IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 28, 2021, accepted August 5, 2021, date of publication August 9, 2021, date of current version August 19, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3103725

Recent Security Trends in Internet of Things: A Comprehensive Survey

YASMINE HARBI[1], ZIBOUDA ALIOUAT[1], ALLAOUA REFOUFI[1], AND SAAD HAROUS[2], (Senior Member, IEEE)

[1]Faculty of Sciences, Ferhat Abbas University of Setif 1, Setif 19000, Algeria
[2]Department of Computer Science, College of Computing and Informatics, University of Sharjah, Sharjah, United Arab Emirates

Corresponding author: Saad Harous (harous@sharjah.ac.ae)

ABSTRACT The Internet of Things (IoT) aims to transform everyday physical objects into an interconnected ecosystem with digital data accessible anywhere and anytime. ''Things'' in IoT are embedded with sensing, processing, and actuating capabilities and cooperate in providing smart and innovative services autonomously. The rapid spread of IoT services arises different security vulnerabilities that need to be carefully addressed. Several emerging and promising technologies and techniques are introduced to improve the security of IoT. This paper aims to provide an up-to-date vision of the current research topics related to IoT security. Initially, we introduce common elements and protocols of IoT to demystify the origins of threats in IoT. Then, we propose a taxonomy of IoT attacks and analyze the security vulnerabilities of IoT at different layers. Subsequently, we provide a comparison of recent security schemes based on emerging solutions including fog computing, edge computing, software-defined networking (SDN), blockchain, lightweight cryptography, homomorphic and searchable encryption, and machine learning. Finally, security challenges are discussed and future directions are highlighted for future interested researchers.

INDEX TERMS Blockchain, edge computing, fog computing, IoT, lightweight cryptography, machine learning, SDN.

I. INTRODUCTION

The Internet of Things (IoT) refers to a growing network of everyday physical objects connected to the Internet. The ultimate goal of IoT is the transformation of Internet-enabled devices to an interconnected ecosystem with digital data accessible anywhere and anytime.

The IoT devices ranging from small wearable objects to large machines, equipped with sensors and actuators, smartly perceive their surroundings and perform actions autonomously [1], [2]. According to Cisco, 50 billion of devices are currently estimated to be connected to the Internet [3]. These devices are inherently resource-constrained, they have limited memory space, low processing capacity, and computation power.

Different enabling technologies such as cloud computing evolve as essential components for the emergence of IoT paradigm [4], as shown in Figure 1. In near future, the IoT data will be produced from billions of devices using device-to-device (D2D) interactions where devices will be connected to each other and exchange a massive amount of data through the Internet. The number of connected IoT devices is predicted to grow to 1 trillion by 2025. According to this prediction, the IoT will offer potential economic revenue of $11 trillion per year by 2025 [5]. Consequently, this growth will face several security issues that must be addressed.

The security of IoT has attracted significant attention in the academic field. A large number of researchers discussed the security of IoT systems [6]–[20]. Most of the existing surveys investigated relevant security aspects such as attacks, requirements, and challenges in IoT. However, various emerging technologies and techniques have been recently adopted as promising solutions to improve IoT security.

The main goal of this paper is to provide an up-to-date review of the current research topics related to IoT security. Specifically, several security schemes based on different emerging technologies and techniques, namely fog computing, edge computing, SDN, blockchain, lightweight cryptography, homomorphic and searchable encryption, and

The associate editor coordinating the review of this manuscript and approving it for publication was Gautam Srivastava.

machine learning are evaluated. In addition, a comparison of the studied schemes in terms of security and performance is provided. Accordingly, the key contributions of this work are the following.

- Introduce common elements, protocols, and applications of IoT systems.
- Provide a taxonomy of IoT attacks to identify the security vulnerabilities of IoT systems.
- Present emerging solutions that address the IoT security issues and provide a comparison of recent research works based on these solutions.
- Discuss security challenges and future directions for the IoT systems.

Figure 2 shows the organization of the paper. In Section 2, we explore relevant studies that address IoT security. In Section 3, we present three-layered IoT architecture and introduce common elements, protocols, and applications of IoT. The security threats of each layer of IoT are analyzed in Section 4. Emerging security solutions used in IoT are discussed in Section 5. In Section 6, we report the security challenges and highlight future directions for IoT security. We conclude our study and provide future work in Section 7.

II. RELATED SURVEYS

This section explores recent relevant studies that cover different aspects of IoT security. The main security aspects discussed in the reviewed surveys are summarized in Table 1.

Adat and Gupta [6] presented the history, statistics and architecture of IoT. They discussed the security features according to IoT layers and provided a taxonomy of security issues and challenges in IoT systems. Moreover, they analyzed existing defense mechanisms including intrusion detection systems.

Kouicem *et al.* [7] pinpointed the security requirements and challenges in different IoT applications such as smart grids, smart cities, healthcare, transportation, and manufacturing. They classified the security solutions into classical and new approaches. The classical approaches cover confidentiality, privacy, and availability, while new solutions include SDN-based and blockchain-based schemes. The authors also focused on context-awareness and safety related to IoT security.

Lu and Xu [8] discussed the security issues at four-layered IoT architecture and provided a taxonomy of different attacks. They described the security measures for WSNs and RFIDs and classified the security schemes into three categories: host identity protocol-based schemes, datagram transport layer security-based schemes, and capability-based access control schemes.

Noor [9] presented the security attacks and challenges at perception, network, and application layers of IoT. They reviewed a large number of proposed security schemes that address authentication, encryption, trust management, and secure routing. The authors also highlighted the simulation tools involved in the reviewed schemes.

Tewari and Gupta [10] addressed the security issues of three-layered IoT architecture. They described the security designs of IoT protocols and discussed the security challenges of enabling technologies such as cloud and RFID. Moreover, the authors presented key factors that must be achieved to provide a trustworthy IoT network and highlighted the impact of IoT in different fields.

Harbi *et al.* [11] analyzed several security attacks that may be launched in IoT systems. They provided a taxonomy of security requirements including data security, communication security, and device security. Furthermore, the authors described many security schemes proposed for various IoT applications and pinpointed major security challenges.

Hassija *et al.* [12] discussed the security issues of various IoT applications and highlighted possible attacks on IoT layers. They reviewed proposed solutions based on blockchain, fog computing, edge computing, and machine learning to secure IoT environments.

Meneghello *et al.* [13] classified the security requirements for IoT into three levels, namely information level, access level, and functional level. They reported the vulnerabilities and possible attacks at different IoT layers. They presented the security mechanisms designed to satisfy security in IoT and focused on security designs of popular IoT communication protocols.

Neshenko *et al.* [14] focused on IoT vulnerabilities in the context of various dimensions. They provided a comprehensive taxonomy of IoT vulnerabilities including layers (security of each IoT layer), attacks (performed on exploited vulnerabilities), countermeasures (available techniques to mitigate vulnerabilities), security impact (impact of vulnerabilities on security requirements), and situational awareness capabilities (available techniques to capture malicious activities).

Hamad *et al.* [15] discussed common security attacks that target IoT systems. They identified the security requirements to overcome such attacks in different IoT applications. They reviewed proposed schemes that address security services such as access control, integrity, authentication, confidentiality, and privacy.

Mahbub [16] identified the security concerns of various IoT applications. They introduced threat modeling frameworks that can be used in the security designing of IoT systems. They reported the security attacks at sensing, network, middleware, and application layers. Moreover, the authors presented security techniques using cryptography, fog computing, edge computing, and machine learning to solve IoT attacks.

Mrabet *et al.* [17] proposed new IoT architecture that includes five layers; perception, network, transport, application, and cloud layer. They analyzed the security threats at different IoT architectural layers and discussed open challenges to secure IoT systems.

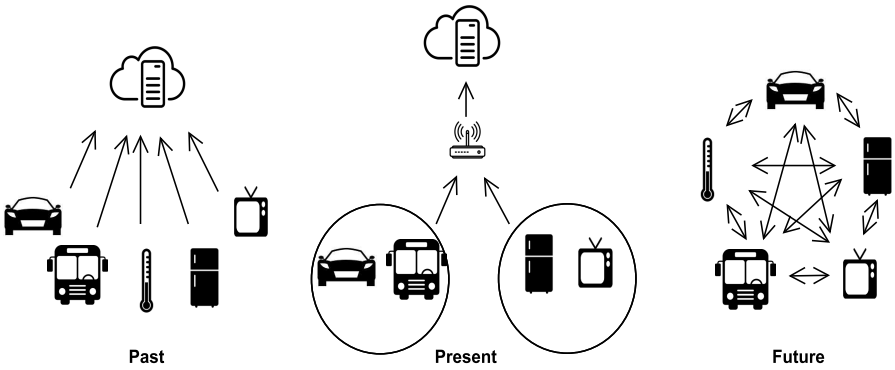


FIGURE 1. Evolution of IoT.

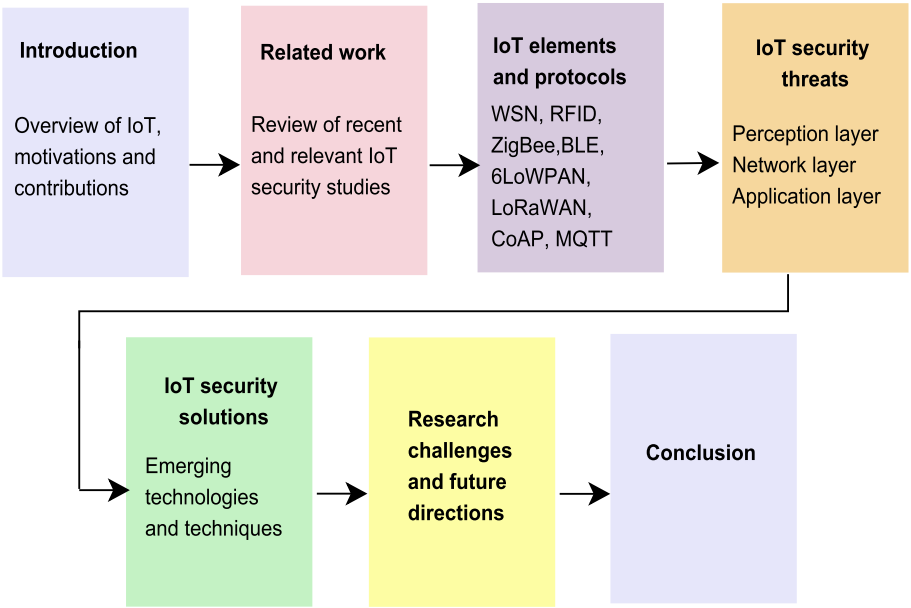


FIGURE 2. Organization of the paper.

Malhotra *et al.* [18] presented a taxonomy of IoT security attacks, anomalies, and vulnerabilities. They focused on learning-based techniques to provide intelligent intrusion detection IoT systems. In addition, the authors highlighted critical issues that need to be addressed to secure IoT environments.

Thakor *et al.* [19] focused on evaluating lightweight cryptographic algorithms for constrained IoT devices. They classified the lightweight cryptographic algorithms into two main classes; symmetric and asymmetric, and analyzed the hardware and software performance metrics of symmetric lightweight cryptographic algorithms. Furthermore, they discussed several challenges to provide a trade-off between cost, performance, and security.

Jayalaxmi *et al.* [20] explored the security issues and attacks at different layers of industrial IoT (IIoT). They presented several frameworks that provide various security requirements for smart factory systems. Moreover, they investigated intrusion detection techniques proposed for IIoT devices.

Table 2 presents the contributions of the aforementioned studies and our survey. According to Table 2, the state-of-the-art surveys covered several research topics in IoT. However, our survey extends the previous researches by introducing emerging solutions that promise to enhance the IoT security. In addition, it provides an objective comparison of recent security schemes based on the emerging solutions by considering relevant key parameters.

III. OVERVIEW OF IOT

This section provides a brief overview of IoT systems. It aims to present characteristics of IoT elements, protocols, and applications to understand the origins of security risks and set a common ground for the security threats that will be discussed in the next section.

TABLE 1. Summary of related surveys.

Related survey	Year	IoT layers	Security aspects
Adat *et al.* [6]	2017	Perceptual, network, support, application	Security features of each IoT layer Security issues and challenges IoT intrusion detection systems
Kouicem *et al.* [7]	2018	-	Security requirements and challenges
Lu *et al.* [8]	2018	Sensing, network, middleware, application	Security issues of each IoT layer
Noor *et al.* [9]	2018	Perception, network, application	Security attacks and challenges IoT security schemes
Tewari *et al.* [10]	2018	Perception, middleware, application	Security issues of each IoT layer Security designs of IoT protocols Security issues of IoT enabling technologies
Harbi *et al.* [11]	2019	Perception, network, application	Security attacks and requirements Security solutions and challenges
Hassija *et al.* [12]	2019	Sensing, network, middleware, application	Security issues of IoT applications Security attacks of IoT layers Security solutions and challenges
Meneghello *et al.* [13]	2019	Edge, access, application	Taxonomy of security requirements and attacks Security mechanisms and threats of IoT protocols
Neshenko *et al.* [14]	2019	Devices, network subsystems, application	IoT vulnerabilities in context of various domains
Hamad *et al.* [15]	2020	Physical, information, application	Security attacks and requirements Security solutions and open issues
Mahbub [16]	2020	Sensing, network, middleware, application	Security concerns of IoT applications Threat modelling frameworks Security attacks at IoT layers Security techniques and challenges
Mrabet *et al.* [17]	2020	Perception, network, transport, application, cloud	Security threats and solutions Open issues and challenges
Malhotra *et al.* [18]	2021	Perception, network, support, application	Taxonomy of attacks, anomalies, and vulnerabilities Open issues and challenges
Thakor *et al.* [19]	2021	-	Lightweight cryptographic algorithms Security challenges
Jayalaxmi *et al.* [20]	2021	Perception, network, support, application	Security attacks and requirements Intrusion detection techniques

- : not discussed

TABLE 2. Contributions of related surveys and our survey.

Contribution	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]
IoT architecture	✓	×	✓	✓	✓	×	✓	✓
IoT applications	×	✓	✓	×	✓	×	✓	×
IoT protocols	✓	×	×	×	✓	×	×	✓
IoT attacks	✓	×	✓	✓	✓	✓	✓	✓
Security requirements	✓	✓	✓	✓	✓	✓	×	✓
Fog computing	×	×	×	×	×	×	✓	×
Edge computing	×	×	×	×	×	×	✓	×
SDN	×	✓	×	✓	×	×	×	×
Blockchain	×	✓	×	✓	×	×	✓	×
Lightweight cryptography	×	×	×	×	×	×	×	✓
Homomorphic encryption	×	×	×	×	×	×	×	×
Searchable encryption	×	×	×	×	×	×	×	×
Machine learning	×	×	×	×	×	×	✓	×
Challenges and future directions	✓	✓	✓	×	✓	✓	✓	✓

A. IOT ARCHITECTURE

The architecture of IoT is not standardized; typical IoT architecture has three layers: perception, network, and application [21], as shown in Figure 3.

1) PERCEPTION LAYER

The perception layer includes different physical IoT devices; it is responsible for interaction among devices and collection of IoT data. Data collection is performed using smart devices such as radio frequency identification (RFID) tags and sensors.

RFID technology is a major element of IoT due to its identification, tracking, and monitoring of objects [22]. An RFID system consists of a radio signal transponder (tag) that stores a unique identity of an object and a tag reader that identifies the object through radio waves. The tag reader transfers the identification number to a computer to track and monitor the object as shown in Figure 4.

Wireless sensors play an essential role in IoT by providing sensing and communicating services [23]. A Wireless sensor network (WSN) consists of a large number of intelligent sensors deployed in remote environments to sense and collect

TABLE 3. Cont.

Contribution	[14]	[15]	[16]	[17]	[18]	[19]	[20]	Our survey
IoT architecture	✓	✓	✓	✓	✓	×	✓	✓
IoT applications	×	✓	✓	×	×	×	×	✓
IoT protocols	✓	✓	✓	✓	×	×	×	✓
IoT attacks	✓	✓	✓	✓	✓	✓	×	✓
Security requirements	×	✓	×	✓	×	×	✓	✓
Fog computing	×	×	✓	×	×	×	×	✓
Edge computing	×	×	✓	×	×	×	×	✓
SDN	×	×	×	×	×	×	×	✓
Blockchain	×	✓	×	×	×	×	✓	✓
Lightweight cryptography	×	×	✓	×	×	✓	×	✓
Homomorphic encryption	×	✓	×	×	×	×	×	✓
Searchable encryption	×	×	×	×	×	×	×	✓
Machine learning	×	×	✓	✓	✓	×	✓	✓
Challenges and future directions	✓	✓	✓	✓	✓	✓	✓	✓

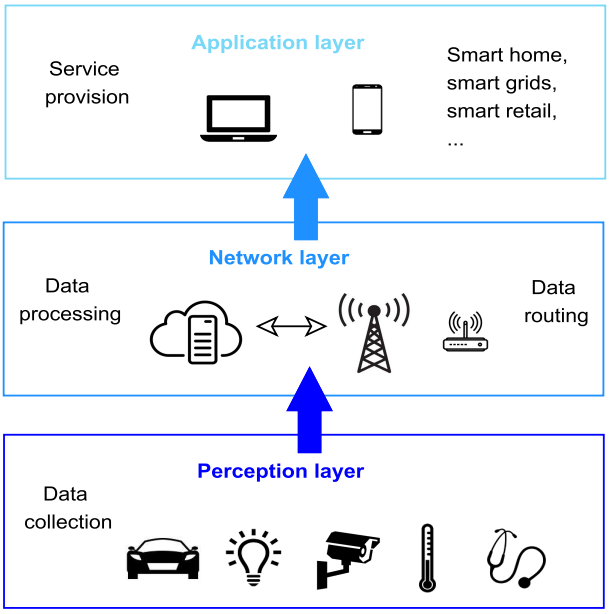


FIGURE 3. Three-layered IoT architecture.

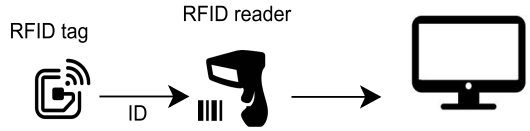


FIGURE 4. RFID system.

data such as temperature, humidity, vibration, etc. Sensed data are transmitted through one or multi-hop to a gateway/base station as depicted in Figure 5.

2) NETWORK LAYER

The network layer processes the collected data provided by the perception layer and stores or sends the data to the application layer. It is the most important layer of IoT architecture because it integrates various communication technologies that enable the connectivity of IoT devices. The widely used

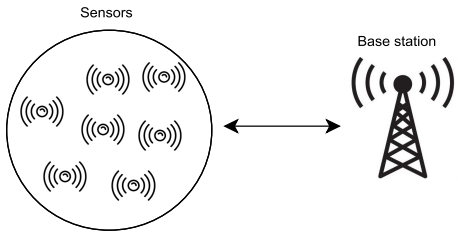


FIGURE 5. WSN architecture.

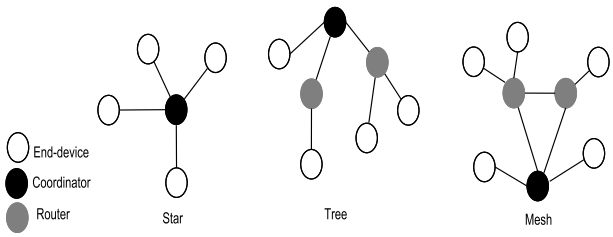


FIGURE 6. ZigBee topologies.

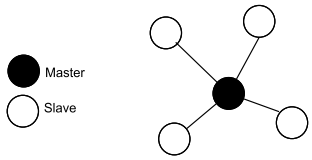


FIGURE 7. BLE topology.

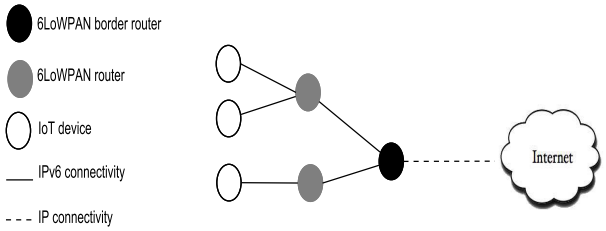


FIGURE 8. 6LoWPAN architecture.

communication technologies include ZigBee, Bluetooth low energy (BLE), IPv6 over low power wireless personal area networks (6LoWPAN), and long-range wide area network (LoRaWAN).

ZigBee is a wireless communication technology designed for short-range communications [24]. It can be used in smart homes, smart meters, and smart healthcare. The ZigBee protocol stack includes physical (PHY) and medium access control (MAC) layers based on IEEE 802.15.4 standard [25], a network (NWK) layer, and an application (APP) layer. A ZigBee network can have a star, tree, or mesh topology and each network has a coordinator node (trusted node) that manages the network and maintains security between devices. In a star network, end-devices are directly connected to the coordinator while in tree or mesh networks, intermediate routers are used to extend the network, as shown in Figure 6. The NWK layer provides data routing using cluster-tree and modified ad hoc on-demand distance vector (AODV) algorithms [26]. A ZigBee device can only communicate with another ZigBee device, and thus, it has limited interoperability.

BLE is a short-range communication technology that reduces energy consumption compared to classic Bluetooth [27]. It is widely used in IoT vehicular systems. BLE has a protocol stack composed of PHY layer, MAC layer, logical link control and adaptation protocol (L2CAP), and attribute protocol (ATT). The BLE adopts a star topology including master and slave devices as demonstrated in Figure 7. Each slave node is associated with a single master node. The master node is responsible to initiate the communication and provide the scheduling table according to time division multiple access (TDMA).

6LoWPAN combines the latest version of Internet protocol (IPv6) and low power wireless personal area network (LoWPAN) [28]. It enables IoT devices with limited capabilities to transmit data through wireless channels using IPv6. It is suitable for resource-constrained devices because it reduces transmission cost, supports mobility, etc. The most common use cases of 6LoWPAN are smart home, smart agriculture, and industrial IoT. Compared to ZigBee, a 6LoWPAN device can communicate with another 6LoWPAN device or IEEE 802.15.4 device. It can also communicate with an IP-based network such as Wi-Fi as presented in Figure 8. The specification of 6LoWPAN defines a complete protocol stack that consists of PHY and MAC layers based on IEEE 802.15.4 standard, the NWK layer, the transport layer, and APP layer [29]. The routing within the 6LoWPAN network uses routing protocol for low-power and lossy networks (RPL) [30]. RPL supports point-to-point, point-to-multipoint, and multipoint-to-point communications. It is based on the direct acyclic graph (DAG). From DAG, RPL creates a destination-oriented direct acyclic graph (DODAG) tree that contains one root from the leaf node to the root.

LoRaWAN is a long-range communication protocol designed for low-power and scalable IoT applications [31]. As depicted in Figure 9, a LoRaWAN network consists of end-devices, gateways, and a single server in a star or star-of-star topology. The end devices can communicate to one or more gateways using the ALOHA scheme through one-hop links. The gateways are connected to the network server via Internet protocol. The communications are bidirectional and initiated by the end device.

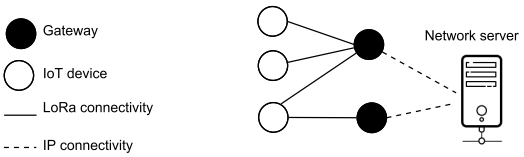


FIGURE 9. LoRaWAN architecture (star-of-star topology).

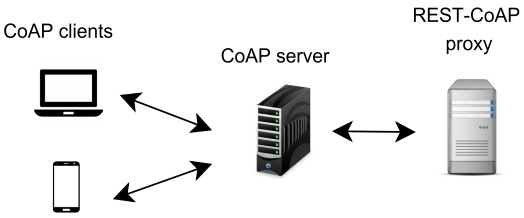


FIGURE 10. CoAP architecture.

Table 4 provides a comparison of the studied IoT wireless technologies. This comparison helps to select the suitable protocol for a defined IoT system.

3) APPLICATION LAYER

The application layer receives the data from the network layer and provides the required services to IoT users. It supports a large variety of applications such as smart home, smart retail, smart grids, etc. The most common application protocols are constrained application protocol (CoAP) and message queuing telemetry transport (MQTT).

Since IoT devices are resource-constrained, HTTP protocol is not suitable for low-power devices due to its complexity. CoAP was designed to include features of HTTP dedicated to IoT devices. As demonstrated in Figure 10, CoAP is a messaging protocol based on representational state transfer (REST) architecture [32]. It has four message types: confirmable, non-confirmable, acknowledgment and reset. It provides features that are not available on HTTP such as push notification (i.e., the server sends a notification to the device) and resource discovery (i.e., the server can store the list of devices).

MQTT is a lightweight messaging protocol that provides the connectivity of networks and users with applications. It is based on publish/subscribe architecture where the system consists of three main components: publishers, subscribers, and a broker as presented in Figure 11. In the context of IoT, publishers are embedded devices that send data to the broker and subscribers are applications servers.

A comparison of IoT application layer protocols is provided in Table 5.

B. IOT APPLICATIONS

The IoT provides a large number of applications to enhance people's daily lives and activities. Figure 12 shows potential examples of IoT applications.

TABLE 4. Comparison of IoT wireless technologies.

Wireless technology	ZigBee	BLE	6LoWPAN	LoRaWAN
Topology	star, tree, mesh	Star	Star, mesh	star, star-of-star
Range	10-20m	<100m	10-20m	3-5km
Application	smart home smart meters smart healthcare	smart vehicule	smart home smart agriculture smart industry	smart city
Interoperability	No	No	Yes	Yes
Security	Yes	Yes	No	Yes
Scalability	Yes	No	Yes	Yes

TABLE 5. Comparison of IoT application protocols.

Application protocol	CoAP	MQTT
Transport layer	UDP	TCP
REST	Yes	No
Request/response	Yes	No
Publish/Subscribe	Yes	Yes
Security	DTLS	SSL

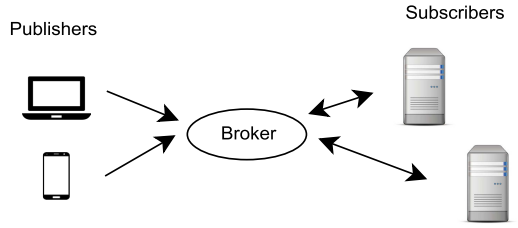


FIGURE 11. MQTT architecture.

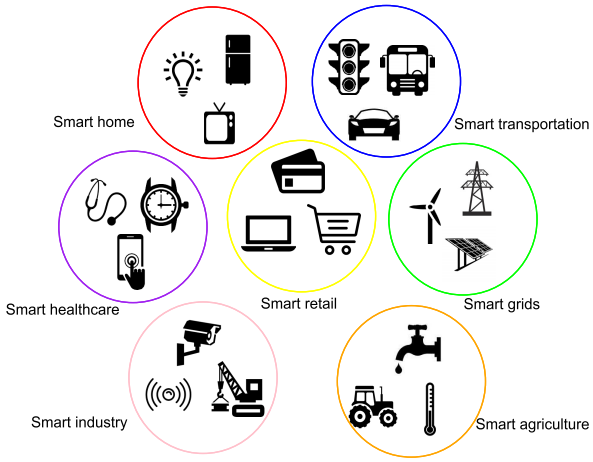


FIGURE 12. IoT applications.

1) SMART HOME

Encompasses a collection of smart devices (e.g., smart lock, baby monitor, fire detector) deployed at home and locally communicate over wireless channels. Home devices can be remotely accessed through a home gateway.

2) SMART HEALTHCARE

Enables collection, transmission, and storage of patients' physiological information. For instance, a patient's heart rate can be collected by medical sensors and transmitted to a hospital server for diagnosis and tracking purposes.

3) SMART TRANSPORTATION

Includes a large number of smart vehicles which can communicate with each other (vehicle-to-vehicle), to the outside station (vehicle-to-infrastructure), and to pedestrians (vehicle-to-pedestrian) over wireless networks. A smart vehicle can detect current traffic status, manage speed, and exchange data to provide efficient and safe driving.

4) SMART AGRICULTURE

Allows remote control of temperature, humidity, irrigation, soil moisture, and micro-climate conditions to provide high production/quality and prevent financial losses. In an intelligent farming system, sensors can be attached to animals to track livestock behaviors and health conditions.

5) SMART INDUSTRY

Known as industrial IoT (IIoT) uses machine-to-machine technology to automate the process of manufacturing with insignificant human intervention. The IIoT aims to better control the production process, data, and issues to provide efficient and reliable final products.

6) SMART RETAIL

Permits the tracking of products in warehouses or during traveling. Sensors can be attached to a retail item to track the product status. Various smart shopping systems were developed to provide intelligent services for customers and thus gain more clients.

7) SMART GRID

Is a common application of IoT that measures, monitors, and manages electricity consumption. It enables efficient and reliable electricity management, provides energy-saving, and reduces powers grids issues/failures.

C. LESSONS LEARNED

IoT systems are empowered with diverse elements and protocols which allow to continually expand possible attacks and introduce several vulnerabilities. IoT integrates the Internet with the physical world to provide various intelligent applications, from smart homes to smart grids. Consequently, the IoT devices can be targeted by adversaries to launch potential attacks. Therefore, it is very necessary to analyze the attack surfaces of IoT systems to satisfy the desired level of security.

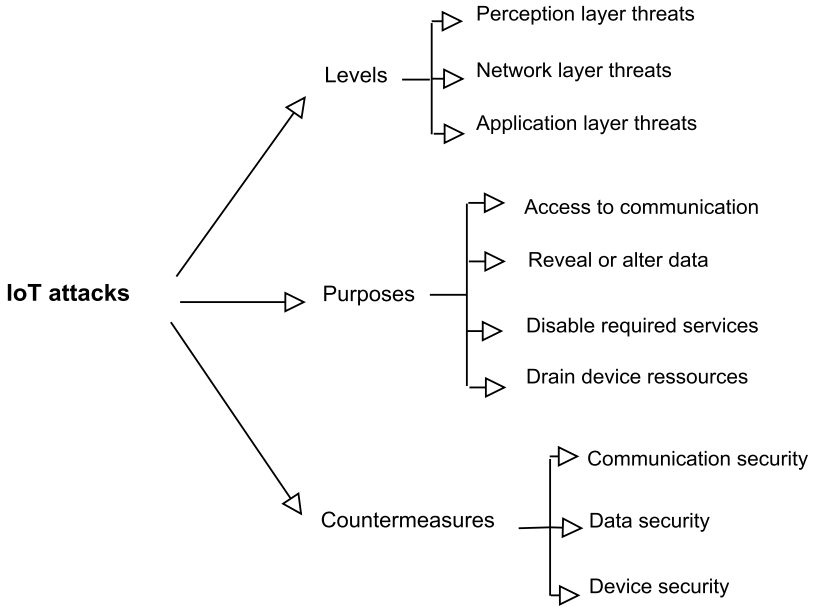


FIGURE 13. Taxonomy of IoT attacks.

IV. SECURITY THREATS OF IOT

In this section, we provide a taxonomy of IoT attacks based on levels, purposes, and countermeasures as shown in Figure 13. Then, we focus on the security vulnerabilities of IoT at the three layers.

Levels: Examine the security issues of IoT at the three layers. Perception layer threats address the security attacks within major elements of IoT such as WSNs and RFID. Network layer threats analyze vulnerabilities of the aforementioned communication protocols. Application layer threats include attacks related to IoT software and end-user devices.

Purposes: Evaluate the impacts of security attacks on IoT systems. The main purposes of IoT attacks are the following:

- Access to communication.
- Reveal or alter data.
- Disable required services.
- Drain device resources.

Countermeasures: Consist of the security requirements to mitigate the identified purposes of IoT attacks. This class includes communication security, data security, and device security. IoT communications can be secured by providing authentication, access control, and non-repudiation. To protect data, relevant security requirements such as confidentiality, privacy, and integrity must be considered. Other fundamental requirements including trust and availability of IoT devices are needed in different environments. For more details about these security requirements, the reader is referred to our previous survey [11].

A. PERCEPTION LAYER THREATS

The limited resources and heterogeneous nature of IoT devices make them vulnerable to various security attacks.

WSNs are generally deployed in harsh and unattended environments, and thus, they are prone to several attacks. Common security attacks of WSNs are sinkhole, blackhole, wormhole, sybil, denial of service (DoS), node capture, and node injection attack [11]. Brief descriptions of these security attacks are provided in Table 6.

Similar to the WSN, the RFID networks are susceptible to different types of attacks including spoofing, cloning, and sniffing attacks (See Table 6).

The IoT inherits the security threats of WSNs and RFID because they are vital elements of IoT networks.

B. NETWORK LAYER THREATS

ZigBee protocol implements security mechanisms including advanced encryption standards with cipher block chaining message authentication code (AES-CCM) and message integrity code (MIC) to provide confidentiality, authentication, and integrity. The ZigBee security is based on three keys: a link key (for unicast communications), a network key (for broadcast communications), and a master key (for link key and network key generation). As mentioned in [33], the master key is installed in the device during the manufacturing process. The link key can be generated using key transport or key establishment methods, while the network key can be acquired using the key transport method.

As the master key is stored on the device, an attacker can read it from the memory after the node capture attack's success. Another possible attack presented in [34] that aims to drain the energy of ZigBee nodes. The authors in [35] evaluated the vulnerability of the ZigBee network against sinkhole attack. In [36], the authors showed that three ZigBee-based smart light systems are susceptible to several types of attacks

such as denial of service (DoS), network key extraction, and code injection attacks.

BLE protocol provides confidentiality and authentication using the 128-bits AES-CCM algorithm as ZigBee. The symmetric key is generated using the pairing procedure. First, the IoT devices exchange necessary information for authentication. Second, they generate and exchange temporary keys based on a pairing method. Finally, the device may exchange and store common keys to be used for further communications.

The pairing methods have several security issues including eavesdropping, man-in-the-middle (MTM), and brute force attacks as presented in [37] and [38]. Latter, a new pairing procedure has been designed based on elliptic curve diffie hellman (ECDH). However, the authors in [39], [40] demonstrated that it has similar problems. In [41], the authors presented other types of attack such as data leakage and DoS attack that can be performed in a BLE-based smart door lock system.

6LoWPAN protocol enables resource-constrained devices to connect to the Internet using IPv6 addresses. It uses IPv6 header compression and packet fragmentation to reduce transmission overhead. However, it does not provide confidentiality, authentication, or integrity preservation. An adversary can inject fake fragments with the header of a legitimate fragment; the receiver node uses the injected fragment in packet reassembly causing the construction of a corrupted packet. Consequently, the buffer space of the receiver node will be reserved and not be able to receive further fragments [42]. Consecutive repetitions of fragment injection attack lead to a DoS attack [43].

RPL defines three security modes: unsecured, preinstalled, and authenticated in the packet header. The unsecured mode is adopted when security is provided by the MAC layer. In preinstalled mode, preinstalled keys are used to join the RPL network. The authenticated mode is not fully defined by the specification of RPL. If security is not provided at any layer, an attacker can perform different types of attacks in the RPL network. A sinkhole, blackhole, flooding, Sybil, and DoS attacks against RPL networks are presented in [43]–[45].

The security of 6LoWPAN relies on securing communications at the MAC layer or APP layer. The security of the MAC layer is provided using AES-CCM and MIC. However, the specification of IEEE 802.15.4 does not define the key management procedure.

LoRaWAN protocol adopts 128-bits AES algorithm and MIC to guarantee data confidentiality and integrity. When an IoT device is allowed to join the LoRaWAN network, the network server sends two session keys, namely network session key and application session key, to the end device. These keys are used for data encryption/decryption and MIC. The main security weakness of the LoRaWAN protocol is related to key management; an intruder can access session keys using a side channels attack since they are stored on the end device. Moreover, the end devices share the same session keys to secure multicast communications. This enables the intruder to read the keys from one node and thus reveal communications of other devices [46]. The authors in [47] demonstrated that the LoRaWAN network is vulnerable to DoS and MTM attacks.

Table 7 summarizes the security threats of IoT communication protocols.

C. APPLICATION LAYER THREATS

CoAP is the application layer protocol that enables resource-constrained devices to achieve RESTful interactions. Since CoAP is built on UDP transport protocol, datagram TLS (DTLS) was proposed to provide confidentiality, authentication, and integrity preservation in CoAP protocol [48]. However, the limitations of DTLS can be considered as security threats of CoAP protocol [49].

Secure socket layer (SSL) was introduced to secure data transfer using the MQTT protocol. SSL uses an asymmetric cryptographic technique to encrypt/decrypt the data. However, it is stills prone to MTM attack [50]. An extension of MQTT called secure MQTT (SMQTT) was proposed to provide security during data transfer [51]. The publishers and subscribers register to the broker and get a secret key. This key is used for data encryption and decryption performed by publishers and subscribers, respectively. However, the key generation and encryption algorithms are not standardized.

In IoT, software vulnerabilities and users devices can be exploited by attackers. An adversary can impersonate or manipulate legal users to gain access to IoT systems by injecting malicious software. The lack of user authentication has led to several IoT attacks such as Bashlite and Mirai attacks [52].

D. LESSONS LEARNED

IoT devices are inherently resource-constrained and generally deployed in unattended environments. In addition, they usually communicate with each other through wireless channels. Consequently, an intruder can remotely control the interconnected objects or intercept private information from the communications. Therefore, there is a need to explore the security vulnerabilities of IoT systems to increase awareness about the consequences of potential threats and possible attacks.

V. EMERGING SECURITY SOLUTIONS

In this section, we discuss the emerging computing technologies and techniques proposed in the literature to increase the level of security in IoT. We also provide a comparison of recent research works based on these technologies and techniques in terms of attack level (i.e., IoT layer targeted by the adversary), countermeasures (i.e., data security, communication security, and device security), and performance (i.e., computation cost, communication cost, and storage cost). The selected comparison parameters are usually considered to design security mechanisms suitable for IoT systems. A summary of the proposed security schemes for IoT is provided in Table 8.

TABLE 6. Description of security attacks.

Security attack	Description
Sinkhole attack	Claim significant resources
Black hole attack	Send replay messages to source node
Wormhole attack	Create fake tunnel between two malicious nodes
Sybil attack	Pretend the identities of IoT devices
DoS attack	Send a large number of packets to target node
Node capture attack	Capture node from the network
Node injection attack	Deploy malicious nodes in the network
RFID spoofing attack	Imitate valid RFID tag information
RFID cloning attack	Clone valid RFID tag information
RFID sniffing attack	Intercept data transfer in RFID network
MTM attack	Intercept and modify the communication between two parties
Code/fragment injection	Inject malicious code/fake fragment in the network
Eavesdropping attack	Intercept secretly the communications
Brute force attack	Try many keys to guess the correct one
Encryption key attack	Extract the key used for data encryption

TABLE 7. Security threats of IoT communication technologies.

Wireless technology	Security attacks
ZigBee	Encryption key, sinkhole, DoS, code injection
BLE	Eavesdropping, MTM, DoS, brute force
6LoWPAN	Fragment injection, sinkhole, blackhole, sybil, DoS
LoRaWAN	Encryption key, DoS, MTM

TABLE 8. Summary of research works based on emerging technologies.

Security schemes	References
Fog computing-based schemes	[53]–[61]
Edge computing-based schemes	[62]–[66]
SDN-based schemes	[67]–[72]
Blockchain-based schemes	[73]–[80]
Lightweight cryptography-based schemes	[81]–[94]
Homomorphic encryption-based schemes	[95]–[97]
Searchable encryption-based schemes	[98]–[101]
Machine learning-based schemes	[102]–[107]

A. FOG COMPUTING-BASED SOLUTIONS

Fog computing has been introduced as a new paradigm to extend (not to replace) the computational resources of Cloud computing. It provides storage, computation, and networking/communication at the edge of the network [108].

Fog computing architecture consists of fog nodes deployed close to IoT devices and connected to the cloud server as shown in Figure 14. The fog architecture helps to reduce the amount of data exchanged between the IoT devices and the cloud infrastructure.

Fog computing supports mobility, location awareness, low latency, heterogeneity, scalability and thus can be perfectly adopted into real-time or latency-sensitive IoT applications.

Since IoT devices have limited resources, fog nodes can provide various security requirements to secure IoT environments. To achieve authentication, Alrawais *et al.* [53] focused on securing communications in fog-assisted IoT environments using ciphertext-policy attribute-based encryption (CP-ABE). They analyzed the security of the proposed scheme against different attacks and provided a comparison with a certificate-based method. Gope [54], the authors proposed three lightweight authentication schemes for device-to-device communications that can be used in various IoT applications. The proposed schemes ensure mutual authentication and key agreement and they are efficient in terms of computation cost.

To ensure privacy-preserving, Hu *et al.* [55] presented a face identification and resolution framework based on fog computing for IoT. The framework is mainly comprised of user devices, fog nodes, and cloud servers. The authors adopted several cryptographic techniques to preserve the personal information of users. Lu *et al.* [56] addressed privacy-preserving of data aggregation in heterogeneous IoT environments. The aggregated data is filtered by fog nodes, and thus the scheme can resist false data injection attack. Moreover, the proposed scheme can also resist differential attacks. Yang *et al.* [57] proposed privacy-preserving scheme for IoT location-awareness applications. The authors used bilinear pairing and asymmetric scalar-product preserving encryption to secure the location of mobile devices. Guan *et al.* [58] employed pseudonym certificates to preserve the privacy of sensitive data during data aggregation in fog-enhanced IoT systems. The data aggregation is performed by fog nodes, while the pseudonym certificates are generated and updated by two certification authorities. The authors evaluated the proposed scheme in terms of computation complexity and communication overhead.

To guarantee confidentiality, Boakye-Boateng *et al.* [59] adopted one-time pad (OTP) and random number generators (RNG) to encrypt the collected data in WSN in the context of IoT. The security of OTP is based on the strength of RNG. The proposed scheme is computationally efficient because it requires lightweight operations to perform the data encryption. In [109], the authors enhanced the security of medical data in healthcare IoT applications using fog

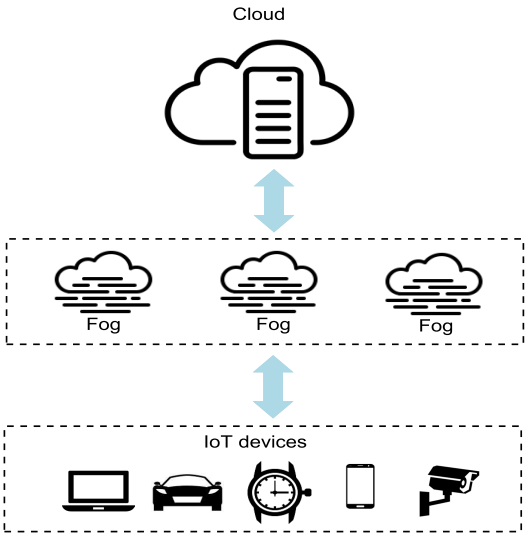


FIGURE 14. Fog computing architecture.

computing. The proposed architecture allows patients' data to be analyzed and secured by fog-based gateways, it also supports the MQTT protocol and M2M communications. The authors provided a comparison to cloud-based architecture to highlight the benefits of fog computing. However, they did not define the encryption technique used for medical data security. Zhang [60] proposed a key management scheme based on contributory broadcast encryption where fog nodes negotiate a public key with an end-user device. This latter sends an encrypted session key to the fog nodes to achieve confidentiality of further communications. The authors in [61] investigated the IoT data encryption using the CP-ABE technique that involves four algorithms, namely, setup, key generation, encryption, and decryption. They defined a formal security model using game theory and analyzed their proposed scheme based on this model.

Table 9 compares the IoT security schemes based on fog computing. It is observed that fog computing can improve the security of IoT systems at perception and network layers. The fog-based security schemes satisfy major requirements such as authentication (i.e., communication security), privacy, and confidentiality (i.e., data security). Moreover, they have acceptable computation cost and communication overhead. However, most of the surveyed articles did not consider the storage cost which is an important parameter for resource-constrained IoT devices.

B. EDGE COMPUTING-BASED SOLUTIONS

Edge computing is another extension of Cloud computing that provides promising services to edge IoT devices including sensors, actuators, and RFID tags. Both fog computing and edge computing offer the same functionalities to carry out computation tasks closer to IoT devices. The main difference between cloud, fog, and edge computing is the location of computational resources [110].

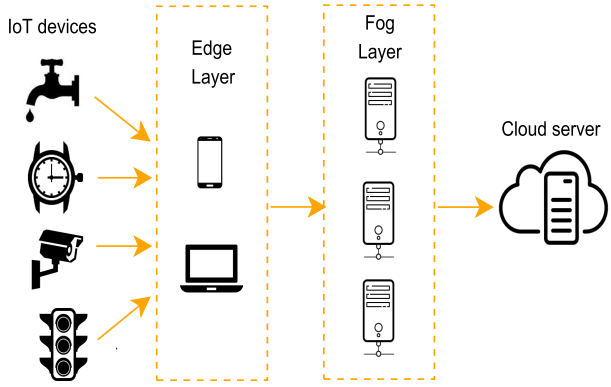


FIGURE 15. Edge computing architecture.

Edge computing architecture consists of smart IoT devices, edge devices, fog nodes, and cloud server as presented in Figure 15. In an edge-enabled IoT application, the data is processed within the device itself without being transferred to fog nodes or cloud server [111]. This enhances the performance of the network in terms of communication overhead, decreases the latency of data processing, and improves the security of the IoT application.

Mobile edge computing (MEC) is a type of edge computing that extends the capabilities of cloud computing to deploy processing and storage services close to IoT mobile users [112].

Several researchers adopted the edge layer to increase the security of IoT systems by providing crucial security requirements such as access control, authentication, and privacy-preserving [113].

Cui *et al.* [62] introduced edge computing to achieve an effective access control for IoT networks. They proposed a proxy-aided CP-ABE scheme where partial decryption computations are maintained by edge devices. The proposed scheme significantly reduces the computational cost compared to CP-ABE schemes.

Hsu *et al.* [63] designed an efficient framework to strengthen the security of resource-limited IoT devices using edge computing. The proposed framework is based on an edge device called a security agent which is responsible for performing cryptographic computations to secure communications among IoT devices.

Wazid *et al.* [64] focused on device authentication and key management for securing communication in an edge-based IoT environment. The proposed scheme is based on a lightweight cryptographic hash function and thus, it is efficient in terms of computation cost. In addition, it resists known security attacks.

Razaque *et al.* [65] addressed the detection of digital crimes in industry 4.0 and identification of criminals and evidence of crimes. The proposed scheme is based on edge-cloud computing and consists of a detection model and validation model to increase the efficiency and security of industrial forensics.

TABLE 9. Comparison of IoT security schemes based on fog computing.

Scheme	Attack level	Countermeasure	Performance
[53]	Network layer	Communication security	- Medium computation cost - Low communication cost - Storage cost is not considered
[54]	Perception layer	Communication security	- Low computation cost - Medium communication cost - Storage cost is not considered
[55]	Network layer	Data security	- Medium computation cost - Medium communication cost - Storage cost is not considered
[56]	Network layer	Data security	- Low computation cost - Medium communication cost - Storage cost is not considered
[57]	Perception layer	Data security	- High computation cost - High communication cost - Storage cost is not considered
[58]	Network layer	Data security	- High computation cost - Medium communication cost - Storage cost is not considered
[59]	Network layer	Data security	- Low computation cost - Low communication cost - Storage cost is not considered
[60]	Network layer	Data security	- Medium computation cost - Low communication cost - Low storage cost
[61]	Network layer	Data security	- Medium computation cost - Communication cost in not considered - Medium storage cost

Li *et al.* [66] investigated the integration of IoT, mobile edge computing, and cloud computing technologies to guarantee data privacy. Their system architecture includes user devices, edge servers, and a public cloud center. The edge servers are located at the edge of the network (i.e., IoT user devices) and perform data aggregation to provide privacy preservation.

Table 10 compares the IoT security schemes based on edge computing. The integration of edge computing and IoT technologies enhances the performance of IoT systems in terms of communication overhead by providing data processing and aggregation at the edge layer. Consequently, the security of IoT collected data is improved.

C. SOFTWARE-DEFINED NETWORKING-BASED SOLUTIONS

Software-defined networking (SDN) is an emerging computing concept that facilitates network management by separating routing decisions of network elements (e.g., routers, switches, and gateways) and forwarding process.

In SDN architecture, the network control operations like forwarding tables and ACL rules are handled by a centralized component called SDN controller, while data forwarding is managed by the network elements as depicted in Figure 16 [7].

The SDN can be an effective solution for achieving several security requirements in IoT systems. In [67], the authors proposed a role-based SDN architecture for IoT environments. Their network model includes three controllers, and thus the communication traffic is distributed. The proposed

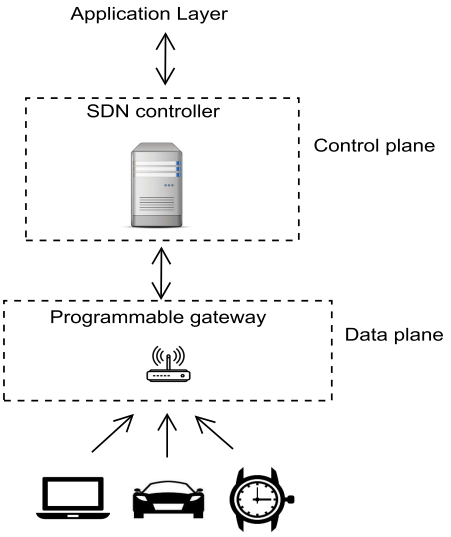


FIGURE 16. Software-defined networking architecture.

distributed architecture provides different security properties. Wang *et al.* [68] proposed an identity-based SDN network to overcome the IoT security threats. The generated identity of the IoT device is based on its IPv6 address and secured using data encryption operation.

To provide authentication in heterogeneous IoT networks, Salman *et al.* [69] presented an identity-based authentication scheme. The proposed scheme has three main components; things, gateway, and SDN controller that is responsible for security management. The formal security verification

TABLE 10. Comparison of IoT security schemes based on edge computing.

Scheme	Attack level	Countermeasure	Performance
[62]	Perception layer	Communication security	- Low computation cost - Communication cost is not considered - Storage cost is not considered
[63]	Perception layer	Communication security	- Medium computation cost - Low communication cost - Storage cost is not considered
[64]	Perception and network layer	Communication security	- Low computation cost - Low communication cost - Storage cost is not considered
[65]	Network and application layer	Communication security	- Low computation cost - Communication cost is not considered - Storage cost is not considered
[66]	Network and application layer	Data security	- Medium computation cost - Low communication cost - Storage cost is not considered

showed that it is secure against masquerade, man-in-the-middle, and replay attacks.

The authors in [70] introduced the SDN in IIoT to secure real-time data transmission. The proposed encryption method requires lightweight operations such as substitution and permutation to provide data confidentiality.

To protect the IoT devices from malicious attacks and mitigate the damage upon an attack, the authors in [71] focused on monitoring anomalous behaviors of IoT devices using SDN gateway with an associated controller. The use of SDN improves the accuracy of attacks detection and enhance the resilience of mitigation action. Bhunia and Gurusamy [72] proposed SDN-based framework. The SDN controller analyzes the communication traffic and determines if it is normal or not. If an attack is detected, it applies rate limiting to reduce the impact of a suspicious attack. The authors considered three different attack scenarios to evaluate the performance of the proposed scheme.

Table 11 compares the IoT security schemes based on SDN. It is noticed that SDN technology can provide security for the IoT environments because security mechanisms can be implemented easily by exploiting the SDN controller capabilities. However, the additional functions of the SDN controller can decrease the network efficiency due to the high communication overhead caused by the control traffic between the SDN controller and the IoT devices.

D. BLOCKCHAIN-BASED SOLUTIONS

Blockchain is a disruptive technology that has revolutionized the world of cryptocurrency. It is a distributed ledger/database that contains transactions of nodes in a peer-to-peer (P2P) network. A set of transactions are grouped into a single block and validated in a distributed way using a consensus algorithm.

The consensus process is executed by some nodes in the network called miners. Common consensus algorithms include proof of work (PoW), proof of stake (PoS), and practical byzantine fault tolerance (PBFT).

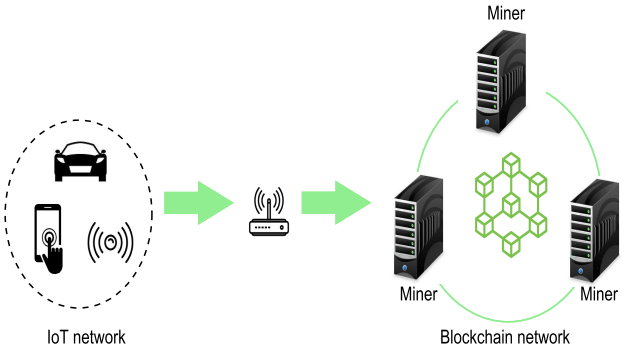


FIGURE 17. Blockchain architecture.

There are two main types of blockchain, namely public (permissionless) and private (permissioned) [114]. Figure 17 demonstrates the architecture of blockchain in IoT.

Due to its prominent features such as decentralization, immutability, transparency, blockchain technology can be applied in several IoT applications. To achieve authentication, Hammi *et al.* [73] proposed a decentralized mechanism called bubbles of trust based on a public blockchain that implements smart contracts. They considered a network with a large number of heterogeneous smart things where each device can communicate only with devices of its zone (i.e., the bubble). Lin *et al.* [74] designed an anonymous authentication scheme using blockchain technology and group signature. The proposed scheme enables users to remotely access smart home devices through a gateway node. To verify a transaction, the gateway node executes a smart contract and all valid transactions are added to the blockchain by consensus nodes. Hong [75] proposed a decentralized authentication system for sensor networks in the context of IoT. The network architecture consists of two main components; sink node and sensor node, and is organized into levels. Each sensor node should prove its legitimacy to top-level root using the blockchain's Merkle tree. Khalid *et al.* [76] adopted the public blockchain to provide a secure environment for IoT smart city scenarios. The proposed mechanism

TABLE 11. Comparison of IoT security schemes based on SDN.

Scheme	Attack level	Countermeasure	Performance
[67]	Perception and network layer	Data, communication and device security	- Low computation cost - High communication cost - Low storage cost
[68]	Perception layer	Device security	- High computation cost - High communication cost - Storage cost is not considered
[69]	Network layer	Communication security	- Low computation cost - Medium communication cost - Low storage cost
[70]	Network layer	Data security	- Low computation cost - Communication cost is not considered - Storage cost is not considered
[71]	Perception layer	Communication security	- High computation cost - Communication cost is not considered - Storage cost is not considered
[72]	Network layer	Communication security	- High computation cost - Communication cost is not considered - Storage cost is not considered

consists of three main phases that include, the initialization phase, device authentication phase, and device-to-device communication phase. In the latter phase, two devices either from the same group or different, communicate with each other after the mutual authentication. Cui *et al.* [77] presented a hybrid blockchain-based authentication mechanism for remote users in WSN-enabled IoT. The proposed scheme includes a base station, cluster head node, ordinary node, and end-user device. It relies on private blockchain for ordinary node authentication and public blockchain for cluster head node authentication and remote user authentication. The user is identified using its certificate distributed by a certificate authority (CA).

To provide secure access control to IoT devices and data, Dorri *et al.* [78] proposed a blockchain-based architecture for IoT smart home systems. They employed a local blockchain that stores all transactions and is managed by the home miner. To establish a secure trusted system in IoT, the authors in [79] investigated the use of blockchain with a reputation mechanism. They introduced a credit-based blockchain to build trust between a service provider and service consumers. The proposed system allows users to consume services by providing obligations as specified by the service provider. These obligations are stored on the blockchain and verified based on the users' reputation information. In [80], the authors evaluated the trustworthiness of sensor data using blockchain technology. Their network architecture consists of a large number of sensors and multiple gateways that maintain the blockchain. The transactions of data including its collection and communication are stored on the blockchain. The block validation is based on a reputation model.

Table 12 compares the IoT security schemes based on blockchain. We notice that we did not consider the computation cost of the mining process because it is well known that it is computationally expensive and requires significant resources. In addition, it depends on the used blockchain (e.g., 14 seconds for Ethereum blockchain). Therefore, we only focused on operations performed on IoT nodes. Most of the reviewed papers have high communication overhead because they employed local blockchains that are not distributed causing in providing high network traffic between the blockchain and the IoT nodes. Therefore, they should be improved to meet the decentralization property of blockchain technology.

E. LIGHTWEIGHT CRYPTOGRAPHY-BASED SOLUTIONS

Cryptography is an effective tool to guarantee confidentiality, integrity, and authentication. However, most IoT devices have challenging characteristics such as processing, memory, and battery power. Thus, traditional cryptographic algorithms are not suitable for resource-constrained IoT devices. Recently, lightweight cryptographic primitives were proposed to secure IoT systems. As presented in Figure 18, lightweight cryptographic algorithms can be classified into four main classes: block ciphers, stream ciphers, hash functions and elliptic curve cryptography (ECC) [115].

In block ciphers, a block of plaintext is encrypted at a time, while stream ciphers encrypt/decrypt a single bit or byte of plaintext/ciphertext.

Hash functions are used to provide data integrity by generating a fixed-length message from an arbitrary-length message. ECC is a lightweight asymmetric cryptographic technique that provides the same level of security as rivest-shamir-adleman (RSA) algorithm with a smaller key size.

Several recent research works [81]–[94] adopt lightweight cryptographic techniques to achieve key security requirements including confidentiality, privacy, integrity, and authentication.

Usman *et al.* [81] presented a lightweight encryption scheme for the IoT. It is a symmetric key block cipher algorithm based on substitution-permutation and feistel networks. The substitution-permutation architecture satisfies Shannon's confusion and diffusion properties. In the feistel architecture, encryption and decryption operations are almost the same. The proposed scheme guarantees data confidentiality and integrity.

TABLE 12. Comparison of IoT security schemes based on blockchain.

Scheme	Attack level	Countermeasure	Performance
[73]	Perception and network layer	Communication and device security	- Low computation cost - Low communication cost - Low storage cost
[74]	Network layer	Communication security	- High computation cost - High communication cost - Storage cost is not considered
[75]	Network layer	Communication security	- Low computation cost - Communication cost is not considered - Storage cost is not considered
[76]	Perception layer	Communication security	- Low computation cost - Low communication cost - Storage cost is not considered
[77]	Perception and network layer	Communication security	- Low computation cost - High communication cost - Low storage cost
[78]	Network layer	Communication security	- Medium computation cost - High communication cost - Storage cost is not considered
[79]	Application layer	Device security	- High computation cost - High communication cost - Storage cost is not considered
[80]	Perception layer	Device security	- Medium computation cost - Communication cost is not considered - Storage cost is not considered

Shahzadi *et al.* [82] focused on securing IoT remote health monitoring systems. They addressed the limitations of Rivest Cipher (RC5) block cipher algorithm and proposed an improved scheme based on a 2D chaotic map. This latter is used for the symmetric key schedule during the encryption and decryption process.

Sharafi *et al.* [83] proposed an enhanced block cipher based on chaotic cryptography for WSNs. They adopted the substitution-permutation network to provide high confusion and diffusion. The proposed scheme is more secure than benchmark algorithms such as RC5 and Skipjack. It is also more efficient than Block Cipher based on Chaotic (BCC) algorithm.

Noura *et al.* [84] proposed a lightweight stream cipher method for real-time IoT applications. Their scheme is based on dynamic key-dependent where a dynamic key is used for one-time data encryption. It is more efficient in terms of encryption time than the AES algorithm since it requires one iteration to provide the ciphertext.

Liu *et al.* [85] investigated the privacy-preserving in dynamic and real-time IoT environments. They proposed two algorithms to protect the private data of resource-constrained IoT devices. They also introduced the edge computing concept to improve the efficiency of their framework. The proposed algorithms are based on the RC4 stream cipher algorithm and chaotic logistic map.

Wazid *et al.* [86] presented a lightweight user authentication mechanism in the context of hierarchical IoT. The proposed scheme is based on a cryptographic hash function and symmetric cryptography. In this scheme, the user can access the information of IoT devices after authentication and session key establishment through a central controller.

Sharma and Kalra [87] designed a secure user authentication approach for cloud-based IoT applications. The proposed scheme is based on a lightweight hash function where the remote user and the cloud server are mutually authenticated and share a session key to secure future communications.

Shen *et al.* [88] proposed two authentication and key establishment protocols for wireless body area networks (WBANs). The two protocols are based on a hash function, elliptic curve cryptography, and symmetric cryptography that provides high security with low computation cost.

Wu *et al.* [89] presented an efficient user authentication scheme for wireless medical sensor networks in IoT. Their scheme uses two factors: user identity and password, and it is based on a cryptographic hash function. The formal security verification showed that the proposed method achieves secure mutual authentication and session key agreement.

Gupta *et al.* [90] proposed a lightweight authentication and key agreement protocol based on hash function for healthcare IoT. Their network consists of wearable devices, a user device, and a server. Before sending the medical data collected by the wearable device, this latter must authenticate the user device using a lightweight cryptographic hash function.

Harbi *et al.* [91] proposed an enhanced ECC-based authentication and session key agreement scheme for WSNs in IoT systems. Their network architecture is organized into clusters to reduce the energy consumption of sensors. The security analysis demonstrated that their scheme resists known attacks and provides major requirements.

Deebak *et al.* [92] proposed a remote user authentication framework based on ECC, cryptographic hash function, and symmetric cryptography for smart healthcare IoT systems.

The proposed scheme involves the user's biometrics to resist the user impersonation attack.

Lee *et al.* [93] proposed an improved user authentication scheme for IoT networks. The proposed scheme is lightweight and suitable for constrained IoT environments. However, the remote user directly authenticates and negotiates a session key with the IoT device without involving a gateway node.

Sadhukhan *et al.* [94] proposed a three-factor user authentication and session key agreement scheme in IoT applications. The proposed scheme is based on ECC, cryptographic hash function, and symmetric cryptography to provide mutual authentication and session key agreement. However, it does not preserve user anonymity and untraceability.

Table 13 compares the IoT security schemes based on lightweight cryptography. It is obvious that most of the surveyed articles are computationally effective because they require lightweight operations to provide the corresponding security requirements. However, they are based on a centralized architecture, and thus, they are limited in terms of scalability, availability, and security. Some of the proposed methods are less efficient in terms of computation and storage cost because they combined lightweight cryptography with traditional symmetric cryptography. Hence, they should be improved to provide security while being suitable for constrained IoT devices.

F. HOMOMORPHIC AND SEARCHABLE ENCRYPTION-BASED SOLUTIONS

The number of IoT devices is increasing to enable the creation of more intelligent applications. These devices generate a massive amount of data that needs to be gathered and analyzed. Cloud computing provides computation and storage services for IoT collected data. These data can be highly sensitive and thus need to be protected from unauthorized access. To provide privacy preservation, the collected data are encrypted then stored in the public cloud.

Homomorphic encryption (HE) allows calculations on encrypted data without revealing the original data. There are two basic types of homomorphic encryption: partially and fully homomorphic methods [116].

Searchable encryption (SE) enables a secure search over encrypted data stored on a cloud server. The SE techniques include symmetric SE, asymmetric SE, and attribute-based SE [117].

The proposed HE-based schemes [95]–[97] and SE-based techniques [98]–[101] aim to provide privacy-preserving in different IoT applications.

Shafagh *et al.* [95] presented data protection scheme based on partially homomorphic encryption (PHE). The proposed scheme is specifically tailored for IoT mobile systems where the cloud stores only encrypted data. It supports encrypted data processing (i.e., sum and average) and encrypted data sharing (i.e., re-encryption). The security analysis showed that the proposed scheme is secure against passive attacks targeted at data on the cloud and prevents access of unauthorized users.

Zouari *et al.* [96] introduced fully additive encryption and fully additive secret sharing to secure aggregation of collected data of heterogeneous IoT devices. They applied their scheme to a smart grid scenario to show its efficiency and resilience.

Lu [97] employed BGN homomorphic encryption to preserve the privacy of user range query in fog-enhanced IoT. The proposed scheme includes three components; IoT devices, fog device, and user that generates BGN public and private keys to secure the transmitted range query. It achieves privacy-preserving and provides efficient communication overhead.

In [98], the authors addressed the limitations of public-key encryption with keyword search (PEKS) technique (i.e., low search efficiency) and proposed a certificateless searchable scheme with multiple keywords for cloud-based IIoT systems. They defined the security model based on game theory and demonstrated that their scheme resists chosen keyword attack.

Li *et al.* [99] proposed a searchable encryption scheme to securely retrieve the encrypted data stored on a cloud server in IoT environments. The proposed scheme consists of five phases, namely, setup, key generation, storage, trapdoor, and search. The authors only considered the computation cost of the storage phase, trapdoor phase, and search phase, while communication overhead and storage cost are not evaluated.

Wang *et al.* [100] suggested the use of attribute-based searchable encryption with equality test for ciphertexts outsourcing in IoT. The equality test enables data users to search ciphertexts without decryption, and thus decreasing the storage cost of IoT devices. The proposed scheme is secure against chosen plaintext attack and chosen keyword attack.

Zhang *et al.* [101] focused on the encrypted data search problem in IIoT and proposed an improved scheme based on a certificateless public key searchable encryption. The cloud server retrieves the ciphertext via trapdoor information. The security analysis using the random oracle model showed that the improved scheme satisfies the ciphertext indistinguishability, trapdoor indistinguishability, and user unforgeability.

Table 14 compares the IoT security schemes based on homomorphic and searchable encryption. It is clearly observed that the reviewed research papers enhance IoT security by effectively providing privacy-preserving at network and application layers. However, they require complex calculations to satisfy the desired level of security.

G. MACHINE LEARNING-BASED SOLUTIONS

Machine learning (ML) is a promising technology that offers embedded intelligence to IoT devices to cope with different security issues. It is a subset of artificial intelligence (AI) that can be used to develop intelligent security systems for IoT networks.

The ML algorithms are classified into five classes: supervised, unsupervised, semi-supervised, reinforcement, and deep learning as shown in Figure 19.

TABLE 13. Comparison of IoT security schemes based on lightweight cryptography.

Scheme	Attack level	Countermeasure	Performance
[81]	Network layer	Data security	- Low computation cost - Communication cost is not considered - Low storage cost
[82]	Network layer	Data security	- Low computation cost - Communication cost is not considered - Storage cost is not considered
[83]	Network layer	Data security	- Low computation cost - Communication cost is not considered - Low storage cost
[84]	Network layer	Data security	- Low computation cost - Communication cost is not considered - Storage cost is not considered
[85]	Network layer	Data security	- Low computation cost - Communication cost is not considered - Low storage cost
[86]	Application layer	Communication security	- Medium computation cost - Low communication cost - High storage cost
[87]	Application layer	Communication security	- Low computation cost - Low communication cost - Low storage cost
[88]	Perception layer	Communication security	- Medium computation cost - Low communication cost - High storage cost
[89]	Application layer	Communication security	- Low computation cost - Low communication cost - Storage cost is not considered
[90]	Application layer	Communication security	- Low computation cost - Low communication cost - Low storage cost
[91]	Perception layer	Communication security	- Low computation cost - Low communication cost - Low storage cost
[92]	Application layer	Communication security	- Medium computation cost - Low communication cost - High storage cost
[93]	Application layer	Communication security	- Low computation cost - Low communication cost - Low storage cost
[94]	Application layer	Communication security	- Medium computation cost - Low communication cost - High storage cost

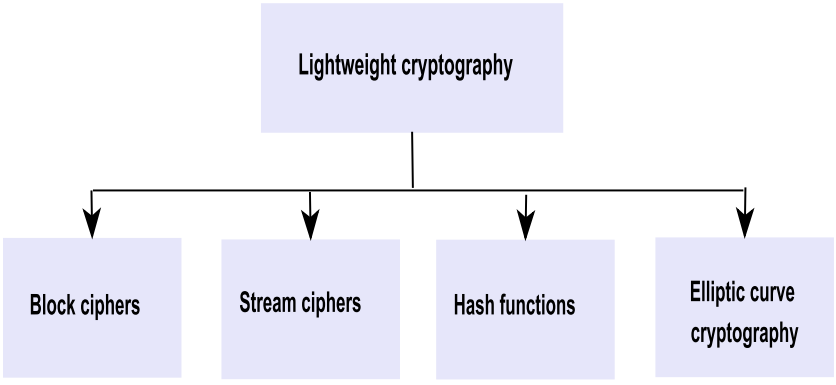


FIGURE 18. Lightweight cryptography for IoT.

Various types of attacks launched on IoT systems such as DoS attack can be detected and mitigated using ML techniques. The ML algorithms can also be used to detect anomalies and intrusions in IoT networks.

Supervised learning algorithms such as support vector machines (SVM), decision tree (DT), and naive bayes (NB) are used to secure IoT systems. However, they require large storage and time for data training.

TABLE 14. Comparison of IoT security schemes based on homomorphic and searchable encryption.

Scheme	Attack level	Countermeasure	Performance
[95]	Application layer	Data security	- High computation cost - High communication cost - High storage cost
[96]	Network layer	Data security	- Medium computation cost - Medium communication cost - Storage cost is not considered
[97]	Application layer	Data security	- Medium computation cost - Low communication cost - Storage cost is not considered
[98]	Application layer	Data security	- High computation cost - Medium communication cost - Storage cost is not considered
[99]	Application layer	Data security	- High computation cost - Communication cost is not considered - Storage cost is not considered
[100]	Application layer	Data security	- High computation cost - Communication cost is not considered - Storage cost is not considered
[101]	Application layer	Data security	- Medium computation cost - Communication cost is not considered - Storage cost is not considered

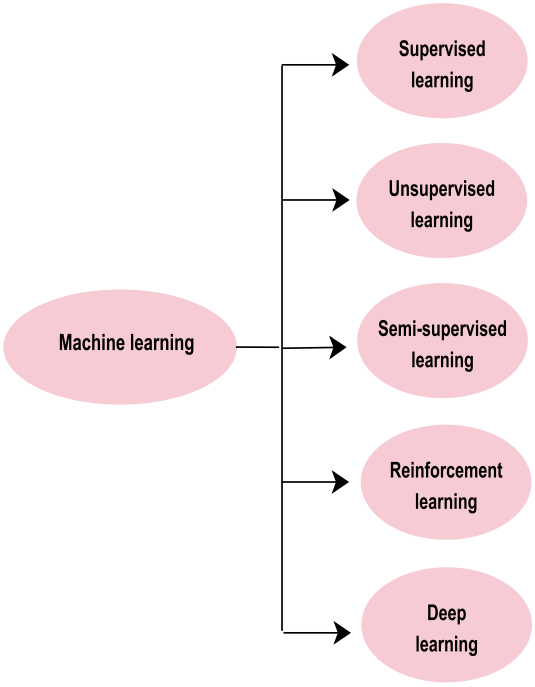


FIGURE 19. Machine learning algorithms.

K-means clustering and hierarchical clustering are two common algorithms of unsupervised learning that do not require data training. The unsupervised algorithms are less efficient than supervised approaches.

Semi-supervised learning was introduced to reduce the datasets needed for training. Nevertheless, it does not provide detection accuracy compared to supervised learning.

Reinforcement learning techniques do not need a rich training dataset but require the knowledge of state transition function.

Deep learning techniques have been employed to address the limitations of other ML techniques [118], [119]. Major deep learning algorithms such as convolutional neural network (CNN), recurrent neural network (RNN), deep belief network (DBN), deep Q-network (DQN) can be used to improve security in IoT systems.

The schemes presented in [102]–[107] were recently proposed to detect various IoT attacks and anomalies using different ML algorithms.

Canedo and Skjellum [102] adopted artificial neural networks to secure IoT systems. They used device ID, sensed value, and timestamp of data transmission as input neurons to train the neural network. They also added invalid data to the database to enable the neural network to detect malicious data. After the training phase, the validity of the IoT device reading is verified within the proposed model.

Nobakht *et al.* [103] proposed an intrusion detection and mitigation framework for IoT smart homes. They addressed potential attacks (e.g., DoS attack) on smart home devices. The proposed scheme examines the network traffic to identify malicious activities and take appropriate countermeasures (i.e., block or redirect the malicious traffic). It requires a set of labeled data for the training phase which is executed in an offline mode. The SVMs algorithm is used for data classification.

Lee *et al.* [104] focused on the abnormal behavior profiling of IoT sensors that collect four different types of data (i.e., temperature, humidity, light, and voltage). The authors used k-Means and SVM algorithms to detect sensed data compromise in two cases; if one data was modified or all data were modified. The k-Means algorithm provided better detection accuracy than the SVM algorithm.

Doshi *et al.* [105] investigated the DoS attacks launched on IoT smart home devices. They employed five machine learning algorithms, namely, K-nearest neighbors, SVM, DT,

Random Forest, and Neural Networks to detect the DoS attacks. All five algorithms had a high detection accuracy.

Alrashdi *et al.* [106] presented a network-based anomaly detection scheme for IoT smart city applications. The proposed scheme consists of a training phase and a testing phase where data classification is performed using the Random Forest algorithm. It achieves high classification accuracy with a low false positive rate.

Bagaa *et al.* [107] designed a security framework to address external and internal attacks in IoT systems. The proposed scheme uses the tempo-spatial correlation between different sensor data based on the SVM algorithm to detect anomaly behaviors (i.e., uncommon sensor data values).

Table 15 compares the IoT security schemes based on machine learning algorithms. These algorithms cannot be applied directly on IoT devices because they involve data training and testing or classification that require large processing capabilities and storage cost. Therefore, most of the surveyed articles employed other emerging technologies like fog computing and SDN to meet the resource-constrained, heterogeneous, and distributed features of the IoT. However, the performance evaluation in terms of communication overhead and storage cost should be considered to show the efficiency of the proposed schemes.

H. LESSONS LEARNED

Securing IoT systems is a complex and challenging task. An effective security solution must not only secure each device independently but provide end-to-end security with low computation complexity, communication overhead, and storage cost based on the target environment. Several promising technologies and techniques were discussed in this section. A comparison of recent research works in terms of major parameters was also provided. This comparison shows that the effectiveness of IoT security schemes does not only depend on the countermeasure mechanisms used against attacks but also performance costs. The proposed security schemes may be improved in terms of performance and robustness by addressing the limitations of the adopted emerging technologies and techniques.

VI. SECURITY CHALLENGES AND FUTURE DIRECTIONS

Although the studied emerging technologies have been introduced to provide improved security in different IoT systems, they impose several security challenges that are not properly solved. Table 16 summarizes the main security purposes and challenges of the studied emerging solutions.

- Most IoT devices are resource-constrained, thus security-enhancing solutions must be computationally efficient. Unfortunately, some emerging technologies and approaches such as blockchain, homomorphic encryption, searchable encryption, and machine learning algorithms require high processing and storage capabilities. Therefore, it is challenging to trade-off between security and performance in IoT infrastructure.
- The IoT takes advantage of fog computing to achieve different security requirements. Fog nodes cooperate to provide real-time and latency-sensitive services to IoT users. However, a fog node does not have any information about other nodes; it is challenging to ensure that all joining fog nodes are trusted. In fact, users have several fog nodes available to cooperate for guaranteeing IoT services. Thus, it is imperative to select trustworthy fog nodes.
- The integration of edge computing and IoT technology improves the performance and security of different IoT applications. However, the edge layer is highly susceptible to attacks and can be easily compromised by adversaries. Common edge computing threats include location-based attack and battery draining attack since edge devices are typically resource-constrained. Moreover, the deployment of edge nodes at the edge of the network (i.e., at a local level) makes recovery mechanisms challenging.
- The IoT is rapidly spreading in different domains. Consequently, physical objects of daily life are progressively integrated into various environments, and thus, the scalability of systems needs to be ensured. However, centralized SDN architecture cannot deal with a large number of IoT devices. In addition, SDN-based solutions are not efficient in high dynamic IoT environments such as vehicular networks. Hence, it is necessary to enforce the scalability property in SDN networks.
- As IoT devices are tremendously increasing, a massive amount of data including sensitive data are generated and exchanged via the Internet. Blockchain technology efficiently tackles the scalability issue due to its distributed architecture. However, it does not ensure the privacy of transactions and it is prone to data leakage. In fog computing-based architecture, fog nodes are responsible for forwarding data to the cloud. If fog nodes are not trustworthy or compromised by an adversary, they can disclose personal information. Furthermore, various threats can be launched against machine learning algorithms during the training process, and thus exposing sensitive data used by the classifiers.
- The security of data transmission can be achieved using encryption techniques. The encryption of transmitted data prevents intruders from revealing the content of messages. This approach can be applied when the communication parties share encryption/decryption keys. In symmetric encryption (i.e., block ciphers, stream ciphers, and hash functions), the key must be pre-distributed or securely communicated. However, in scalable IoT environments, key management including distribution, agreement, update, and revocation remains a meaningful task.

Shortly, the IoT will be extended to the Internet of everything (IoE), the security of future IoT systems will be vital. Several research efforts are required to face the integration of

TABLE 15. Comparison of IoT security schemes based on machine learning algorithms.

Scheme	Attack level	Countermeasure	Performance
[102]	Perception layer	Device security	- High computation cost - Communication cost is not considered - Storage cost is not considered
[103]	Network layer	Device security	- Medium computation cost - Medium communication cost - Storage cost is not considered
[104]	Network layer	Device security	- High computation cost - Communication cost is not considered - Storage cost is not considered
[105]	Network layer	Device security	- Medium computation cost - Communication cost is not considered - Storage cost is not considered
[106]	Network layer	Device security	- Medium computation cost - Communication cost is not considered - Storage cost is not considered
[107]	Perception layer	Device security	- High computation cost - Communication cost is not considered - Storage cost is not considered

TABLE 16. Security purposes and challenges of the studied emerging technologies.

Emerging solution	Security purpose	Security challenge
Fog computing	Authentication, confidentiality	Trust management
Edge computing	Access control, authentication, privacy-preserving	Attack and fault resilience
SDN	Key management, identity management	Scalability
Blockchain	Authentication, access control, trust	Computation complexity, privacy
Lightweight cryptography	Confidentility, integrity, authentication	Key management
HE and SE	Privacy-preserving	Computation complexity
Machine learning	Anomaly detection, attack detection	Computation complexity, privacy

IoT and emerging technologies to guarantee a resilient and desirable level of security.

- Since fog/edge computing is an extension of cloud computing, fog/edge nodes are still prone to various types of attacks. If the fog/edge layer is compromised, then the entire IoT system may be compromised. Machine learning algorithms can be adopted to enhance the security of the fog/edge layer.
- Consensus algorithms of blockchain technology are highly resource hungry, it is recommended to design more efficient and lightweight consensus algorithms suitable for resource-constrained IoT devices.
- The immutability feature of blockchain allows invalid data to be permanently stored, hence, there is a need to explore techniques and methods to handle the permanent storage of invalid data in blockchains.
- IoT devices are more susceptible to attacks due to user's carefulness, an attacker can easily access the devices. Proper guidelines need to be well defined to increase user's awareness about the consequences of possible attacks. Further, the IoT devices should perform self-management mechanisms to defend and recover from possible damages.
- Data reliability is highly required for critical IoT applications such as healthcare systems. Machine learning and artificial intelligence techniques can be used to analyze and classify the collected data by the IoT devices.
- Implementing machine learning algorithms at the fog layer can improve energy efficiency and enhance the scalability of lightweight IoT devices.
- Because machine learning algorithms are susceptible to many threats that can decrease the accuracy of the classifiers, blockchain technology can enhance the reliability of training data by providing decentralization and transparency.
- Data transmission between different IoT layers must be secure; the data should be only revealed at the intended destination. Security mechanisms must be applied at the three IoT layers to provide end-to-end security.
- As IoT wireless technologies have different vulnerabilities, a new generation of communication such as 5G and 6G can be used to enhance the reliability, scalability, and cost-effectiveness of IoT systems.

VII. CONCLUSION

In this paper, we provided a new taxonomy of IoT security attacks based on levels, purposes, and countermeasures. Then, we discussed emerging security solutions for IoT based on different technologies and techniques including fog computing, edge computing, SDN, blockchain, lightweight cryptography, homomorphic and searchable encryption, and machine learning. Furthermore, a comparative study of security schemes based on these emerging technologies and techniques in terms of security and performance was provided. Finally, we presented the security challenges related to

these emerging solutions and highlighted future directions to enhance the security of IoT. This paper will help researchers to have an idea about the current state-of-the-art of security in IoT to address their respective interests.

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.
[2] S. Hammoudi, Z. Aliouat, and S. Harous, "Challenges and research directions for Internet of Things," *Telecommun. Syst.*, vol. 67, no. 2, pp. 367–385, 2018.
[3] D. Evans, "The Internet of Things: How the next evolution of the internet is changing everything," *CISCO White Paper*, vol. 1, pp. 1–11, Apr. 2011.
[4] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, 2013.
[5] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, and D. Aharon, "Unlocking the potential of the Internet of Things," McKinsey Global Inst., Tech. Rep., 2015, vol. 1.
[6] V. Adat and B. B. Gupta, "Security in Internet of Things: Issues, challenges, taxonomy, and architecture," *Telecommun. Syst.*, vol. 67, no. 3, pp. 423–441, 2017.
[7] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things security: A top-down survey," *Comput. Netw.*, vol. 141, pp. 199–221, Aug. 2018.
[8] Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019.
[9] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2018.
[10] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Gener. Comput. Syst.*, vol. 108, pp. 909–920, Jul. 2018.
[11] Y. Harbi, Z. Aliouat, S. Harous, A. Bentaleb, and A. Refoufi, "A review of security in Internet of Things," *Wirel. Pers. Commun.*, vol. 108, no. 1, pp. 325–344, Sep. 2019.
[12] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.
[13] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019.
[14] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019.
[15] S. A. Hamad, Q. Z. Sheng, W. E. Zhang, and S. Nepal, "Realizing an internet of secure things: A survey on issues and enabling technologies," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1372–1391, 2nd Quart., 2020.
[16] M. Mahbub, "Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics," *J. Netw. Comput. Appl.*, vol. 168, Oct. 2020, Art. no. 102761.
[17] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," *Sensors*, vol. 20, no. 13, p. 3625, Jun. 2020.
[18] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, "Internet of Things: Evolution, concerns and security challenges," *Sensors*, vol. 21, no. 5, p. 1809, Mar. 2021.
[19] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28177–28193, 2021.
[20] P. Jayalaxmi, R. Saha, G. Kumar, N. Kumar, and T.-H. Kim, "A taxonomy of security issues in industrial Internet-of-Things: Scoping review for existing solutions, future implications, and research challenges," *IEEE Access*, vol. 9, pp. 25344–25359, 2021.
[21] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.
[22] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," in *Proc. 2nd Int. Conf. Consum. Electron., Commun. Netw. (CECNet)*, Apr. 2012, pp. 1282–1285.
[23] M. Kocakulak and I. Butun, "An overview of wireless sensor networks towards Internet of Things," in *Proc. IEEE 7th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2017, pp. 1–6.
[24] *Zigbee Document 053474r13*, Z. Specification, ZgBee Standards Org., USA, 2006.
[25] *Wireless Medium Access Control and Physical Layer Specifications for Low-Rate Wireless Personal Area Networks*, I. W. Group, IEEE Standard 802.15.4, vol. 802, no. 4, 2003, p. 2003.
[26] J. Li, X. Zhu, N. Tang, and J. Sui, "Study on ZigBee network architecture and routing algorithm," in *Proc. 2nd Int. Conf. Signal Process. Syst.*, vol. 2, Jul. 2010, pp. V2-389–V2-393.
[27] *Bluetooth Core Specification Version 4.0*, Specification Bluetooth Syst., USA, vol. 1, 2010, p. 7.
[28] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 packets over IEEE 802.15. 4 networks," *Internet Proposed Standard RFC*, vol. 4944, p. 130, Sep. 2007.
[29] G. Mulligan, "The 6LoWPAN architecture," in *Proc. 4th Workshop Embedded Networked Sensors (EmNets)*, 2007, pp. 78–82.
[30] T. Winter, P. Thubert, A. Brandt, J. W. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J.-P. Vasseur, and R. K. Alexander, *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks*, document RFC 6550, 2012, pp. 1–157.
[31] *Lorawan 1.1 Specification*, Tech. Specification, L. Alliance, USA, 2017.
[32] Z. Shelby, K. Hartke, and C. Bormann, *The Constrained Application Protocol (COAP)*, document RFC 7252, 2014.
[33] T. Zillner and F. Eichelberger, "ZigBee smart homes: A hacker's open house," in *Proc. CRESTCon Conf.*, 2016.
[34] X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen, "Ghost-in-ZigBee: Energy depletion attack on ZigBee-based wireless networks," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 816–829, Oct. 2016.
[35] L. Coppolino, V. D'Alessandro, S. D'Antonio, L. Levy, and L. Romano, "My smart home is under attack," in *Proc. IEEE 18th Int. Conf. Comput. Sci. Eng.*, Oct. 2015, pp. 145–151.
[36] P. Morgner, S. Mattejat, Z. Benenson, C. Müller, and F. Armknecht, "Insecure to the touch: Attacking ZigBee 3.0 via touchlink commissioning," in *Proc. 10th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jul. 2017, pp. 230–240.
[37] M. Ryan, "Bluetooth: With low energy comes low security," in *Proc. 7th USENIX Workshop Offensive Technol. (WOOT)*, 2013, pp. 1–7.
[38] A. Y. Lindell, "Attacks on the pairing protocol of Bluetooth v2. 1," Black Hat USA, Las Vegas, NV, USA, Tech. Rep., 2008.
[39] W. K. Zegeye, "Exploiting Bluetooth low energy pairing vulnerability in telemedicine," Int. Found. Telemetering, USA, Tech. Rep., 2015.
[40] T. Rosa, "Bypassing passkey authentication in Bluetooth low energy," *IACR Cryptol. ePrint Arch.*, vol. 2013, p. 309, May 2013.
[41] M. Ye, N. Jiang, H. Yang, and Q. Yan, "Security analysis of Internet-of-Things: A case study of August smart lock," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2017, pp. 499–504.
[42] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle, "6LoWPAN fragmentation attacks and mitigation mechanisms," in *Proc. 6th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, 2013, pp. 55–66.
[43] A. Rghiout, A. Khannous, and M. Bouhorma, "Denial-of-service attacks on 6LoWPAN-RPL networks: Issues and practical solutions," *J. Adv. Comput. Sci. Technol.*, vol. 3, no. 2, pp. 143–153, 2014.
[44] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," in *Proc. Int. Conf. Pervas. Comput. (ICPC)*, Jan. 2015, pp. 1–6.
[45] A. Mayzaud, R. Badonnel, I. Chrisment, and I. G. Est-Nancy, "A taxonomy of attacks in RPL-based Internet of Things," *Int. J. Netw. Secur.*, vol. 18, no. 3, pp. 459–473, 2016.
[46] R. Miller, "LoRa security: Building a secure LoRa solution," MWR Labs, White Paper, 2016.
[47] X. Yang, E. Karampatzakis, C. Doerr, and F. Kuipers, "Security vulnerabilities in LoRaWAN," in *Proc. IEEE/ACM 3rd Int. Conf. Internet-of-Things Design Implement. (IoTDI)*, Apr. 2018, pp. 129–140.
[48] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, Aug. 2015.

[49] R. A. Rahman and B. Shah, "Security analysis of IoT protocols: A focus in CoAP," in *Proc. 3rd MEC Int. Conf. Big Data Smart City (ICBDSC)*, Mar. 2016, pp. 1–7.

[50] J. Cynthia, H. P. Sultana, M. Saroja, and J. Senthil, "Security protocols for IoT," in *Ubiquitous Computing and Computing Security of IoT*. Cham, Switzerland: Springer, 2019, pp. 1–28.

[51] M. Singh, M. A. Rajan, V. L. Shivraj, and P. Balamuralidhar, "Secure MQTT for Internet of Things (IoT)," in *Proc. 5th Int. Conf. Commun. Syst. Netw. Technol.*, Apr. 2015, pp. 746–751.

[52] A. Marzano, D. Alexander, O. Fonseca, E. Fazzion, C. Hoepers, K. Steding-Jessen, M. H. P. C. Chaves, I. Cunha, D. Guedes, and W. Meira, "The evolution of bashlite and mirai IoT botnets," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2018, pp. 00813–00818.

[53] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng, "An attribute-based encryption scheme to secure fog communications," *IEEE Access*, vol. 5, pp. 9131–9138, 2017.

[54] P. Gope, "LAAP: Lightweight anonymous authentication protocol for D2D-aided fog computing paradigm," *Comput. Secur.*, vol. 86, pp. 223–237, Sep. 2019.

[55] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, "Security and privacy preservation scheme of face identification and resolution framework using fog computing in Internet of Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1143–1155, Oct. 2017.

[56] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[57] X. Yang, F. Yin, and X. Tang, "A fine-grained and privacy-preserving query scheme for fog computing-enhanced location-based service," *Sensors*, vol. 17, no. 7, p. 1611, 2017.

[58] Z. Guan, Y. Zhang, L. Wu, J. Wu, J. Li, Y. Ma, and J. Hu, "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT," *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, Jan. 2019.

[59] K. Boakye-Boateng, E. Kuada, E. Antwi-Boasiako, and E. Djaba, "Encryption protocol for resource-constrained devices in fog-based IoT using one-time pads," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3925–3933, Apr. 2019.

[60] L. Zhang, "Key management scheme for secure channel establishment in fog computing," *IEEE Trans. Cloud Comput.*, early access, Mar. 5, 2019, doi: 10.1109/TCC.2019.2903254.

[61] H. Li and T. Jing, "A ciphertext-policy attribute-based encryption scheme with public verification for an IoT-fog-cloud architecture," *Procedia Comput. Sci.*, vol. 174, pp. 243–251, Jan. 2020.

[62] H. Cui, X. Yi, and S. Nepal, "Achieving scalable access control over encrypted data for edge computing networks," *IEEE Access*, vol. 6, pp. 30049–30059, 2018.

[63] R.-H. Hsu, J. Lee, T. Q. S. Quek, and J.-C. Chen, "Reconfigurable security: Edge-computing-based framework for IoT," *IEEE Netw.*, vol. 32, no. 5, pp. 92–99, Sep./Oct. 2018.

[64] M. Wazid, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, "LDAKM-EIoT: Lightweight device authentication and key management mechanism for edge-based IoT deployment," *Sensors*, vol. 19, no. 24, p. 5539, Dec. 2019.

[65] A. Razaque, M. Aloqaily, M. Almiani, Y. Jararweh, and G. Srivastava, "Efficient and reliable forensics using intelligent edge computing," *Future Gener. Comput. Syst.*, vol. 118, pp. 230–239, May 2021.

[66] X. Li, S. Liu, F. Wu, S. Kumari, and J. J. P. C. Rodrigues, "Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4755–4763, Jun. 2019.

[67] K. Kalkan and S. Zeadally, "Securing Internet of Things with software defined networking," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 186–192, Sep. 2017.

[68] X. Wang, K. Xu, W. Chen, Q. Li, M. Shen, and B. Wu, "ID-based SDN for the Internet of Things," *IEEE Netw.*, vol. 34, no. 4, pp. 76–83, Jul. 2020.

[69] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, "Identity-based authentication scheme for the Internet of Things," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2016, pp. 1109–1111.

[70] D. Ma and Y. Shi, "A lightweight encryption algorithm for edge networks in software-defined industrial Internet of Things," in *Proc. IEEE 5th Int. Conf. Comput. Commun. (ICCC)*, Dec. 2019, pp. 1489–1493.

[71] P. Bull, R. Austin, E. Popov, M. Sharma, and R. Watson, "Flow based security for IoT devices using an SDN gateway," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2016, pp. 157–163.

[72] S. S. Bhunia and M. Gurusamy, "Dynamic attack detection and mitigation in IoT using SDN," in *Proc. 27th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2017, pp. 1–6.

[73] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, Sep. 2018.

[74] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, and K.-K.-R. Choo, "HomeChain: A blockchain-based secure mutual authentication system for smart Homes," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 818–829, Feb. 2020.

[75] S. Hong, "P2P networking based Internet of Things (IoT) sensor node authentication by blockchain," *Peer-to-Peer Netw. Appl.*, vol. 13, no. 2, pp. 579–589, Mar. 2020.

[76] U. Khalid, M. Asim, T. Baker, P. C. Hung, M. A. Tariq, and L. Rafferty, "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," *Cluster Comput.*, vol. 23, pp. 1–21, Feb. 2020.

[77] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 241–251, Apr. 2020.

[78] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.

[79] R. Di Pietro, X. Salleras, M. Signorini, and E. Waisbard, "A blockchain-based trust system for the Internet of Things," in *Proc. 23nd ACM Symp. Access Control Models Technol.*, Jun. 2018, pp. 77–83.

[80] V. Dedeoglu, R. Jurdak, G. D. Putra, A. Dorri, and S. S. Kanhere, "A trust architecture for blockchain in iot," in *Proc. 16th EAI Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services*, 2019, pp. 190–199.

[81] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, "SIT: A lightweight encryption algorithm for secure Internet of Things," 2017, *arXiv:1704.08688*. [Online]. Available: https://arxiv.org/abs/1704.08688

[82] R. Shahzadi, S. M. Anwar, F. Qamar, M. Ali, and J. J. P. C. Rodrigues, "Chaos based enhanced RC5 algorithm for security and integrity of clinical images in remote health monitoring," *IEEE Access*, vol. 7, pp. 52858–52870, 2019.

[83] M. Sharafi, F. Fotouhi-Ghazvini, M. Shirali, and M. Ghassemian, "A low power cryptography solution based on chaos theory in wireless sensor nodes," *IEEE Access*, vol. 7, pp. 8737–8753, 2019.

[84] H. Noura, R. Couturier, C. Pham, and A. Chehab, "Lightweight stream cipher scheme for resource-constrained IoT devices," in *Proc. Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2019, pp. 1–8.

[85] T. Liu, Y. Wang, Y. Li, X. Tong, L. Qi, and N. Jiang, "Privacy protection based on stream cipher for spatiotemporal data in IoT," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 7928–7940, Sep. 2020.

[86] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, Feb. 2017.

[87] G. Sharma and S. Kalra, "A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications," *J. Inf. Secur. Appl.*, vol. 42, pp. 95–106, Oct. 2018.

[88] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Gener. Comput. Syst.*, vol. 78, pp. 956–963, Jan. 2018.

[89] F. Wu, X. Li, A. K. Sangaiah, L. Xu, S. Kumari, L. Wu, and J. Shen, "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," *Future Gener. Comput. Syst.*, vol. 82, pp. 727–737, May 2018.

[90] A. Gupta, M. Tripathi, T. J. Shaikh, and A. Sharma, "A lightweight anonymous user authentication and key establishment scheme for wearable devices," *Comput. Netw.*, vol. 149, pp. 29–42, Feb. 2019.

[91] Y. Harbi, Z. Aliouat, A. Refoufi, S. Harous, and A. Bentaleb, "Enhanced authentication and key management scheme for securing data transmission in the Internet of Things," *Ad Hoc Netw.*, vol. 94, Nov. 2019, Art. no. 101948.

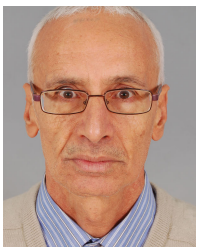
[92] B. D. Deebak, F. Al-Turjman, M. Aloqaily, and O. Alfandi, "An authentic-based privacy preservation protocol for smart e-Healthcare systems in IoT," *IEEE Access*, vol. 7, pp. 135632–135649, 2019.

[93] H. Lee, D. Kang, J. Ryu, D. Won, H. Kim, and Y. Lee, "A three-factor anonymous user authentication scheme for Internet of Things environments," *J. Inf. Secur. Appl.*, vol. 52, Jun. 2020, Art. no. 102494.

[94] D. Sadhukhan, S. Ray, G. P. Biswas, M. K. Khan, and M. Dasgupta, "A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography," *J. Supercomput.*, vol. 77, no. 2, pp. 1114–1151, Feb. 2021.
[95] H. Shafagh, A. Hithnawi, L. Burkhalter, P. Fischli, and S. Duquennoy, "Secure sharing of partially homomorphic encrypted IoT data," in *Proc. 15th ACM Conf. Embedded Netw. Sensor Syst.*, Nov. 2017, pp. 1–14.
[96] J. Zouari, M. Hamdi, and T.-H. Kim, "A privacy-preserving homomorphic encryption scheme for the Internet of Things," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 1939–1944.
[97] R. Lu, "A new communication-efficient privacy-preserving range query scheme in fog-enhanced IoT," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2497–2505, Apr. 2018.
[98] M. Ma, D. He, N. Kumar, K.-K. R. Choo, and J. Chen, "Certificateless searchable public key encryption scheme for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 759–767, Feb. 2017.
[99] S. Li, M. Li, H. Xu, and X. Zhou, "Searchable encryption scheme for personalized privacy in IoT-based big data," *Sensors*, vol. 19, no. 5, p. 1059, Mar. 2019.
[100] S. Wang, L. Yao, J. Chen, and Y. Zhang, "KS-ABESwET: A keyword searchable attribute-based encryption scheme with equality test in the Internet of Things," *IEEE Access*, vol. 7, pp. 80675–80696, 2019.
[101] Y. Zhang, X. Liu, X. Lang, Y. Zhang, and C. Wang, "VCLPKES: Verifiable certificateless public key searchable encryption scheme for industrial Internet of Things," *IEEE Access*, vol. 8, pp. 20849–20861, 2020.
[102] J. Canedo and A. Skjellum, "Using machine learning to secure IoT systems," in *Proc. 14th Annu. Conf. Privacy, Secur. Trust (PST)*, Dec. 2016, pp. 219–222.
[103] M. Nobakht, V. Sivaraman, and R. Boreli, "A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow," in *Proc. 11th Int. Conf. Availability, Rel. Secur. (ARES)*, Aug. 2016, pp. 147–156.
[104] S.-Y. Lee, S.-R. Wi, E. Seo, J.-K. Jung, and T.-M. Chung, "Profiot: Abnormal behavior profiling (ABP) of IoT devices based on a machine learning approach," in *Proc. 27th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2017, pp. 1–6.
[105] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer Internet of Things devices," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2018, pp. 29–35.
[106] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming, "AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2019, pp. 0305–0310.
[107] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "A machine learning security framework for iot systems," *IEEE Access*, vol. 8, pp. 114066–114077, 2020.
[108] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things characterization of fog computing," in *Proc. MCC Workshop Mobile Cloud Comput.*, 2016, pp. 13–17.
[109] P. H. Vilela, J. J. P. C. Rodrigues, P. Solic, K. Saleem, and V. Furtado, "Performance evaluation of a fog-assisted IoT solution for e-health applications," *Future Gener. Comput. Syst.*, vol. 97, pp. 379–386, Aug. 2019.
[110] N. Hassan, S. Gillani, E. Ahmed, I. Ibrar, and M. Imran, "The role of edge computing in Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 110–115, Nov. 2018.
[111] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: State of the art and challenges," *Proc. IEEE*, vol. 107, no. 8, pp. 1608–1631, Aug. 2019.
[112] R. Atiqur, G. Wu, and A. M. Liton, "Mobile edge computing for Internet of Things (IoT): Security and privacy issues," *Indonesian J. Elect. Eng. Comput. Sci.*, vol. 18, no. 3, pp. 1486–1493, 2020.
[113] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing-based designs for IoT security," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 195–202, 2020.
[114] A. Herbadji, H. Goumidi, Y. Harbi, K. Medani, and Z. Aliouat, "Blockchain for internet of vehicles security," in *Blockchain for Cybersecurity and Privacy*. Boca Raton, FL, USA: CRC Press, 2020, p. 159.
[115] S. S. Dhanda, B. Singh, and P. Jindal, "Lightweight cryptography: A solution to secure IoT," *Wireless Pers. Commun.*, vol. 112, no. 3, pp. 1–34, 2020.
[116] G. Peralta, R. G. Cid-Fuentes, J. Bilbao, and P. M. Crespo, "Homomorphic encryption and network coding in IoT architectures: Advantages and future challenges," *Electronics*, vol. 8, no. 8, p. 827, Jul. 2019.
[117] U. Varri, S. Pasupuleti, and K. V. Kadambari, "A scoping review of searchable encryption schemes in cloud computing: Taxonomy, methods, and recent developments," *J. Supercomput.*, vol. 76, no. 4, pp. 3013–3042, Apr. 2020.
[118] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1686–1721, 3rd Quart., 2020.
[119] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1646–1685, 3rd Quart., 2020.

YASMINE HARBI received the B.Sc., M.Sc., and Ph.D. degrees in computer science from Ferhat Abbas University of Setif 1, Setif, Algeria, in 2015, 2017, and 2021, respectively. She is currently an Adjunct Professor with the Faculty of Sciences, Ferhat Abbas University of Setif 1. Her main research interests include wireless sensor networks, security, and privacy in the Internet of Things, blockchain, and applied cryptography.

ZIBOUDA ALIOUAT received the M.Sc. degree in computer science from Constantine University, in 1993, and the Ph.D. degree from Ferhat Abbas University of Setif 1, Setif, Algeria. She is currently a Professor with the Department of Computer Science, Ferhat Abbas University of Setif 1. Her research interests include computer networks, communication modeling, and simulation, wireless sensor networks, fault tolerance of embedded systems, and security and privacy in the Internet of Things.



ALLAOUA REFOUFI received the M.Sc. degree in computer science from the University of Colorado Boulder, USA, in 1980, and the Ph.D. degree from The University of Sheffield, England, in 1990. He is currently a Professor with Ferhat Abbas University of Setif 1, Algeria. His research interests include artificial intelligence, ontology matching algorithms, and big data systems.

SAAD HAROUS (Senior Member, IEEE) received the Ph.D. degree in computer science from Case Western Reserve University, Cleveland, OH, USA, in 1991. He has more than 30 years of experience in teaching and research in three different countries, namely USA, Oman, and United Arab Emirates. He is currently a Professor with the College of Computing and Informatics, University of Sharjah. He has published more than 200 journal articles and conference papers. His teaching interests include programming, data structures, design and analysis of algorithms, operating systems, and networks. His research interests include parallel and distributed computing, P2P delivery architectures, wireless networks, and the use of computers in education and processing Arabic language.