following section:

6.1 Augmented Reality (AR) or Virtual Reality-Based IoT

Augmented Reality (AR) is "extending the view of the real world and computer-generated images, videos, sound and GPS data" [84]. AR technology includes camera, image, and display processing engine, location sensors, etc. Some of the applications of AR are in the military, industry, medical, entertainment, and commercial [84]. An example of AR in smart cities is SmartSantander Project [2, 106]. SmartSantander RA applications include "environmental monitoring, outdoor parking area management, mobile environmental monitoring, traffic intensity monitoring, parks and garden irrigation, free parking guidance, etc". Some of the other examples are "AR-enhanced automotive windshields and powerful head-mounted displays (HMDs) such as Microsoft's HoloLens [3, 65], Apple's AR system [4], smartphones transformed into HMDs using low-cost peripherals like HoloKit [5]". The latest research on VR is on stress Diagnosis. Electromyography (EMG), galvanic skin response, oxygen saturation level, and heart rate are some of the features to detect stress. Ahilan et al. [7] explored statistical data analysis with CNN and MATLAB software. Even though it is beneficial, more exploration is required. As AR/VR technology is adopted rapidly in different sectors and security, privacy is in its infancy. Therefore, intelligent solutions for immersive yet safe future AR applications are essential [8].

6.2 Coorporate Sector and IoT

IoT in business helps to meet the requirements of business enterprises [23]. Some of the examples of such applications are Microsoft cloud-based solutions, IoT-based video developed by Banco de Cordoba [23], IBM smart car launch service called Car2go [1]. These design solutions have enabled security solutions for their efficiency. IoT enhanced in Business can elevate operational efficiency and productivity [25]. There is a massive

challenge in combining technological and modeling structures of both domains concerning systems, devices, and operations. Efficient systems security design is also challenging.

6.3 Industry 4.0

The new concept of the industrial revolution with IoT is industry 4.0 [39, 100]. Industry 4.0 vision is to provide large-scale manufacturing and production of goods with efficient, fast, and cost-effective features compared to traditional manufacturing. It aims to provide autonomous manufacturing to small, medium, and large-scale industries with Artificial Intelligence (AI) and Internet of Things technologies. The industrial IoT connects a large number of sensors and actuators, so providing robust security is essential.

6.4 Next Generation IoT

Various initiatives for establishing, defining, and specifying 5 g-enabled IoT are taken. The 5 G enabled technology has addressed major issues of the traditional cellular networks, such as large bandwidth, higher data rate, a better quality of service, massive connectivity, cost efficiency, and more. Some of the examples of such 5 G enabled IoT is International Mobile Technology (IMT) [38], Third Generation Partnership Project (3GPP) [48], and International Telecommunication Union-Radio Communication (ITU-R) 5 G technology [57]. With the advancement in technology comes the challenges of providing basic security without compromising the network.

6.5 Recent Trends in IoT

The concept of ubiquitous learning by [122] evolved the vision of a smart environment. The emerging smart environment is diverse due to its coverage in transportation, healthcare, utilities, homes, etc. The applications like augmented maps, autonomous cars, and mobile ticketing are already in practice. Some of the recent future applications are Robot taxi [109, 128], and remote patient monitoring, smart biosensors, wearable devices, telemedicine, smart ambulance in healthcare [62, 74, 120]. The concept of smart meters and smart grids in the utility sector is also blooming [58, 112].

7 Conclusion

Security is necessary for 6LoWPAN enabled devices as they are always connected and accessible over the un-trusted Internet. When collecting data from multiple fragments, collated, analyzed, ensuring security to IoT devices becomes a significant problem. IoT security protocols are different from traditional security protocols because conventional security protocols need more processing power and are not suitable in battery-operated devices. This paper discusses the recent trends of security schemes for IoT using 6LoWPAN based networks. A recent survey is provided on layered security schemes for the 6LoWPAN protocol stack. Designing lightweight security schemes for IoT by keeping the same security balance as traditional schemes is challenging. The current works are not sufficient for a complete IoT solution to ensure end-to-end security for such a network.

Acknowledgements The authors are thankful to Visvesvaraya Ph.D. Scheme for Electronics & IT(Ref: DIC/MUM/GA/10(43)), Ministry of Electronics & Information Technology (MeitY), Government of India, for their support in this work.

Author Contributions The author Leki Chom Thungon wrote the manuscript under the guidance of the author Md. Iftekhar Hussain. The structure of the review paper was designed with the help of the author Nurzaman Ahmed. The author Debashis De made the necessary corrections and modifications to the paper.

Funding The authors declare that they have no funding associated with the paper.

Data availability We do not analyse or generate any datasets, because our work proceeds within a theoretical approach.

Declaration

Conflict of interest The authors Leki Chom Thungon, Nurzaman Ahmed, Debashis De and Md. Iftekhar Hussain declared that there is no Conflict of interest directly related to the submitted work.

Ethical Approval This article does not contain any study with human participants or animals performed by any of the authors.

References

1. Daimler's car2go: Rent a smart anywhere, anytime. (2012). https://www.autoblog.com/2008/10/21/daimlers-car2go-rent-a-smart-anywhere-anytime, Last Accessed: 27th January, 2022.
2. Smart Santader FP7 project. (2014). "SmartSantanderRA - Santander augmented reality application,". http://www.smartsantander.eu/index.php/blog/item/174- smartsantanderra-santander-augmented-reality-applicationion, Last Accessed: 27th January, 2022.
3. (2016) Microsoft. (2016). HoloLens. https://www.microsoft.com/en-us/hololens, Last Accessed: 27th January, 2022.
4. Apple is ramping up work on AR headset to succeed iPhone. (2017). https://www.bloomberg.com/news/articles/2017-11-08/apple-is-said-to-ramp-up-work-on-augmented-reality-headset, Last Accessed: 27th January, 2022.
5. Holokit. (2017). https://holokit.io/, Last Accessed: 27th January, 2022.
6. Abhinaya, E., & Sudhakar, B. (2021) A secure routing protocol for low power and lossy networks based 6LoWPAN networks to mitigate DIS flooding attacks. *Journal of Ambient Intelligence and Humanized Computing*, 1–12
7. Ahilan, A., Rejula, M. A., Kumar, S., & Kumar, B. M. (2023) Virtual reality sensor based IoT embedded system for stress diagnosis. *IEEE Sensors Journal*.
8. Ahn, S., Gorlatova, M., Naghizadeh, P., Chiang, M., & Mittal, P. (2018). Adaptive fog-based output security for augmented reality. In *Proceedings of the 2018 morning workshop on virtual reality and augmented reality network*, pp. 1–6
9. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of things security: A survey. *Journal of Network and Computer Applications, 88*, 10–28.
10. Alcaraz, C., & Lopez, J. (2010). A security analysis for wireless sensor mesh networks in highly critical systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 40*(4), 419–428.
11. Amaral, J. P., Oliveira, L. M., Rodrigues, J. J., Han, G., & Shu, L. (2014). Policy and network-based intrusion detection system for ipv6-enabled wireless sensor networks. In *IEEE International Conference on Communications (ICC), IEEE*, (pp. 1796–1801).
12. Arteaga-Falconi, J. S., Al Osman, H., & El Saddik, A. (2018). ECG and fingerprint bimodal authentication. *Sustainable Cities and Society, 40*, 274–283.
13. Ashrif, F. F., Sundararajan, E. A., Ahmad, R., Hasan, M. K., & Yadegaridehkordi, E. (2023). Survey on the authentication and key agreement of 6LoWPAN: Open issues and future direction. *Journal of Network and Computer Applications*, 103759

14. Bayou, L., Espes, D., Cuppens-Boulahia, N., & Cuppens, F. (2016) Security analysis of wirelesshart communication scheme. In *International symposium on foundations and practice of security*, (pp 223–238), Springer.
15. Bhale, P., Biswas, S., & Nandi, S. (2024). A hybrid IDS for detection and mitigation of sinkhole attack in 6LoWPAN networks. *International Journal of Information Security, 23*(2), 915–934.
16. Bouaziz, M., & Rachedi, A. (2016). A survey on mobility management protocols in wireless sensor networks based on 6LoWPAN technology. *Computer Communications, 74*, 3–15.
17. Brilli, L., Pecorella, T., Pierucci, L., & Fantacci, R. (2016). A novel 6LoWPAN-ND extension to enhance privacy in IEEE 802.15. 4 networks. In *Global Communications Conference (GLOBECOM), IEEE*, (pp. 1–6).
18. Chawla, D., & Mehra, P. S. (2023). A survey on quantum computing for internet of things security. *Procedia Computer Science, 218*, 2191–2200.
19. Chen, J., Jordan, M. I., & Wainwright, M. J. (2020) Hopskipjumpattack: A query-efficient decision-based attack. In *2020 IEEE symposium on security and privacy (sp), IEEE*, (pp. 1277–1294).
20. Cheng, C., Lu, R., Petzoldt, A., & Takagi, T. (2017). Securing the internet of things in a quantum world. *IEEE Communications Magazine, 55*(2), 116–120.
21. Chom Thungon, L., Ahmed, N., Chandra Sahana, S., & Hussain, M. I. (2021). A lightweight authentication and key exchange mechanism for IPv6 over low-power wireless personal area networks-based internet of things. *Transactions on Emerging Telecommunications Technologies, 32*(5), e4033.
22. Cirani, S., Picone, M., Gonizzi, P., Veltri, L., & Ferrari, G. (2015). IoT-OAS: An Oauth-based authorization service architecture for secure services in IoT scenarios. *IEEE Sensors Journal, 15*(2), 1224–1234.
23. Council, N. (2008). Six technologies with potential impacts on us interests out to 2025. *Disruptive Civil Technologies, 2008*, 31.
24. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2019). LSB: A lightweight scalable blockchain for IoT security and anonymity. *Journal of Parallel and Distributed Computing, 134*, 180–197. https://doi.org/10.1016/j.jpdc.2019.08.005
25. Fedeli, A., Fornari, F., Polini, A., Re, B., Torres, V., & Valderas, P. (2024) FloBP: A model-driven approach for developing and executing IoT-enhanced business processes. *Software and Systems Modeling*, 1–30.
26. Fisher, R., & Hancke, G. (2014). DTLS for lightweight secure data streaming in the internet of things. In *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), IEEE*, (pp. 585–590).
27. Fuentes-Samaniego, R. A., Cavalli, A. R., & Nolazco-Fores, J. A. (2016). An Analysis of secure M2M communication in WSNs using DTLS. In *36th international conference on distributed computing systems workshops (ICDCSW), IEEE*, (pp. 78–83).
28. Glissa, G., & Meddeb, A. (2019). 6LoWPSec: An end-to-end security protocol for 6LoWPAN. *Ad Hoc Networks, 82*, 100–112.
29. Granjal, J., & Monteiro, E. (2016). End-to-end transparent transport-layer security for internet-integrated mobile sensing devices. In *IFIP Networking Conference (IFIP Networking) and Workshops, IEEE*, (pp. 306–314).
30. Hall, R., Rinaldo, A., & Wasserman, L. (2013). Differential privacy for functions and functional data. *Journal of Machine Learning Research, 14*, 703–727.
31. Hammad, M., Luo, G., & Wang, K. (2019). Cancelable biometric authentication system based on ECG. *Multimedia Tools and Applications, 78*(2), 1857–1887.
32. Hammi, M. T., Livolant, E., Bellot, P., Serhrouchni, A., & Minet, P. (2016). MAC sub-layer node authentication in OCARI. In *International conference on performance evaluation and modeling in wired and wireless networks (PEMWN), IEEE*, (pp. 1–6).
33. Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security, 78*, 126–142.
34. Hennebert, C., & Dos Santos, J. (2014). Security protocols and privacy issues into 6LoWPAN Stack: A synthesis. *IEEE Internet of Things Journal, 1*(5), 384–398.
35. Hossain, M., Karim, Y., & Hasan, R. (2018). SecuPAN: A security scheme to mitigate fragmentation-based network attacks in 6LoWPAN. In *Proceedings of the eighth ACM conference on data and application security and privacy, ACM*, (pp. 307–318)
36. Hummen, R., Ziegeldorf, J. H., Shafagh, H., Raza, S., & Wehrle, K. (2013). Towards viable certificate-based authentication for the internet of things. In *2nd ACM workshop on Hot topics on wireless network security and privacy, ACM*, (pp. 37–42).
37. Ingale, M., Cordeiro, R., Thentu, S., Park, Y., & Karimian, N. (2020). Ecg biometric authentication: A comparative analysis. *IEEE Access, 8*, 117853–117866.
38. Jaber, M., Imran, M. A., Tafazolli, R., & Tukmanov, A. (2016). 5G backhaul challenges and emerging research directions: A survey. *IEEE Access, 4*, 1743–1766.

39. Jan, Z., Ahamed, F., Mayer, W., Patel, N., Grossmann, G., Stumptner, M., & Kuusk, A. (2023). Artificial intelligence for industry 4.0: Systematic review of applications, challenges, and opportunities. *Expert Systems with Applications, 216*, 119456.
40. Jara, A. J., Fernandez, D., Lopez, P., Zamora, M. A., & Skarmeta, A. F. (2014). Lightweight MIPv6 with IPSec support. *Mobile Information Systems, 10*(1), 37–77.
41. de Jesus Martins, R., Schaurich, V. G., Knob, L. A. D., Wickboldt, J. A., Schaeffer Filho, A., Granville, L. Z., & Pias, M. (2016). Performance analysis of 6LoWPAN and CoAP for secure communications in smart homes. In *International conference on advanced information networking and applications (AINA), IEEE*, (pp. 1027–1034).
42. Jiang, Q., Zeadally, S., Ma, J., & He, D. (2017). Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. *IEEE Access, 5*, 3376–3392.
43. Jo, Y. H., Jeon, S. Y., Im, J. H., & Lee, M. K. (2016). Security analysis and improvement of fingerprint authentication for smartphones. *Mobile Information Systems, 2016*(1), 8973828.
44. Kambourakis, G., Damopoulos, D., Papamartzivanos, D., & Pavlidakis, E. (2016). Introducing touchstroke: Keystroke-based authentication system for smartphones. *Security and Communication Networks, 9*(6), 542–554.
45. Kempf, J., Nikander, P., & Nordmark, E. (2004). IPv6 neighbor discovery (ND) trust models and threats. *RFC 3756*, https://doi.org/10.17487/rfc3756
46. Kim, E., Kaspar, D., Gomez, C., & Bormann, C. (2012a). Problem statement and requirements for IPv6 over low-power wireless personal area network (6LoWPAN) routing. *RFC 6606*, https://doi.org/10.17487/RFC6606
47. Kim, E., Kaspar, D., & Vasseur, J. (2012b). Design and application spaces for ipv6 over low-power wireless personal area networks (6LoWPANs). *RFC 6568*, https://doi.org/10.17487/rfc6568
48. Kim, J., Kim, D., & Choi, S. (2017). 3GPP SA2 architecture and functions for 5G mobile communication system. *ICT Express, 3*(1), 1–8.
49. Komninos, N., Philippou, E., & Pitsillides, A. (2014). Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys & Tutorials, 16*(4), 1933–1954.
50. Krentz, K. F., & Meinel, C. (2015). Handling reboots and mobility in 802.15. 4 security. In *Proceedings of the annual computer security applications conference, ACM*, (pp. 121–130).
51. Krentz, K. F., Rafiee, H., & Meinel, C. (2013). 6LoWPAN security: Adding compromise resilience to the 802.15. 4 security sublayer. In *Proceedings of the international workshop on adaptive security, ACM*, (pp. 1–10).
52. Kumar, J. S., & Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications, 90*(11).
53. Kwon, G., Kim, J., Noh, J., & Cho, S. (2016). Bluetooth low energy security vulnerability and improvement method. In *Consumer Electronics-Asia (ICCE-Asia), IEEE*, (pp. 1–4).
54. La, V. H., & Cavalli, A. R. (2016). A misbehavior node detection algorithm for 6LoWPAN wireless sensor networks. In *36th international conference on distributed computing systems workshops (ICDCSW), IEEE*, (pp. 49–54).
55. Labati, R. D., Muñoz, E., Piuri, V., Sassi, R., & Scotti, F. (2019). Deep-ECG: Convolutional neural networks for ECG biometric recognition. *Pattern Recognition Letters, 126*, 78–85.
56. Lakkundi, V., & Singh, K. (2014) Lightweight DTLS implementation in CoAP-based internet of things. In *20th annual international conference on advanced computing and communications (ADCOM), IEEE*, (pp. 7–11).
57. Langtry, C. (2016). ITU-R activities on 5G. In *Proceedings of the IEEE world forum internet things*
58. Lloret, J., Tomas, J., Canovas, A., & Parra, L. (2016). An integrated IoT architecture for smart metering. *IEEE Communications Magazine, 54*(12), 50–57.
59. Ma, H., Wang, C., Xu, G., Cao, Q., Xu, G., & Duan, L. (2023). Anonymous authentication protocol based on physical unclonable function and elliptic curve cryptography for smart grid. *IEEE Systems Journal*.
60. Ma, X., & Luo, W. (2008). The analysis of 6LoWPAN technology. In *Pacific-Asia workshop on computational intelligence and industrial application (PACIIA), IEEE*, (pp. 963–966).
61. Malani, S., Srinivas, J., Das, A. K., Srinathan, K., & Jo, M. (2019). Certificate-based anonymous device access control scheme for IoT environment. *IEEE Internet of Things Journal, 6*(6), 9762–9773.
62. Malasinghe, L. P., Ramzan, N., & Dahal, K. (2019). Remote patient monitoring: A comprehensive study. *Journal of Ambient Intelligence and Humanized Computing, 10*(1), 57–76.
63. Mantas, G., Lymberopoulos, D., & Komninos, N. (2009). Integrity mechanism for E-health tele-monitoring system in smart home environment. In *Engineering in medicine and biology society (EMBC), IEEE*, (pp. 3509–3512).

64. Marksteiner, S., Jimenez, V. J. E., Valiant, H., & Zeiner, H. (2017). An overview of wireless IoT protocol security in the smart home domain. In *Internet of things business models, users, and networks, IEEE*, (pp. 1–8).
65. May, M. (2015). Augmented reality in the car industry. https://www.linkedin.com/pulse/augmented-reality-car-industry-melanie-may/, Last Accessed: 27th January, 2022.
66. Mbarek, B., Ge, M., & Pitner, T. (2021). Proactive trust classification for detection of replication attacks in 6LoWPAN-based IoT. *Internet of Things, 16*, 100442.
67. Mendes, Tiago D P., Godina, Radu, Rodrigues, Eduardo M G., Matias, João. C. O., & Catalão, João. P. S. (2015). Smart home communication technologies and applications: Wireless protocol assessment for home area network resources. *Energies, 8*(7), 7279–7311.
68. Migault, D., Palomares, D., Guggemos, T., Wally, A., Laurent, M., & Wary, J. P. (2015). Recommendations for IPsec configuration on homenet and M2M devices. In *11th ACM symposium on QoS and security for wireless and mobile networks, ACM*, (pp. 9–17).
69. Montenegro, G., Hui, J., Culler, D., & Kushalnagar, N. (2007). Transmission of IPv6 packets over IEEE 802.15.4 networks. *RFC 4944*, https://doi.org/10.17487/rfc4944
70. Navas, R. E., Lagos, M., Toutain, L., & Vijayasankar, K. (2016). Nonce-based authenticated key establishment over OAuth 2.0 IoT proof-of-possession architecture. In *3rd world forum on internet of things (WF-IoT), IEEE*, (pp. 317–322).
71. Neuman, B. C., & Ts'o, T. (1994). Kerberos: An authentication service for computer networks. *IEEE Communications magazine, 32*(9), 33–38.
72. Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., & Gomez, C. (2015). IPv6 over BLUETOOTH(R) low energy. *RFC 7668*, https://doi.org/10.17487/RFC7668
73. Nikshepa, V. P., & Shenoy, U. K. K. (2018) 6LowPan-performance analysis on low power networks. In *International conference on computer networks and communication technologies: ICCNCT 2018*, (vol. 15, p. 145), Springer.
74. Nimgampalle, M., Chakravarthy, H., Sharma, S., Shree, S., Bhat, A. R., Pradeepkiran, J. A., & Devanathan, V. (2023). Neurotransmitter systems in the etiology of major neurological disorders: Emerging insights and therapeutic implications. *Ageing Research Reviews*, 101994.
75. Nixon, M., & Round Rock, T. (2012). A Comparison of WirelessHART^{TM} and ISA100. 11a. Whitepaper, Emerson Process Management, (pp. 1–36).
76. Odelu, V., Das, A. K., & Goswami, A. (2015). A secure biometrics-based multi-server authentication protocol using smart cards. *IEEE Transactions on Information Forensics and Security, 10*(9), 1953–1966.
77. Ogonji, M. M., Okeyo, G., & Wafula, J. M. (2020). A survey on privacy and security of Internet of Things. *Computer Science Review, 38*, 100312.
78. Ooko, S. O., Kadam'manja, J., Uwizeye, M. G., & Lemma, D. (2020). Security issues in IPv6 over low-power wireless personal area networks (6LoWPAN): A review. In *2020 21st international arab conference on information technology (ACIT), IEEE*, (pp. 1–5).
79. Park, J., Kwon, H., & Kang, N. (2016). IoT–cloud collaboration to establish a secure connection for lightweight devices. *Wireless Networks*, 1–12.
80. Park, S., Kim, K., Haddad, W., Chakrabarti, S., & Laganier, J. (2011a). IPv6 over low power WPAN security analysis. Technical report, IETF Internet Draft draft-6Iowpan-security-analysis-05, (pp. 1–23).
81. Park, S. D., Kim, K. H., Haddad, W., Chakrabarti, S., & Laganier, J. (2011b). IPv6 over low power WPAN security analysis. Internet-Draft draft-daniel-6lowpan-security-analysis-05, Internet Engineering Task Force, work in Progress.
82. Piro, G., Boggia, G., & Grieco, L. A. (2014). A standard compliant security framework for IEEE 802.15. 4 Networks. In *IEEE world forum on internet of things (WF-IoT), IEEE*, (pp. 27–30).
83. Pohrmen, F. H., Das, R. K., Khongbuh, W., & Saha, G. (2018). Blockchain-based security aspects in internet of things network. In *International conference on advanced informatics for computing research*, (pp. 346–357), Springer.
84. Pokrić, B., Krco, S., & Pokrić, M. (2014). Augmented reality based smart city services using secure iot infrastructure. In *28th international conference on advanced information networking and applications workshops, IEEE*, (pp. 803–808).
85. Pongle, P., & Chavan, G. (2015). A survey: Attacks on RPL and 6LoWPAN in IoT. In *International conference on pervasive computing (ICPC), IEEE*, (pp. 1–6).
86. Punithavathi, P., Geetha, S., Karuppiah, M., Islam, S. H., Hassan, M. M., & Choo, K. K. R. (2019). A lightweight machine learning-based authentication framework for smart IoT devices. *Information Sciences, 484*, 255–268.
87. Puthal, D., Mohanty, S. P., Bhavake, S. A., Morgan, G., & Ranjan, R. (2019). Fog computing security challenges and future directions [energy and security]. *IEEE Consumer Electronics Magazine, 8*(3), 92–96.

88. Qiu, Y., & Ma, M. (2016). A mutual authentication and key establishment scheme for M2M communication in 6LoWPAN networks. *IEEE Transactions on Industrial Informatics, 12*(6), 2074–2085.
89. Qiu, Y., & Ma, M. (2016b). A PMIPv6-based secured mobility scheme for 6LoWPAN. In *Global communications conference (GLOBECOM), IEEE*, (pp. 1–6).
90. Rahman, RA., & Shah, B. (2016). Security analysis of IoT protocols: A focus in CoAP. In *3rd MEC international conference on big data and smart city (ICBDSC), IEEE*, (pp. 1–7).
91. Rajeswari, S. R., & Seenivasagam, V. (2016). Comparative study on various authentication protocols in wireless sensor networks. *The Scientific World Journal*, *2016*.
92. Rao, M., Newe, T., Grout, I., Lewis, E., & Mathur, A. (2015). FPGA based Reconfigurable IPSec AH core suitable for IoT applications. *IEEE international conference on computer and information technology, ubiquitous computing and communications, dependable* (pp. 2212–2216). Autonomic and Secure Computing, Pervasive Intelligence and Computing: IEEE.
93. Raza, S., Shafagh, H., Hewage, K., Hummen, R., & Voigt, T. (2013). Lithe: Lightweight secure CoAP for the internet of things. *IEEE Sensors Journal, 13*(10), 3711–3720.
94. Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the internet of things. *Ad Hoc Networks, 11*(8), 2661–2674.
95. Raza, S., Duquennoy, S., Höglund, J., Roedig, U., & Voigt, T. (2014). Secure communication for the internet of things-a comparison of link-layer security and IPsec for 6LoWPAN. *Security and Communication Networks, 7*(12), 2654–2668.
96. Raza, S., Misra, P., He, Z., & Voigt, T. (2015). Bluetooth smart: An enabling technology for the internet of things. In *Wireless and mobile computing* (pp. 155–162). Networking and Communications (WiMob), IEEE.
97. Razouk, W., Crosby, G. V., & Sekkaki, A. (2014). New security approach for Zigbee Weaknesses. *Procedia Computer Science, 37*, 376–381.
98. Rghioui, A., Bouhorma, M., & Benslimane, A. (2013). Analytical study of security aspects in 6LoWPAN networks. In *5th international conference on information and communication technology for the muslim world (ICT4M), IEEE*, (pp. 1–5).
99. Riaz, R., Kim, K. H., & Ahmed, H. F. (2009). Security analysis survey and framework design for IP connected lowpans. In *International symposium on autonomous decentralized systems, IEEE*, (pp. 1–6).
100. Routray, S. K., Sharmila, K., Javali, A., Ghosh, A. D., & Sarangi, S. (2020). An outlook of narrowband IoT for industry 4.0. In *2020 second international conference on inventive research in computing applications (ICIRCA), IEEE*, (pp. 923–926).
101. Sain, M., Kang, Y. J., & Lee, H. J. (2017). Survey on Security in Internet of things: State of the art and Challenges. In *19th international conference on advanced communication technology (ICACT), IEEE*, (pp. 699–704).
102. Sajjad, S. M., & Yousaf, M. (2014). Security analysis of IEEE 802.15. 4 MAC in the context of internet of things (IoT). In *Information assurance and cyber security (CIACS), IEEE*, (pp. 9–14).
103. Saldamli, G., Ertaul, L., & Kodirangaiah, B. (2018). Post-quantum cryptography on IoT: Merkle's tree authentication. In *Proceedings of the international conference on wireless networks (ICWN), the steering committee of the world congress in computer science, computer*, (pp. 35–41).
104. Salman, T., & Jain, R. (2019). A survey of protocols and standards for internet of things. arXiv preprint arXiv:1903.11549
105. Samuel, S. S. I. (2016). A review of connectivity challenges in IoT-smart home. In *2016 3rd MEC international conference on big data and smart city (ICBDSC), IEEE*, (pp. 1–4).
106. Sanchez, L., Muñoz, L., Galache, J. A., Sotres, P., Santana, J. R., Gutierrez, V., Ramdhany, R., Gluhak, A., Krco, S., Theodoridis, E., et al. (2014). SmartSantander: IoT experimentation over a smart city testbed. *Computer Networks, 61*, 217–238.
107. Sciancalepore, S., Piro, G., Vogli, E., Boggia, G., & Grieco, L. A. (2014). On securing IEEE 802.15. 4 networks through a standard compliant framework. In *Euro Med Telco Conference (EMTC), IEEE*, (pp. 1–6).
108. Sciancalepore, S., Vučinić, M., Piro, G., Boggia, G., & Watteyne, T. (2017). Link-layer security in TSCH networks: Effect on slot duration. *Transactions on Emerging Telecommunications Technologies, 28*(1), 1–14.
109. Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., & Mustaqim, M. (2020). Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. *Ieee Access, 8*, 23022–23040.
110. Shreenivas, D., Raza, S., & Voigt, T. (2017). Intrusion detection in the RPL-connected 6LoWPAN networks. In *3rd ACM international workshop on IoT privacy, trust, and security, ACM*, (pp. 31–38).

111. Singh, M., Rajan, M., Shivraj, V., & Balamuralidhar, P. (2015). Secure Mqtt for internet of things (IoT). In *Fifth international conference on communication systems and network technologies (CSNT), IEEE*, (pp. 746–751).
112. Slanỳ, V., Lučanskỳ, A., Koudelka, P., Mareček, J., Krčálová, E., & Martínek, R. (2020). An integrated IoT architecture for smart metering using next generation sensor for water management based on LoRaWAN technology: a pilot study. *Sensors, 20*(17), 4712.
113. Tabassum, A., Erbad, A., & Guizani, M. (2019). A survey on recent approaches in intrusion detection system in IoTs. In *2019 15th international wireless communications and mobile computing conference (IWCMC), IEEE*, (pp. 1190–1197).
114. Tiloca, M., Gehrmann, C., & Seitz, L. (2016). On improving resistance to denial of service and key provisioning scalability of the DTLS handshake. *International journal of information security*, (pp. 1–21).
115. Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, J. P. & Alexander, R. (2012). RPL: IPv6 routing protocol for low-power and lossy networks. *RFC 6550*, https://doi.org/10.17487/RFC6550
116. Vatambeti, R., Krishna, E. P., Karthik, M. G., & Damera, V. K. (2024). Securing the medical data using enhanced privacy preserving based blockchain technology in Internet of Things. *Cluster Computing, 27*(2), 1625–1637.
117. Vohra, S., & Srivastava, R. (2015). A survey on techniques for securing 6LoWPAN. In *Fifth international conference on communication systems and network technologies (CSNT), IEEE*, (pp. 643–647).
118. Wallgren, L., Raza, S., & Voigt, T. (2013). Routing attacks and countermeasures in the RPL-based internet of things. *International Journal of Distributed Sensor Networks, 9*(8), 1477–1550.
119. Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on blockchain for internet of things. *Computer Communications, 136*, 10–29.
120. WangJulie, B., Cadmus-BertramLisa, A., WhiteMartha, M., NicholsJeanne, F., AyalaGuadalupe, X., & PierceJohn, P., et al. (2015). Wearable sensor/device (Fitbit One) and SMS text-messaging prompts to increase physical activity in overweight and obese adults: A randomized controlled trial. *Telemedicine and e-Health*.
121. Weber, R. H., & Weber, R. (2010). *Internet of things* (Vol. 10). New York: Springer.
122. Weiser, M. (1991). The computer for the 21st century. *Scientific American, 265*(3), 94–105.
123. Wu, L., Du, X., Wang, W., & Lin, B. (2018). An out-of-band authentication scheme for internet of things using blockchain technology. In *International conference on computing* (pp. 769–773). Networking and Communications (ICNC), IEEE.
124. Xiao, Y., Chen, H. H., Sun, B., Wang, R., & Sethi, S. (2006). MAC security and security overhead analysis in the IEEE 802.15. 4 wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking, 2006*(1), 093830.
125. Xiaomei, Y., & Ke, M. (2016). Evolution of wireless sensor network security. In *World automation congress (WAC), IEEE*, (pp. 1–5).
126. Yang, Z., & Chang, C. H. (2019). 6LoWPAN overview and implementations. In *Proceedings of the 2019 international conference on embedded wireless systems and networks*, (pp. 357–361), Junction Publishing.
127. Yeole, A., Kalbande, D., & Sharma, A. (2019). Security of 6LoWPAN IoT networks in hospitals for medical data exchange. *Procedia Computer Science, 152*, 212–221.
128. Zhang, M., Yu, T., & Zhai, G. F. (2011). Smart transport system based on"the internet of things''. *Applied Mechanics and Materials, 48*, 1073–1076. https://doi.org/10.4028/www.scientific.net/AMM.48-49.1073
129. Zhou, L., Wen, Q., & Zhang, H. (2012). Preserving sensor location privacy in internet of things. In *Fourth international conference on computational and information sciences (ICCIS), IEEE*, (pp. 856–859).

Leki Chom Thungon is an Assistant Professor at the School of Computer Science and Engineering, Vellore Institute of Technology Chennai Campus, India. She received her B.E in Computer Science and Engineering from Coimbatore Institute of Technology, India and M.Tech degree in Computer Science and Engineering from North-Eastern Regional Institute of Science and Technology, India and PhD from North-Eastern Hill University (NEHU), India. Her research interest includes Internet-of-Things and Network Security.

Nurzaman Ahmed is a Postdoctoral Scholar at Dartmouth College, USA. Before joining Dartmouth, Dr. Ahmed was a Senior Research Associate at Indian Institute of Technology, Kharagpur, India. He received the B.Tech. and M.Tech. degrees in information technology from North-Eastern Hill University, Shillong, India, in 2013 and 2020. He completed his postdoctoral researcher from Department of Computer Science & Engineering, Indian Institute of Technology, Kharagpur, India. His current research interests include machine-to-machine networks, Internet of Things, and WiFi-based long distance networks. Mr. Ahmed is a student member of the IEEE and Indian Science Congress Association.

Debashis De is Professor with the Department of Computer Science and Engineering, Maulana Abul Kalam Azad University of Technology, West Bengal, and Adjunct Research Fellow with the University of Western Australia. He is the senior member of IEEE and member of International Union of Radio science. He established the Center of Mobile Cloud Computing. He has published more than sixty peer reviewed international journals, fifty conference papers, two research monographs and ten books. Dr. De was the recipient of the Young Scientist Award in 2005 in New Delhi, India, and in 2011 in Istanbul, Turkey, from the International Union of Radio Science, Belgium. His research interest includes location and handoff management, mobile cloud computing, traffic forecasting, green mobile networks and low power Nano device designing for mobile application.

Md. Iftekhar Hussain is an Associate Professor at North-Eastern Hill University (NEHU), India. He received his B.E in Computer Science and Engineering from Dibrugarh University, and M.Tech in Information Technology and Ph.D in Computer Science and Engineering from Tezpur University. He is a member of IEEE and a life member of the Indian Science Congress Association. His research interests include Wireless Mesh Networks and Internet of Things (IoT).