

Received 6 September 2022, accepted 15 September 2022, date of publication 26 September 2022, date of current version 7 October 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3209355



Security in Internet of Things: A Review

NAQASH AZEEM KHAN^{ID1}, (Member, IEEE), AZLAN AWANG^{ID1}, (Senior Member, IEEE),
AND SAMSUL ARIFFIN ABDUL KARIM^{ID2,3}

¹Department of Electrical and Electronic Engineering, Universiti Teknologi PETRONAS, Seri Iskandar, Perak 32610, Malaysia

²Software Engineering Programme, Faculty of Computing and Informatics, Universiti Malaysia Sabah, Jalan UMS, Kota Kinabalu, Sabah 88400, Malaysia

³Data Technologies and Applications (DaTA) Research Group, Universiti Malaysia Sabah, Jalan UMS, Kota Kinabalu, Sabah 88400, Malaysia

Corresponding author: Azlan Awang (azlan.awang@ieee.org)

This research work is fully supported by the Yayasan Universiti Teknologi PETRONAS Fundamental Research Grant (YUTP-FRG) under Grant no. 015LC0-389.

ABSTRACT Internet of Things (IoT) is the paramount virtual network that enables remote users to access connected multimedia devices. It has dragged the attention of the community because it encompasses real-world scenarios with implicit environs. Despite several beneficial aspects, IoT is surrounded by provocations for successful implementation, as data travels in different layers. One of the critical challenges is the security of the data in these layers. Researchers conducted numerous studies focusing on the level of security at a single technique, creating loopholes to address the entire scenario of securing an IoT network. This study aims to comprehensively review current security issues, wireless communication techniques, and technologies for securing IoT. This work's utmost significance is addressing all the security perspectives at a glance. For this purpose, research contributions from the previous years are investigated for better understanding. Some countermeasures and snags from security perspectives have also been analyzed in detail concerning the current industry trends. Blockchain, machine learning, fog, and edge computing are possible solutions to secure IoT. After studying these techniques and their immunity to attacks, machine learning can become a hope if incorporated with end-to-end security. This comprehensive review will provide adequate understanding and knowledge in defining security lines of action for the successful implementation of IoT.

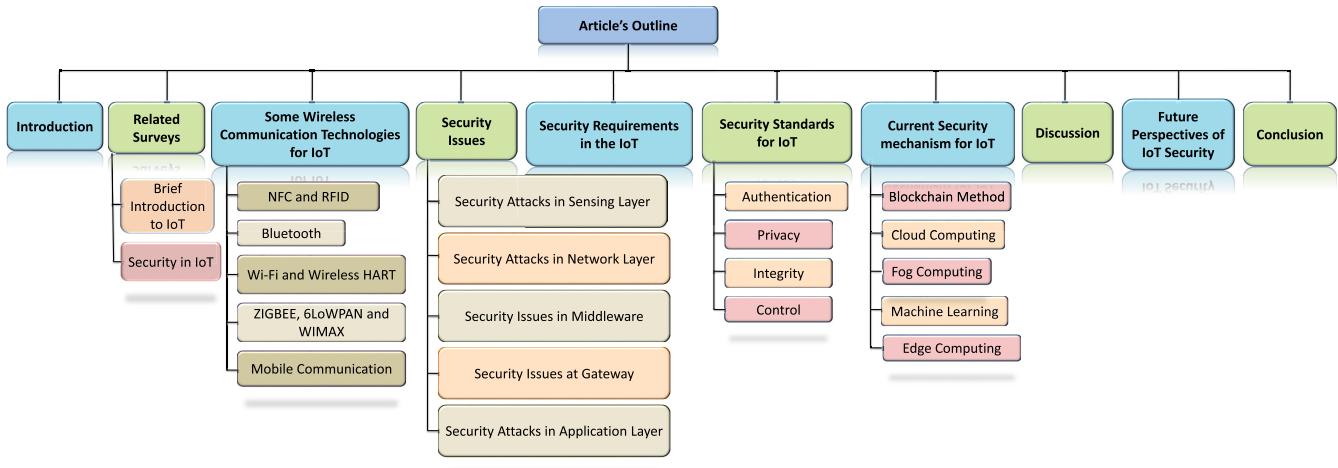
INDEX TERMS Security in IoT, attacks on IoT, threats, solutions in IoT.

I. INTRODUCTION

Internet of Things (IoT) is the inter-networking of the physical parameters embedded with transducers, sensors, actuators, and intelligent systems for an enhanced extent of applications. The data retrieval between these devices is in a seamless manner, accompanying minimal physical interaction. Prevailing IoT applications are highly promising in terms of efficiency, comfort, and automation, as nowadays, industries are developing a huge number of smart IoT devices with intelligent applications. IoT escalated individual elegance through its smart services like retail [1], homes, smart cities [2], [3], farming, agriculture, smart grids [4], [5], and automation [6], [7]. The drastic increase of intelligent IoT devices and programs surrounds the entire world. Especially

The associate editor coordinating the review of this manuscript and approving it for publication was Giovanni Pau^{ID8}.

when countries are implementing industrial revolutions and taking industries to the next generation of the digital economy. Operators worldwide are supporting such applications with the existing communication and networking technologies. According to Cisco numbers, data exchange will exponentially increase in the upcoming decade to a market value of 14 trillion dollars [8]. This data communication between numerous smart digital devices is conventionally insecure and resource-hungry regarding computations and bandwidth constraints [9]. Especially, in the Pandemic situation, these multimedia devices played a vital role in reducing physical interaction, but on the other hand, information became more vulnerable. Researchers contributed by proposing different protocols such as CoAP, RPL, and IPv6 for IPv4 internet to develop secure IoT networks [10]. These protocols help in machine-to-machine interaction and data transfer [11]. Securing IoT has tremendous challenges that still need to

**FIGURE 1.** Content Organization of the Article.

be resolved, including privacy concerns, user authentication, data management, information storage, recovery from attacks, etc.

Some historical disasters are a living example to understand the importance of the issue. In 2017, the Food and Drug Administration Authority of the United States reported modifications to some of their bio-sensors and received threats regarding it [12]. Distributed Denial of Service (DDoS) attacks had tremendous hype from 2019 to 2021 due to the spread of covid-19 [13]. Cortier *et al.* claimed massive security flaws in South Wales state elections happened online in Australia with 280,000 e-votes [14], [15]. Tariq *et al.* claimed the unawareness of 48 percent of people from such cyber threats on their multimedia devices [16], and according to the Government of the UK, almost 40 percent of people do not perform firmware updates [17]. From users' perspective, it is the duty of industries that design systems and applications to resolve the protection risk issue [18], [19], [20]. On the other hand, industries focus on increasing the number of smart IoT devices with minimal cost, smaller size, and low power-consumption rather than providing adequate quality and security features [16].

The paper's organization is shown in Fig. 1. The concise summary of the paper organization is as follows: Section I is an introduction, and Section II is about related surveys. Section III includes wireless communication trends and their compatibility with IoT. Section IV indicates all possible security threats. Requirements and defined standards for efficient security algorithms are explained in sections V and VI respectively. Section VII comprises the presented solutions to date. Section VIII and IX includes discussions and future directions, and section X concludes the paper. In this article, a comprehensive study of more than 250 articles is conducted, including but not limited to surveys, reviews, industrial projects, and publications. This review provides a detailed study of the IoT, its security requirements, threats, wireless communication techniques, open issues, and the possible solutions to date.

TABLE 1. List of Acronyms.

Notation	Meaning
ABSI	Adaptive Binary Splitting Inspection
AMI	Advanced Metering Infrastructure
AMQP	Advanced Message Queuing Protocol
APT	Advanced Persistent Threat
CoAP	Constrained Application Protocol
DAC	Distributed Autonomous Corporation
DAOs	Decentralized Autonomous Organizations
DDoS	Distributed Denial of Service
GPS	Global Positioning System
HAN	Home Area Network
IoT	Internet of Things
IioT	Industrial Internet of Things
IoE	Internet of Everything
M2M	Machine to Machine
MCC	Mobile Cloud Computing
MEC	Mobile Edge Computing
MQTT	Message Queuing Telemetry Transport
SMQTT	Secure Message Queuing Telemetry Transport
NFC	Near Field Communication
P2P	Peer-to-Peer
NFC	Near Field Communication
QoS	Quality of Service
RFID	Radio Frequency Identification
RSN	RFID Sensor Network
SDN	Software-Defined Networking
SHA	Secure Hash Algorithm
STD	Security Trust and Decentralization
WPA	Wireless Protected Access

II. RELATED SURVEYS

This section of the article discusses the brief introduction of IoT and the contributions from the literature regarding the security in IoT.

A. BRIEF INTRODUCTION OF IoT

IoT has completely revolutionized the networks world, by the diversity in its smart applications. These applications include smart health care, smart grids, smart banking, and other smart services. The entire IoT system is based on four main layers [6] as shown in Fig. 2. The antecedent one is the sensing layer that involves sensors and actuators to observe



FIGURE 2. Layers in IoT System - adapted from [6].

data or control signals from physical scenarios. The gathered information from the external environment is converted to electrical signals and forwarded to a wireless communication channel under the network layer. The next layer is renowned as evolving layer or middleware layer as it provides a bridge between the prior two layers. The last layer imparts end-to-end applications to accommodate smart devices, smart transport, smart health, and smart factories, etc. At every layer, there are several security threats concerned with them along with various gateways and numerous privacy issues. Researchers tried to endeavor these security challenges by applying different approaches [21] and proposed solutions classified as, blockchain solutions, fog computing, edge computing, and machine learning-based solutions [6]. Several contributions are added to the literature but unfortunately due to limited and distinct studies, one is not able to gain the entire and diverse perspectives of the security analysis. To cope with this gap a review is required with in-depth analysis. The required analysis should not only highlight issues but also discuss solutions in a broader way. In this review, we aim to provide a broader perspective and focused on each possible point in pursuance to secure IoT. To accomplish the aim

we scrutinized different threats and current communication technologies and analyzed solutions to provide a clear image of the current scenario at securing IoT.

B. SECURITY IN IoT

Securing IoT is a susceptible and critical problem when some of the applications are already deployed, and others future is facing severe risk. The prior task is to identify the open issues. In this regard, the authors of [22] have summarized different security threats in IoT applications. Similarly, [23] indicates many possible vulnerabilities to IoT systems. The authors of [24] identified security issues based on the IoT device location, particularly regarding localization and positioning. Article [25] enlightened middleware issues and analyzed a detailed review of existing protocols and security threats. In [26], authors analyzed various trust management techniques along with their pros and cons. Securing IoT by software-defined networking (SDN) and network function virtualization (NFV) by different mechanisms are discussed in [27]. Some researchers focused on the analysis of security areas based on threats in IoT [28], [29], [30], [31], [32], [33], and others focused on the countermeasures and immunity

TABLE 2. Related Contributions to Secure IoT.

Ref. No. and Year	The solution to secure IoT	Technical concern	Presented methodology	Required enhancement
[65] 2022	Blockchain	Role of blockchain technology in cyber crimes in politics, e-voting, and digital forensic.	A survey article about the loopholes in IoT security, trends in the industrial development regarding device manufacturing and issues in blockchain technology.	Modification is required to focus on different layers and vulnerabilities to these layers for example, DDoS attacks.
[66] 2017	Lightweight computing	Discussion on mechanisms and architectures for authentication and access control	An extensive survey was performed to study IoT device limitations and types of attacks. The central focus was four layers, perception, network, transport, and application layer	The article covers authentication of devices and access control, and it needs further enhancement towards the security of the data
[67] 2021	General discussion on security requirements	A survey article on IoT platforms and topologies in the light of security and privacy	The major focus of this survey article is based on seven parameters: topology, programming languages, third-party support, extended protocol support, event handling, security, and privacy. In term of security concerns to IoT the focus was confidentiality, integrity, availability, and access control.	The study can be further enhanced towards the available solutions to secure IoT involving blockchain technology, machine learning-based, and computing-based solutions.
[68] 2021	Blockchain	Declared blockchain as the most efficient solution for securing IoT	The primary focus of the study is to explain blockchain technology in detail and discuss different techniques like double blockchain and time stamp method to reduce transactional time.	The blockchain technology needs further modifications to cope with dynamic architectures that is variety of sensors, devices and actuators which cannot be treated in similar chain type structure. Similarly numerous types of attacks discussed in section IV requires a highly dynamic technology immune towards confidentiality, integrity, and availability.
[69] 2020	Machine Learning and blockchain	A survey article concerned to IoT security by using blockchain with supervised and unsupervised learning techniques	Discussed infrastructure, protocols, and role of AI and ML in secure IoT. The further study involves discussion regarding machine learning and blockchain technology and their immunity to various attacks.	The survey focused on data security, having zero concern with user authentication. This ultimately makes the system vulnerable to node capture attacks, booting or access attacks, and data theft attacks.
[70] 2021	General discussion and security requirements	A review article on low-power management and security as a basic concern to architecture	A brief discussion on low-power management and infrastructure management presented security as a primary concern in the design of IoT devices.	Focus can be made on security from the broader perspective, such as security requirements, proposed solutions, and problems to be addressed.
[71] 2021	Blockchain	A detailed survey on blockchain technology applications in health, smart homes, and vehicular technology.	A very brief discussion on blockchain related problems and solutions in the fields of decentralized and centralized computing in comparison with cloud, fog, and edge computing techniques.	Blockchain focuses on the data security rather than authenticated users access. Most of the blockchain technology includes costly operations making it susceptible for low cost and constrained IoT devices.
[72] 2019	Edge Computing	A study to achieve user authentication and key generation at physical layer devices by using edge computing to reduce processing burden. In this article, the study and discussions focus is based on heterogeneity, resource constraints, and dynamics of infrastructure under different IoT environments.	The study focuses on the use of mobile edge computing at the physical layer for heterogeneous cloud-based IoT with multiple access mobile edge computing for the smart cities and smart homes.	This approach is highly impactful and can be beneficial if implemented thoroughly on entire IoT rather than focusing only on the physical layer that contains devices like sensors and actuators, etc.
[73] 2017	General discussion and security requirements		The article focused on the security requirements for innovative devices in network infrastructure. The focus was six critical elements in IoT, i.e., networks, cloud, users, attacker, services, and platforms.	The current state of the art in security in IoT is understood. Still, the focus can be the solution for example, blockchain-based solutions, machine learning-based solutions, or end-to-end encryption to resolve these security issues.

towards these vulnerabilities [34], [35], [36], [37], [38], [39]. From the literature study, we can classify the contributions in general categories, which further proposes different dimensions and techniques to secure IoT. These include blockchain, machine learning, and computing-based solutions. Still, some authors focused on the design, and hardware-based security. Another perspective is to secure IoT by using the existing security algorithms, but they are not feasible due to constrained resource architecture of IoT.

The authors of [40] proposed blockchain as an upcoming hope for security in IoT. The major area of blockchain focuses decentralized computing, which is unsuitable for the huge amount of data in IoT. This attracts the use of cloud computing in the field due to its centralized nature. Similarly, the entire data in a single cloud is a huge vulnerability [41]. This leads to the use of fog computing and edge computing to compete with security requirements in IoT. The coherent use of edge computing [42] with a traditional cloud scheme [41]

TABLE 3. Wireless Communication Technologies.

	NFC [10]	RFID [74]	Bluetooth [64]	Wi-Fi [64]	Zigbee [75]	Wireless HART [64]	6LoWPAN [76]	WiMAX [77]	Cellular Network [64]
Network Built-in Security	PAN Nil	PAN Low	PAN Medium	LAN Low	LAN Medium	LAN High	LAN Low	MAN High	WAN Low
Type of Security Power	External Low	External Low	Authentication Low	WPA Low to High	Encryption Low	AES-128 Low	External Low	Internal High	External High
Data rate	400 kbps	400 kbps	700 kbps	10–100 Mbps	250 kbps	250 kbps	250 kbps	10–110 Mbps	1.8–100 Mbps
Coverage Range	< 10 cm	< 3 m	< 30 m	4–20 m	10–300 m	200 m	800 m	50 km	Varies
Cost	Low	Low	Low	Medium	Medium	Medium	Medium	High	High

was proposed to secure IoT systems. A similar approach was implemented to correlate fog computing to IoT [43]. Some researchers used other techniques like authentication and key exchange-based protocol for mobile networks. Similarly, real-time intrusion detection in [44] and use of probabilistic tools like random coefficient selection and mean modification for confidentiality and security in IoT [45] are some common examples. Authors of [46] focused on the use of mobile computing issues and [47] proposed a solution for mobile D2D communication based on android OS. A similar approach for health applications is discussed in [48]. Later on, a survey-based study was implemented in [49] for the analysis of security in smartphones for IoT and [50] proposed a mobile application tool for the analysis of IoT threats. An authentication technique for mobile devices was proposed in [51] using biofeatures. The contribution, in turn became a hope for using supervised and unsupervised learning to be the upcoming hope for securing IoT. As discussed earlier, some authors proposed infrastructure-based solutions [52], [53], [54], [55], [56], [57], [58], [59] to design a separate secure framework at the application layer [58]. In this regard, A study shows that current networking techniques like AWS IoT, Calvin, Brillo/Weave, Kura, ARM Mbed, Homekit, Azure IoT can benefit hardware-based security [60]. A mobile relay-based architecture for Bluetooth has also been discussed in [61]. Similarly, In [62], the authors focused on the security of practical devices like electric bulbs and cameras present in the market and their relation to basic security parameters like confidentiality, integrity, availability, and authentication. A similar approach based on ipv6-enabled RFID tags has been introduced for enhancing authentication in [63]. A brief overview of the work from the previous decade is added in Table 2. There are numerous reviews and survey articles since IoT is an emerging field and is being under observation for its physical implementation from previous years. Still, these articles are unsuccessful in performing a complete study and focus on divergent studies. That's why a review is required, which can converge all concepts in just one paper. It will also help the reader to get sufficient knowledge about securing IoT and explore adequate ideas and understanding of the field. The major contributions of this survey are as follows:

1. A detailed study of layer-based threats and privacy concerns.
2. Identification of the security requirements in IoT system.

3. Classification of the security threats, vulnerabilities, and open issues to IoT.

3. Review on counter measures to security in IoT.

4. Indication of open studies and solutions for IoT security.

III. SOME WIRELESS COMMUNICATION TECHNOLOGIES FOR IoT

Current wireless communication technologies play a vital role in the network layer for intercommunication between the physical and application layers. For IoT, it is much more important to know about wireless communication technologies and their level of security. Moreover, the compatibility of the technology towards security protocols. IoT devices are connected in layers via these wireless communication technologies. So, this section provides a better understanding of security requirements with respect to the practical communication procedure. Inspired by [64], current wireless communication technologies have been incorporated in Table 3. Following are the communication technologies known to date,

A. NEAR FIELD COMMUNICATION AND RADIO FREQUENCY IDENTIFICATION

Near Field Communication (NFC) facilitates its users with short-range RFID-based communication with a high frequency of 13.56 MHz. The only constraint in NFC is that both communication devices must obey their compatibility [10]. NFC provides easy network access and information sharing, making it susceptible to growth in current communication trends. Its high-speed configuration and accessibility provides it an exponential growth. Radio Frequency Identification (RFID) usage in NFC offers some user authentication which can be used in IoT security. NFC has the only drawback in that it reduces connectivity with increasing distance. Texas instruments claimed their current contributions to NFC sensors for IoT applications [10]. RFID is an embedded systems technology with multi-frequency ranges [74]. It supports Low Frequency (125 kHz), High Frequency (13.56 MHz), Ultra High Frequency (860–960 MHz), and microwave communication frequency (2.45–5.8 GHz). RFID offers a license-free communication channel under constrained power. There is no built-in security protocol in NFC and RFID, which means that the security should be provided externally.

B. BLUETOOTH

Based on IEEE 802.15.1 standard, Bluetooth offers a low-cost and low-power wireless communication using 2.4 GHz

frequency [64]. It is highly efficient and cost-effective under short ranges of 8 to 10 m. Its data rate varies from 1 Mbps to 24 Mbps. Its ultra-low power and low-cost versions are also introduced as Bluetooth Low Energy (BLE) or Bluetooth Smart. The security perspective in the bluetooth is better authentication. The devices entering a bluetooth network are authenticated properly, but for data communication, bluetooth is not a secure channel.

C. WIRELESS FIDELITY AND WIRELESS HART

Wi-Fi offers WLAN communication under IEEE 802.11 standard [64]. This standard is further classified into 802.11a which operates in the 5 GHz band, 802.11b and 802.11g operate in the 2.4 GHz band, 802.11n and 802.11ac operate in 5 GHz bands, and 802.11ad operates in the 60 GHz band. Wi-Fi provides 20 m indoor and 100 m outdoor ranges with data rates ranging from 1 Mbps to 6.75 Gbps. Wi-Fi offers a highly secure features including Wireless Protected Access (WPA) and Advanced Encryption Standard (AES). Wireless HART is a Highway Addressable Remote Transducer Protocol (HART) designed for Industrial IoT (IIoT). It was introduced as a multivendor, interoperable wireless protocol. Wireless HART supports the 2.4 GHz ISM band under IEEE 802.15.4 standard radio communication [64]. As the primary focus in Wireless HART was to provide effective communication for industrial applications, so the security was not a major focus in it, but the AES can be implemented as an external encryption.

D. ZigBee, 6LoWPAN AND WiMAX

ZigBee Alliance follows IEEE 802.15.4 specifications with meager cost and power consumption [75]. It can be used for low-power digital radios i.e., home automation, medical devices having line of sight (LoS) communication up to 100 m holding 250 kbps. It can be used for the sensor to sensor and to relay communication in IoT. Zigbee also offers an encryption for the security of the travelling data.

The 6LoWPAN allows IPv6 packet communication over IEEE 802.15.4-based communication channels. 6LoWPAN offers both secure and secure-less modes for transmission [76]. There is no proper built in security algorithm in 6LoWPAN but it can be externally powered by some encryption algorithms.

WiMAX stands for Worldwide Interoperability for Microwave Access, defined under IEEE 802.16, having data rate ranging from 1.5 Mbps to 1 Gbps [77]. A recent IEEE 802.16m provides data rate efficiency from 100 Mbps for mobile stations and 1 Gbps for stationary. Another beneficial perspective of WiMAX includes its internal built in security feature.

E. MOBILE COMMUNICATION

Different generations of mobile communications like 1G include Advanced Mobile Phone System (AMPS), 2G include Global System for Mobile Communication (GSM), 3G including Universal Mobile Telecommunications System (UMTS), and 4G includes Long Term Evaluation (LTE) and

LTE-Advanced [64]. Data rates for these standards range from 9.6 kbps (2G) to 100 Mbps for 4G communication systems. The fifth and sixth generation of mobile communication systems are being deployed and tested worldwide.

From the security perspective, cellular networks do not provide any built in feature but nowadays, smart phones come along internal security and encryption algorithms.

As discussed earlier, the IoT system can be sub-divided into four significant layers. The sensing layer comprises sensors and actuators, which involves a human-machine interface for gathering information from the physical world. Next to the sensing layer is the network layer, responsible for communication between devices, switches, and control units. Further is a middleware that behaves as data storage and provides cloud services. The last one is the application layer which facilitates human life by having a human-machine interface. From the previous section, one can easily understand that vulnerabilities can happen according to the layers. These vulnerabilities can depend upon layer distribution, application, and diverse technologies discussed earlier. Inspired from [6] and based on these dependencies, IoT can face different threats which are described in Section IV.

IV. SECURITY ISSUES

Fig. 3 shows the classification of security discussed in this article. The sensing layer deals with the physical placement of sensors to gather information from the surrounding world [78], [79], [80]. Based on this information, actuators act to control the changes in the physical environment. Sensors can be humidity sensors, smoke detectors, ultrasonic sensors, cameras, temperature sensors, etc or they can be mechanical, electrical, electronic, or chemical sensors to collect information from surroundings. These sensors and actuators hold zero level built-in security.

Similarly, the Network layer is responsible for communication; the primary task is establishing a transmission network with a computational unit without focusing on adequate security. The data in transit flows from the wireless and wired channels via different communication technologies. Such a type of data reaching at receiver end is not trustworthy.

The middleware layer is just an abstraction between the network and application layers. Moreover, it enhances both layers computing and storage resources [81]. It also comprehends persistent data storages, queuing systems, machine learning techniques, etc. The middleware layer is highly reliable and robust for IoT applications, but on the other hand, it is exceedingly susceptible to several attacks. This layer's immense threat is securing databases and clouds from unknown entities. Adversaries can easily access the entire IoT system by attacking the middleware layer.

Gateways provide intercommunication between services, i.e., devices, people, things, and the cloud. They also offer different solutions and data manipulation involving encryption, decryption, and translation of protocols between different

layers [82]. Gateways, being access points, are highly vulnerable if not properly authenticated and reliable.

The application layer deals with services to end-users including smart homes, smart meters, smart cities, and smart-grids, etc. Specific to the applications, security protocols such as data theft and privacy issues are not present in this layer. The middleware layer behaves as a supporting layer for the application layer by intelligent learning of resources and computations. Some of the severe threats encountered by IoT layers are discussed in detail below:

A. SECURITY ATTACKS IN THE SENSING LAYER

Sensing layer is also known as physical layer because of the physical infrastructure. Such a layer involves a large number of devices, for example sensors, actuators, and other smart devices. The security threats and attacks in the sensing layer include the following:

1) NODE CAPTURING

A single sensor or an actuator behaves as a node in the sensing layer. Especially in IoT systems, these nodes are mostly resource-constrained, making them vulnerable to attacks. Adversaries can easily create a node their substrate by capturing or replacing it with a malicious node. The security can be compromised in both cases [83].

2) MALICIOUS CODE INJECTION (MCI) ATTACK

A Malicious Code Injection (MCI) attack involves the injection of malicious code into the node's memory [6]. One can use such nodes as a gateway to perform some unintended operations such as giving falsified information and accessing or hijacking a complete IoT system.

3) FALSE DATA INJECTION (FDI) ATTACK

An attack in which one black sheep can easily inject erroneous data onto the cloud is False Data Injection (FDI). It results in the generation of false results and malfunctioning of the whole system. This attack can cause a denial of service [6].

4) SIDE CHANNEL ATTACKS (SCA)

In some cases, attackers do not attack the nodes directly, but their target is to leak sensitive information [6]. Adversaries focus on the micro-architectures of processors, electromagnetic emanation, and other resource consumption to get sensitive information. Side Channel Attacks (SCA) can be laser-based attacks or timing attacks based upon power consumption. In modern electronics designs, SCA prevention is focused on implementing cryptographic techniques on new FPGA chips.

5) EAVESDROPPING AND INTERFERENCE

Data transmission between different nodes and improper authentication can give eavesdroppers a chance to get access to sensitive data [84].

6) SLEEP DEPRIVATION ATTACK (SDA)

Sleep Deprivation Attack (SDA) refers to the drain out the batteries of low-powered nodes leading to the denial of service [6]. The objective can be achieved by running infinite iterative malicious algorithms into the edge devices, which can cause battery drainage, ending with a sleep deprivation attack.

7) BOOTING ATTACKS

At the time of booting a system, all the devices and security algorithms are at zero potential which is the severely vulnerable stage from a security perspective [6]. Especially for IoT systems, a malicious node can easily enter during booting sessions. Adversaries often take advantage of this stage through sleep-wake cycles during the boot.

B. SECURITY ATTACKS IN THE NETWORK LAYER

The key function of the network layer is to provide communication channel with minimal latency, but on the other hand there are some factors who want to manipulate this data in transit. The security attacks in the network layer include the following:

1) PHISHING SITE ATTACK

Phishing Site Attack includes a whole area to be the substrate, and as a result, some devices are endangered [85]. This can happen with minimal effort by an attacker to access these devices, especially in an IoT system where our nodes are things connected with the worldwide web. If a single user's id or password is compromised, the whole system can become vulnerable to cyber attacks; that is why the network layer is always highly fertile for phishing sites attacks.

2) ACCESS ATTACK

Referring to Advanced Persistent Threat (APT), an access attack aims to get the entry of an unauthorized entity to the network [6], [86]. In such a scenario, adversaries remain undetected for a longer duration and their major intention is to gain valuable data instead of providing any damage to the network. IoT systems continuously transceive important information i.e., location of a person, banking accounts, and medical information, which can be highly sensitive for such attacks.

3) DENIAL OF SERVICE (DoS) ATTACK

In DoS attacks, cryptanalysis is done by flooding target servers with numerous unwanted requests, which incapacitates the server from responding [87]. Secondly, it disrupts the server to communicate with genuine nodes resulting in a denial of service. When using multiple sources to flood substrate servers, such attacks are termed as Distributed-DoS attack. IoT systems have enough heterogeneity and complexity, but the network layer is still prone to DDoS attacks. Due to the weak configuration of devices and applications, attackers can get accessible gateways to launch DDoS attacks onto the

Layer based Attacks and Issues to Internet of Things				
Sensing Layer	Network Layer	Middleware Layer	Gateway	Application Layer
Node Capture Attack	Phishing Site Attack	Cloud Flooding Attack	Secure on-boarding	Access Control Attack
MCI Attack	Access Attack	Cloud Malware Injection	Extra Interfaces	Service Interruption Attack
FDI Attack	DDoS / DoS Attack	Signature Wrapping Attack	End-to-End Encryption	Intervention Attack
Side Channel Attack	Data Transit Attack	SQL Injection Attack	Firmware Updates	Sniffing Attack
Eavesdropping and Interference	Routing Attack	Man-in-the-Middle Attack		Reprogramming Attack
Sleep Deprivation Attack	Unlawful Attack			Data Theft
Booting Attack	Common Attacks			MCI Attack
				DDoS Attack

FIGURE 3. Layer based Attacks and Issues to IoT - adapted from [6].

servers. Such a type of attack was experienced in the Mirai botnet attack [87] in 2017.

4) DATA TRANSIT ATTACK

IoT is nothing without exchanging data and valuable information stored in local servers or the cloud [6]. This data storage is highly unsafe if it is not encrypted properly, but the data in transit is more impulsive and irresistible from adversaries. In the network layer of IoT systems, data swing between sensors, actuators, cloud, etc., occur by using numerous communication techniques, making it susceptible to data breaches.

5) ROUTING ATTACK

Routing attacks refer to redirecting the communication channels during data transmission [6]. A sinkhole attack is one of the most renowned kinds of routing attacks in which artificial displacement paths entice nodes as their more feasible communication channel [88]. A wormhole attack is another kind of routing attack which provides a fast transmission path between two nodes [89]. An adversary can bypass security protocols by creating a wormhole between a node and another device. When combined with any other technique, wormhole can become a severe threat to the IoT system [6].

6) UNLAWFUL ATTACK

There are some parameters which define that every attack is not unlawful because some attacks are for the betterment of mankind. There are some attacks in which attackers intend to perform criminal offense. Such a type of attacks are considered as unlawful attacks.

7) COMMON ATTACK

Common attacks involve some common type of attacks which sometimes are to steal information from sender to receiver and sometimes they are to modify the message from the sender to receiver. Such a type of attacks can be considered as common attacks.

C. SECURITY ISSUES IN THE MIDDLEWARE

Middleware is to provide a connection between network layer and application layer. The security attacks in the middleware include the following:

1) CLOUD FLOODING ATTACK (CFA)

Similar to the DoS attack, clouds are also flooded with unnecessary commands or requests [6]. Executing such requests results in zero quality of service (QoS) and cloud depletion just by an extensive workload increase in the form of unfavorable recommendations.

2) CLOUD MALWARE INJECTION (CMI) ATTACK

Cloud Malware Injection is an attack in which the target is to get control of the cloud by injecting an imaginary machine using malicious code [6]. This virtual machine pretends to be a genuine network member to obtain access to the services provided by the IoT system.

3) SIGNATURE WRAPPING ATTACK (SWA)

For authentication purposes, XML signatures are used at the middle-ware layer [95]. During SWA, the attacker aims to break the signature algorithm to gain the executed targets using the Simple Object Access Protocol (SOAP) [96].

4) STRUCTURED QUERY LANGUAGE (SQL) INJECTION ATTACK

Structured Query Language (SQL) injection means to embed mischievous commands in a program [91], [92] to get and to alter sensitive information of a user [93]. Open Web Application Security Project (OWASP) enlisted SQL injection as the top web security threat in 2018 [94].

5) MAN-IN-THE-MIDDLE ATTACK

IBM introduced the Message Queuing telemetry Transport (MQTT) protocol in 1999, providing the basis for lightweight message transmission [90]. This protocol wields a publish-subscribe model allying clients and subscribers to intervene as a proxy. If the attacker behaves as an agent between the sender and receiver in an IoT environment, he can become man-in-the-middle and can easily get information from both nodes. Similarly, a man-in-the-middle can access sensitive data and inject falsified information throughout the IoT system. This may lead him to complete control of the system any client node's notification [6].

D. SECURITY ISSUES AT THE GATEWAY

Gateways are the entry points of every layer. The basic intention of a gateway is to authenticate the devices and applications to provide end user services. The security attacks in the gateway include the following:

1) SECURE ON-BOARDING

Installing a new device to an IoT system requires proper authentication and integration, which is done by cryptographic algorithms. Such scenarios require the protection of encryption keys. Gateways provide the role of a channel between devices and management of services that's why all keys travel through them [6]. Especially during a man-in-the-middle attack, one can easily get capture the encryption keys during the onboarding of a new device.

2) EXTRA INTERFACES

Minimizing the probability of attacks can be the only possible strategy in the security of IoT especially during the installation of new devices in the system [97]. If some of the services and functions are restricted for end-users, backdoor authentication and information breach can be reduced.

3) END-TO-END ENCRYPTION

The only way to establish a highly secure and reliable channel is to develop high-profile end-to-end encryption [98]. Due to this end-to-end encryption, only genuine users can decrypt the encrypted messages. ZigBee protocols have built-in encryption techniques but they do not support end-to-end encryption. Gateways translate information due to inter-switching protocols, where making decryption of enciphered messages makes gateway more vulnerable to data breaches.

4) FIRMWARE UPDATES

Generally, most IoT devices are resource constrained in terms of power and spectrum even though they do not have decision power to install any firmware. Installing updates depends on gateways by performing a simple validity check.

E. SECURITY ATTACKS IN THE APPLICATION LAYER

The key function of the application layer is to provide the end user services. The devices in the application layer varies with respect to applications. The security attacks in the application layer include the following:

1) ACCESS CONTROL ATTACK

Access control refers to the authorization of the legitimate users to process of the authentic entities. Compromising this access leads to a susceptibility of the entire IoT system.

2) SERVICE INTERRUPTION ATTACKS

Service interruption attacks are referred as illegal interruption attacks, which mean depriving of users performing their operations and exploiting current processing entities resulting in a denial of service.

3) INTERVENTION ATTACK

4) SNIFFING ATTACKS

Sniffing applications allow adversaries to get knowledge about network traffic and sometimes provide a username and pass-keys creating a system quite vulnerable. The adversary can gain access to confidential information if they are just left with zero security [99].

5) RE-PROGRAMMING ATTACKS

Every embedded system has some system software that can be manipulated and the whole system can be misused by inserting some commands inside its programming. Attackers can reprogram IoT objects and gain their desired negative intentions, hijacking the whole IoT system [100].

6) DATA THEFT

Data theft is the possibility in which some of the data is stolen. In such a scenario some other devices outside the network wants to hide their identity and copy the valuable data. Data theft can be done at node level or can be performed at data in transit. Such data theft can be minimized by using techniques of data encryption. This can also be reduced by proper authentication of all of the devices over the network.

7) MCI ATTACK

An MCI attack has been discussed earlier in the subsection A.

8) DDoS ATTACK

A Distributed Denial of Service (DDoS) attack has been discussed earlier in subsection B.

V. SECURITY REQUIREMENTS IN IoT

In the light of the above mentioned threats to the IoT system, we can extract some security requirements recommended to improve the privacy and security concerns. Security features in computer systems can also be added, including firewalls, anti-virus, security software, etc. Some metaheuristic cryptographic algorithms can appropriately fulfill the requirement but at physical layer, there should be some specific algorithms to meet the demands making security in IoT a challenging issue. A well defined and highly secure end-to-end encryption algorithm is still an open issue for the IoT environment. A typical IoT system has a large number of connected devices by using above mentioned wireless communication technologies for example in a smart home system, smart lights and door locking can easily be used to extract user Wi-Fi passwords [101], [102]. Some of the security requirements are as follows,

1. Risk estimation with respect to the location during deployment of devices.
2. Intelligent use of encryption techniques and cryptographic algorithms on the basis of layers and vulnerabilities.
3. Proper authentication to the switching and connected devices can mitigate confidentiality issues.
4. Proper strategies and planning for securing a complete IoT network regardless of focusing on some specific area.
5. Algorithms like RSA, AES, SHA-256, or hash chains to secure the entire IoT environment.
6. Cost and capacity domains should have no constraint [103] due to the rapid increase i.e. IoT should be as public with zero restrictions. Devices should be secure and free to communicate with IoT making it a centralized environment.
7. Cloud, being centralized data storage must be shielded properly. Encrypted data in the cloud can mitigate its chances of being stolen [104].
8. Validation of data-flow mechanism helps in easy handling of errors [105].
9. Intelligent machine learning and artificial intelligence techniques should be used to reduce computational burden and human intervention [106].

Existing literature described several approaches and tactics for IoT security, which can be further classified into four major groups i.e. blockchain-based solutions, fog computing, machine learning and edge computing-based solutions, as explained in Table 4.

VI. SECURITY STANDARDS FOR IoT

On the basis of security requirements for the IoT, some standards have been defined [64]. Once these requirements are met, one can claim the highly secure IoT system. Table 5 shows the security standards defined for IoT in available literature and projects. Some basic standards to secure IoT are as follows:

A. AUTHENTICATION

The most prior task for the IoT security provider is to authenticate the users. IoT system is interconnected with

TABLE 4. Classification of various security areas for IoT with respect to applications.

Blockchain	Edge Computing	Machine Learning	Fog Computing
Financial Transaction [107]– [109]	Medical [120]– [129]	Computer Security [134], [135]	Transportation [140]– [144]
Healthcare [110]– [112]	Energy [123], [124]	Finger Print [136], [137]	Smart Grid [145]– [147]
Electricity [113]– [116]	IoT Devices [125]– [131]	Medical Science [138], [139]	Shopping Cart [148], [149]
Smart IoT Devices [117]– [119]	Smart Grid [132], [133]	Nil	Health Care [150]– [158]

TABLE 5. Security requirements comparison with respect to contributions.

	[160]	[161]	[162]	[163]	[164]	[165]	[166]	[167]
Authentication	✓	—	✓	—	✓	✓	✓	✓
Privacy	✓	✓	✓	✓	✓	✓	✓	✓
Integrity	—	✓	✓	✓	✓	✓	—	✓
Control	✓	✓	✓	✓	✓	✓	✓	✓

switching nodes and sensors making it enough complex and most important operation. Even if a single node is compromised of the sensing layer, the entire system can become vulnerable. There must be some new authentication standard based on autonomous configuration comparative to current standards.

B. PRIVACY

IoT without any privacy concerns is relatively easy for cryptanalysis. With such a backdrop, data sharing within IoT layers become highly susceptible. There should be some end-to-end encryption protocol with high standard security to secure data and messages from black entities.

C. INTEGRITY

The term integrity refers to data integrity, which means whether that received data is from an authentic sender or not. Conventional information security trend is to use public-key cryptography for authentication and keyless-signature infrastructures for communication which can be further extended for data integrity [159].

D. CONTROL

Access control means knowing the entire user library, which plays a vital role [168], [169], [170]. UCON defined three sub-decision factors for control involving authorization, obligation, and conditions with two decision variables of mutability and continuity in [168]. Control is a minor factor as compared to the prior three standards that is the reason behind its negligence.

VII. CURRENT SECURITY MECHANISM FOR IoT

All communication systems should be shielded by applying appropriate security tactics. One of the methods is to secure

them based on the layers i.e. Middleware layer security is a hop-based mechanism with trusted nodes [171]. In such a network, a single pre-shared secret key is used for secure communication. The advantage of a hop-based mechanism is, if an adversary succeeds in attacking a device, it will remain accessed to a single device rather than compromising the entire system. This characteristic limits down the chances of attacks on the system and blocks attackers to a limited range.

Similarly, in 6LoWPAN networks, IPv6 is used to reduce sensor complexity [172], [173], [174], [175]. It further facilitates managing, configuring, and debugging networks [172] which can be the future for the security of communication systems [64].

IPsec can achieve layer security by providing end-to-end security along with authentication, confidentiality, integrity, and compatibility with any network layer [176]. For this purpose, IPsec uses Encapsulated Security Protocol (ESP) [177] and Authentication Header (AH) protocol [178]. Due to these advantages of IPsec, IPv6 uses IPsec as its built-in feature [179].

Securing information and private data rather than securing the entire network is also an efficient technique [180], [181], [182], [183] known as data encryption. This data encryption further enhanced in the shape of selective encryption [11]. Codo [180] provides a security extension for Coffee machine [184], having system software in Contiki OS [185].

Based on the studies performed in the previous decade and different malware detection techniques are discussed in Table 6. Some of the approaches for the security of IoT is shown in Fig. 4. Moreover, the approaches to provide solutions to secure IoT are explained in a systematic way as follows

A. BLOCKCHAIN METHOD

The secure blockchain method is a high-impact process for IoT security using distributed and decentralized security for real-time data [186], [187], as shown in Fig. 4. In this method, the target is accomplished using cryptographic hash keys, which induces enough complexity for the adversaries to tamper within blocks [188], [189]. There are several benefits of the blockchain method i.e., secure data storage assisting distributed blockchains [190], encryption and prevention of data loss from spoofing attacks via authentication and certification [191], [192], proxy-based architecture favors resource-constrained devices [193]. Fig. 5 shows the applications of the blockchain in various fields for example, smart devices, health, electricity and smart grids, and financial transactions.

Merkle tree is an addition to block-chain offering enhancement to security in IoT. Merkle is a binary tree with leaf nodes of data or transactions and roots with hash values of data [194]. It also supports multi-level hashing and reduction in block number endeavoring security compliance [195], making Merkle-based blockchain a promising solution for IoT security [196]. Blockchain, on the one hand, is the current centre of interest due to cryptocurrencies and banking. Still,

TABLE 6. Malware Detection Techniques for IoT Security - adapted from [6].

Ref. No.	Detection Process of Malware	Limitations
[226]	Uses four ways to detect malwares. It divides the applications into four types like malicious, benign aggressive and risky applications.	This technique needs to be more faster for reducing time consumption in analyzing malware.
[227]	Detects the malware by using AOT compiler that changes byte code into machine code form.	Requires to enhance the run time using parallel operations technique to increase speed.
[228]	It uses the machine learning algorithm which was presented by Waikato environment for knowledge analysis (WEKA).	It is only for aggressive applications and provides no classification of risky and benign applications
[229]	Detects application features and decides whether is malicious or not.	The technique discussed is less accurate in detection of malicious application.
[230]	Detects malware by using ensemble classifier for malware detection.	This technique provides less malware detection and gives more false alarm with less accuracy.
[231]	Based upon comparing malicious pattern and normal pattern set and then detects malicious and benign applications.	It requires compatibility with different operating systems
[232]	Uses ADA GRAD optimize algorithm for detecting malware pattern without manual intervention.	Less accuracy rate in malware detection
[233]	Uses machine learning method for android malware detection.	It provides protection only against ransomware attacks
[234]	Andro analysis techniques for evaluating the effectiveness of Andro intense.	It requires to be more accurate.
[235]	Uses Multiflow detection algorithm based upon information flow analysis.	It offers limited attributes to detect malware

on the other hand, due to standardization problems and issues, it is pretty vulnerable too [65].

IoT-Advanced is also Distributed Ledger Technology (DLT) that offers another promising technique of security for IoT. It is designed to focus validation on resource-constrained IoT devices. It is based on the tangle data structure rather than chain-type [197].

B. CLOUD COMPUTING

Cloud Computing offers centralized computing to reduce processing burden. Such a method is helpful in reducing the computational time over IoT network, but in terms of security, it is not an effective method. If an adversary gets access to the cloud then security of the whole system is compromised.

C. FOG COMPUTING

Complementary to cloud computing, fog computing provides better management of IoT data as mentioned in Fig. 6. The figure shows the shielding power of the fog computing to overcome different security threats. Fog computing has two frameworks in its architecture, including the Fog-Device framework and the Cloud-Device framework [198]. Each framework is sub-divided into layers. Fog nodes provide services without involving the cloud layer, but

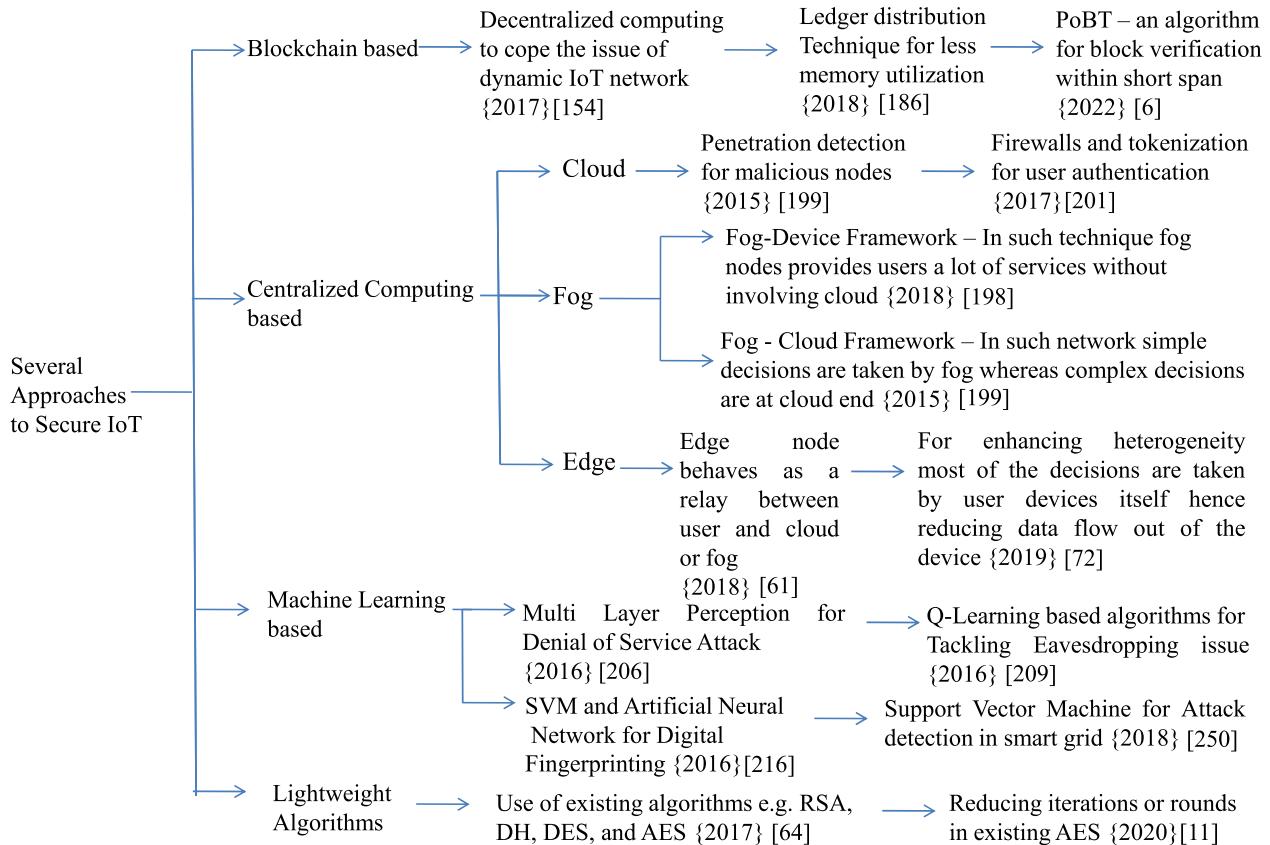


FIGURE 4. Approaches for IoT security.

the Cloud-Device layer involves the cloud in its complex decisions [199]. In [200] the authors claim fog computing is more efficient than the cloud based on latency and energy efficiency. Authors of [201] claim to be 90 percent efficient in latency reduction and twenty percent towards power consumption.

Fog computing also offers better performance than mobile edge computing with real-time video analytics, augmented reality, and big data analysis applications. Another advantage of fog is reducing the frequency of duplex communication between IoT devices and the cloud by consuming minimal network bandwidth [202]. Fog architecture supports data collection at fog nodes having analyzing power of 40 percent, which can reduce the computational burden on cloud and latency issues. Most fog nodes also support cryptographic computations for secure communications, but mere ones require external resources.

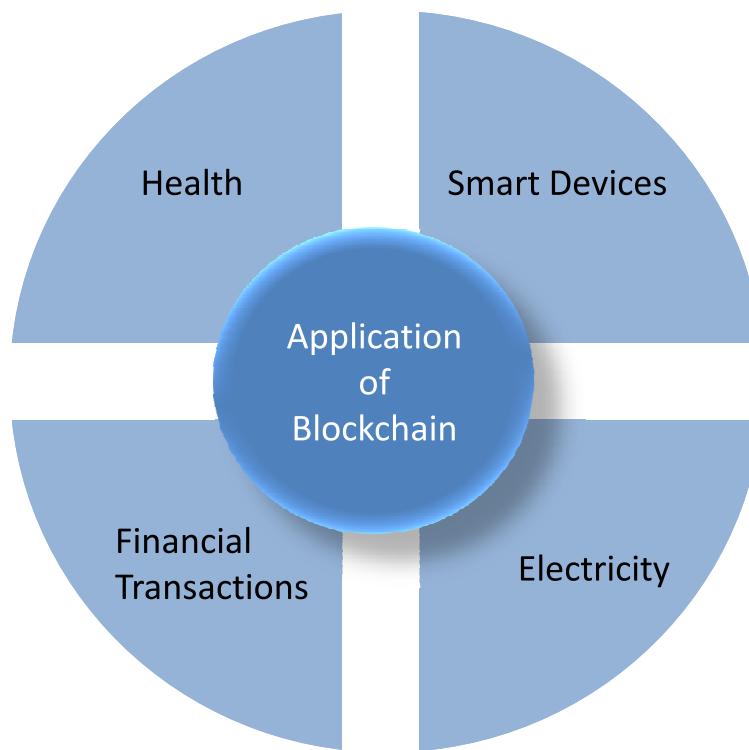
On the other hand, the fog layer invites a new type of threats and challenges towards itself [198]. Fig. 7 shows new challenges and threats that can attack fog. These challenges can be distributed into, real-time services, decentralized computation, data aggregation, data dissemination, and transient storage [6]. On the other hand, Fog computing also provides some solutions for the security of the IoT. Fig. 8 shows the beneficial perspectives of the fog computing for IoT data.

D. MACHINE LEARNING

Machine learning is one of the leading fields in recent years, which provide significant changes in magnificent ways. Many domains use machine learning and IoT is one of them. Several techniques of machine learning are being used to provide solutions to various attacks in new ways, as shown in the Table 7. The solutions of machine learning are far away from conventional methods, e.g., pulse swarm optimization and backpropagation [203] are new trends with promising solutions in the field. The use of neural networks [204] and learning-based algorithms may enhance the concept eventually [205], [206], [207], [208], [209], [210], [211], [212], [213], [214], [215], [216].

E. EDGE COMPUTING

Like fog, edge computing is an add-on to cloud computing, with differing architectures, power, and computing resources. Clouds are mainly at a considerable distance from users, giving a broader concept, especially since a large amount of data is shared in them [217]. Edge computing proposes promising solutions for small cells or edge servers to overcome the issue. Table 8 shows the attack-based immunity of edge computing. The architecture of edge computing constitutes edge devices, cloud servers, and fog nodes [218]. The inter-cooperation and inter-networking of devices enable them to compute data

**FIGURE 5.** Applications of Blockchain.**TABLE 7.** Machine Learning Solutions - based on [6].

Attack	Solution	Ref. No.
Denial of Service	Multilayer Perception, Pulse Swarm Optimization and Back-Propagation algorithm	[205], [206]
Eavesdropping	Q-Learning based offloading, Non-parametric bayesian techniques and Reinforced Learning of Q-Learning and Dyna-Q	[207]–[209]
Spoofing	Q-Learning and Dyna-Q, Support Vector Machine (SVM) based solution, Incremental Aggregated Gradient (IAG) and Distributed Frank Wolfe	[210]–[212]
Privacy Leakage	Privacy Preserving Scientific Computations, Chinese Remainder Theorem	[213], [214]
Digital Fingerprinting	Bio-metric Identification Method, Support Vector Machines and Artificial Neural Networks (ANN)	[215]–[217]

among themselves [219]. This enhances the security level by preventing data from traveling outside the device node, which reduces communication costs, as it avoids data travel to the cloud and back [220].

Edge computing provides enough solutions but also comes with various challenging situations, i.e., entirely relying on edge nodes for all computation reduces the system's reliability. The edge or physical layer includes sensors, actuators, other embedded devices, etc., which are highly susceptible to attacks. Compromising the edge layer will make the entire

**FIGURE 6.** Security and shield provided by fog - based on [6].

IoT system vulnerable. MQTT and COAP are popular protocols of the edge layer, interestingly, both of them have zero built-in security. So, they can be protected externally, i.e., TLS for MQTT and DTLS for COAP, but this also increases bandwidth and computational burden over IoT systems. Other related issues to edge computing are sleep deprivation, battery draining [224], and node attacks, etc.

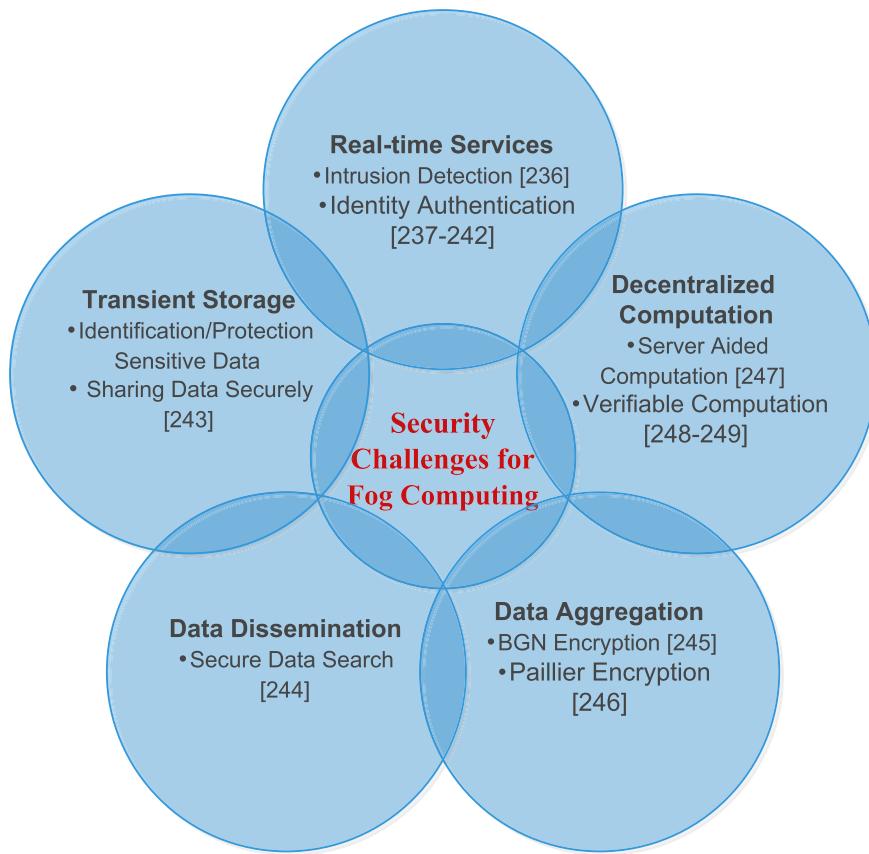


FIGURE 7. Security Challenges to Fog - based on [6].

TABLE 8. Security by Edge Computing - based on [6].

Attack/Issue	Solution/Reason	Ref. No.
Safety and Security	Avoiding latency issues and faster response by intelligent edge nodes on preserve a smart car from being crashed	[220]
Data Breaches	Edge computing avoids data travelling which makes it more secure than fog computing	[221]
Data Compliance	Some countries do not allow data travelling outside their boundaries. Edge computing ensures data sovereignty laws.	[222]
Bandwidth Issues	Reduce raw data movement to cloud hence solving bandwidth issues	[223]

VIII. DISCUSSION

Solutions proposed to date are highly effective and endeavors to performance, but they also have some security and quality issues in using of blockchain, fog computing, edge computing, and machine learning.

Block-chain has a severe issue in its implementation at soft and hard levels, i.e., all transactions being publically transmitted increases the probability of revelation of information. Similarly, due to the increase in the miner's number, cost and speed control becomes another challenging task, leading to scalability and availability issues [225].

The challenges and issues related to fog computing are discussed in [221], as fog computing shares some data with the cloud for decision taking, increasing the vulnerability of sensitive data sharing.

Machine learning algorithms are efficient for IoT but provide heuristic algorithms rather than meta-heuristic nature, so the selection of improper algorithm may lead to an entire system breakdown resulting in garbage outputs. Similarly, the incorrect training data for learning algorithms may lead to erroneous results. The efficiency of machine learning algorithms depends upon factors like diversity in training data selection, improper clustering, and classification of data impact prediction accuracy badly.

Edge computing is mainly concerned with data security and user privacy; compromising a node from a cyber-attack may leak someone's private information. Since edge nodes are involved in all computations, risking a node means risking the entire system.

The whole drill down of the studies indicate that machine learning has minimal constraints, which makes it a bright hope for security in IoT. There is no clear literature on the techniques especially in term of machine learning and edge computing to provide security to IoT. Hence, machine learning and fog computing can be the future of IoT security if their mentioned issues have been resolved.

Characteristics & Solutions provided by Fog Computing

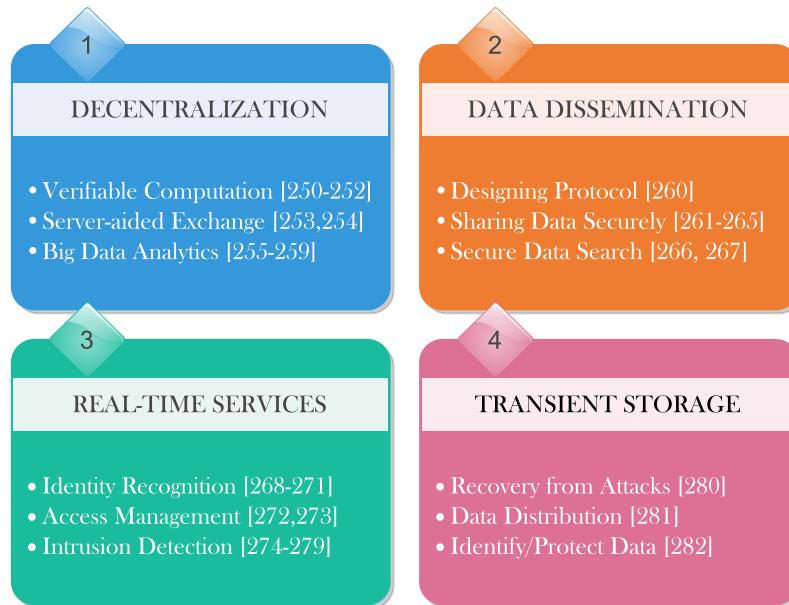


FIGURE 8. Solutions by Fog Computing - based on [6].

IX. FUTURE PERSPECTIVES OF IoT SECURITY

IoT security is highly fertile and still needs plenty of contributions. There are several open studies and challenges that require researchers concern in the field. Some open challenges in IoT security are given as follows:

1. Edge devices need to be highly secure and intelligent to understand adversary attacks.
2. Gateways between different nodes still need enough shielding practices and end-to-end encryption algorithms.
3. In fog sharing, the only target is to secure fog-cloud computation. If achieved, it can be a promising solution.
4. Enhancing the fog layers through machine learning and optimization techniques such as deep learning and artificial intelligence.
5. Blockchain is highly constrained in the case of a number of nodes. The alternative to nodes can be some high efficiency algorithms, and multiple resources can become a prominent solution to solve the issue.
6. Real-time data analysis and efficient hardware design require enough intelligent systems engineering to be developed by using some machine learning and intelligent algorithms.

X. CONCLUSION

This review presents, layer-based threats to IoT covering sensing, middleware, network, and application layer. We have reviewed nearly 200 articles in this area and we have also summarized the promising areas for the research in the IoT security, including blockchain, edge computing, fog computing, and machine learning-based solutions. Some issues and loopholes of these presented solutions have also been

highlighted, making IoT susceptible. According to recent studies, blockchain and machine learning are considered promising solutions to IoT. Blockchain is the principal axis of focus, but its implementation in IoT is yet unsupported due to the standardization issue. Fog computing is a prominent solution but requires a lot of processing burden, resulting in increase in latency. Moreover, it is also infeasible for resource-constrained multimedia devices. Machine learning and end-to-end encryption can be the hope even if it involves a lot of future contributions in terms of newly designed algorithms. The current state of the art and future direction will help enhance IoT security to the premier level. This survey is expected to help understand the entire IoT security issues, challenges, solutions, and further enhancement for the readers, especially the students, researchers, or industry personnel. It will also be a valuable resource for developments in the green future of IoT.

REFERENCES

- [1] N. N. Dlamini and K. Johnston, "The use, benefits and challenges of using the Internet of Things (IoT) in retail businesses: A literature review," in *Proc. Int. Conf. Adv. Comput. Commun. Eng. (ICACCE)*, Nov. 2016, pp. 430-436.
- [2] A. Gharabieh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, "Smart cities: A survey on data management, security, and enabling technologies," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2456-2501, 4th Quart., 2017.
- [3] D. Eckhoff and I. Wagner, "Privacy in the smart city—Applications, technologies, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 489-516, Sep. 2018.
- [4] X. Xia, Y. Xiao, and W. Liang, "ABSI: An adaptive binary splitting algorithm for malicious meter inspection in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 445-458, Feb. 2019.

- [5] V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell, "Toward a secure wireless-based home area network for metering in smart grids," *IEEE Syst. J.*, vol. 8, no. 2, pp. 509–520, Jun. 2014.
- [6] 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.
- [7] A. C. Jose and R. Malekian, "Improving smart home security: Integrating logical sensing into smart home," *IEEE Sensors J.*, vol. 17, no. 13, pp. 4269–4286, Jul. 2017.
- [8] J. Bradley, "The internet of everything: Creating better experiences in unimaginable ways," *Retrieved March*, vol. 12, p. 2019, Nov. 2013.
- [9] R. Wilton, "Four ethical issues in online trust," Identity Privacy-Internet Soc., VA, Tech. Rep. CREDS-PP-2.0, 2014. [Online]. Available: <https://www.internetsociety.org/>
- [10] NFC Transponder for Enabling IoT. Accessed: Sep. 10, 2022. [Online]. Available: <https://connectedworld.net/tag/transponders/>
- [11] N. A. Khan, M. Altaf, and F. A. Khan, "Selective encryption of JPEG images with chaotic based novel S-box," *Multimedia Tools Appl.*, vol. 80, no. 6, pp. 9639–9656, Mar. 2021.
- [12] US Food and Drug Administration. *Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin Home Transmitter: FDA Safety Communication*. Accessed: Sep. 20, 2022. [Online]. Available: <https://www.dicardiology.com/article/fda-confirmed-cybersecurity-vulnerabilities-st-judes-implantable-cardiac-devices-merlin>
- [13] L. Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider, and G. Saldamli, "Predicting and preventing cyber attacks during COVID-19 time using data analysis and proposed secure IoT layered model," in *Proc. 4th Int. Conf. Multimedia Comput., Netw. Appl. (MCNA)*, Oct. 2020, pp. 113–118, doi: [10.1109/mcna50957.2020.9264301](https://doi.org/10.1109/mcna50957.2020.9264301).
- [14] V. Cortier, P. Gaudry, and S. Glondot, "Belenios: A simple private and verifiable electronic voting system," in *Foundations of Security, Protocols, and Equational Reasoning*. Cham, Switzerland: Springer, 2019, pp. 214–238.
- [15] S. Kremer and P. B. Ronne, "To du or not to du: A security analysis of du: A security analysis of du-vote," in *Proc. IEEE Eur. Symp. Secur. Privacy*, Mar. 2016, pp. 473–486.
- [16] T. A. Ahanger, A. Aljumah, and M. Atiquzzaman, "State-of-the-art survey of artificial intelligent techniques for IoT security," *Comput. Netw.*, vol. 206, pp. 1–56, 2022, doi: [10.1016/j.comnet.2022.108771](https://doi.org/10.1016/j.comnet.2022.108771).
- [17] UK Government Developer Documents. Accessed: Jun. 12, 2022. [Online]. Available: <https://assets.publishing.service.gov.uk/>
- [18] M. Ehret and J. Wirtz, "Unlocking value from machines: Business models and the industrial Internet of Things," *J. Marketing Manage.*, vol. 33, nos. 1–2, pp. 111–130, Jan. 2017.
- [19] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-Porisini, "A risk assessment methodology for the Internet of Things," *Comput. Commun.*, vol. 129, pp. 67–79, Sep. 2018.
- [20] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-porisini, "REATO: REActing to denial of service attacks in the Internet of Things," *Comput. Netw.*, vol. 137, pp. 37–48, Jun. 2018.
- [21] G. Yang, "An overview of current solutions for privacy in the Internet of Things," *Frontiers Artif. Intell.*, vol. 5, pp. 1–8, Mar. 2022.
- [22] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.
- [23] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 4, pp. 586–602, Dec. 2016.
- [24] L. Chen, S. Thombore, K. Järvinen, E. S. Lohan, A. Alén-Savikko, H. Leppäkoski, M. Zahidul H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala, and J. Lindqvist, "Robustness, security and privacy in location-based services for future IoT: A survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2017.
- [25] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "IoT Middleware: A survey on issues and enabling technologies," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 1–20, Feb. 2016.
- [26] I. U. Din, M. Guizani, B.-S. Kim, S. Hassan, and M. K. Khan, "Trust management techniques for the Internet of Things: A survey," *IEEE Access*, vol. 7, pp. 29763–29787, 2018.
- [27] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey on emerging SDN and NFV security mechanisms for IoT systems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 812–837, 1st Quart., 2018.
- [28] D. D. López, M. B. Uribe, C. S. Cely, A. V. Torres, N. M. Guataquira, S. M. Castro, P. Nespoli, and F. G. Márquez, "Shielding IoT against cyber-attacks: An event-based approach using SIEM," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–19, Oct. 2018.
- [29] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the Internet of Things," in *Proc. IEEE World Congr. Services*, Jun. 2015, pp. 21–28.
- [30] R. Román-Castro, J. López, and S. Gritzalis, "Evolution and trends in IoT security," *Computer*, vol. 51, no. 7, pp. 16–25, 2018.
- [31] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2015, pp. 180–187.
- [32] F. Meneghelli, 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.
- [33] J. Ahamed and A. V. Rajan, "Internet of Things (IoT): Application systems and security vulnerabilities," in *Proc. 5th Int. Conf. Electron. Devices, Syst. Appl. (ICEDSA)*, 2016, pp. 1–5.
- [34] X. Su, Z. Wang, X. Liu, C. Choi, and D. Choi, "Study to improve security for IoT smart device controller: Drawbacks and countermeasures," *Secur. Commun. Netw.*, vol. 2018, pp. 1–15, May 2018.
- [35] A. Dean and M. O. Agyeman, "A study of the advances in IoT security," in *Proc. 2nd Int. Symp. Comput. Sci. Intell. Control*, Sep. 2018, pp. 1–6.
- [36] A. Girma, "Analysis of security vulnerability and analytics of Internet of Things (IoT) platform," in *Information Technology-New Generations*. Cham, Switzerland: Springer, 2018, pp. 101–104.
- [37] M. Capellupo, J. Liranzo, M. Z. A. Bhuiyan, T. Hayajneh, and G. Wang, "Security and attack vector analysis of IoT devices," in *Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage*, 2017, pp. 593–606.
- [38] I. Sahmi, T. Mazri, and N. Hmina, "Security study of different threats in Internet of Things," in *Proc. 3rd Int. Conf. Smart City App.*, 2018, pp. 785–791.
- [39] V. Mohammadi, A. M. Rahmani, A. M. Darwesh, and A. Sahafi, "Trust-based recommendation systems in Internet of Things: A systematic literature review," *Hum.-Centric Comput. Inf. Sci.*, vol. 9, no. 1, pp. 1–61, Dec. 2019.
- [40] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, "IoT information sharing security mechanism based on blockchain technology," *Future Gener. Comput. Syst.*, vol. 101, pp. 1028–1040, Dec. 2019.
- [41] N. Hadar, S. Siboni, and Y. Elovici, "A lightweight vulnerability mitigation framework for IoT devices," in *Proc. Workshop Internet Things Secur. Privacy*, Nov. 2017, pp. 71–75.
- [42] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2018.
- [43] 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.
- [44] S. Raza, L. Walgreen, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2661–2674, Nov. 2013.
- [45] N. A. Hurrah, S. A. Parah, J. A. Sheikh, F. Al-Turjman, and K. Muhammad, "Secure data transmission framework for confidentiality in IoTs," *Ad Hoc Netw.*, vol. 95, no. 101989, pp. 1–20, 2019.
- [46] A. Kamilaris and A. Pitsillides, "Mobile phone computing and the Internet of Things: A survey," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 885–898, Dec. 2016.
- [47] K. Liu, W. Shen, Y. Cheng, L. X. Cai, Q. Li, S. Zhou, and Z. Niu, "Security analysis of mobile device-to-device network applications," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2922–2932, Apr. 2018.
- [48] A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas, and C. Patsakis, "Security and privacy analysis of mobile health applications: The alarming state of practice," *IEEE Access*, vol. 6, pp. 9390–9403, 2018.

- [49] M. H. Khan and M. A. Shah, "Survey on security threats of smart phones in IoT," in *Proc. 22nd Int. Conf. Autom. Comp. (ICAC)*, 2016, pp. 560–566.
- [50] A. Rodriguez-Mota, P. J. Escamilla-Ambrosio, J. Happa, and E. Aguirre-Anaya, "GARMDROID: IoT potential security threats analysis through the inference of Android applications hardware features requirements," in *Applications for Future Internet*. Cham, Switzerland: Springer, 2017, pp. 63–74.
- [51] M. A. Ferrag, L. Maglaras, and A. Derhab, "Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends," *Secur. Commun. Netw.*, vol. 2019, pp. 1–21, May 2019.
- [52] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.
- [53] W. Jun, M. Lei, and Z. Luo, "Data security mechanism based on hierarchy analysis for Internet of Things," in *Proc. Int. Conf. Innov. Comput. Cloud Comput. (ICCC)*, 2011, pp. 68–70.
- [54] G. George and S. M. Thampi, "Vulnerability-based risk assessment and mitigation strategies for edge devices in the Internet of Things," *Pervas. Mobile Comp.*, vol. 59, Oct. 2019, Art. no. 101068.
- [55] 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. 2020.
- [56] R. Gurunath, M. Agarwal, A. Nandi, and D. Samanta, "An overview: Security issue in IoT network," in *Proc. 2nd Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC)I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)*, Aug. 2018, pp. 104–107.
- [57] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Systematically evaluating security and privacy for consumer IoT devices," in *Proc. Workshop Internet Things Secur. Privacy*, Nov. 2017, pp. 1–6.
- [58] G. Lally and D. Sgandurra, "Towards a framework for testing the security of IoT devices consistently," in *Proc. Int. Workshop Emerg. Technol. Authorization Authentication*, 2018, pp. 88–102.
- [59] F. Semedo, N. Moradpoor, and M. Rafiq, "Vulnerability assessment of objective function of RPL protocol for Internet of Things," in *Proc. 11th Int. Conf. Secur. Inf. Netw.*, Sep. 2018, pp. 1–6.
- [60] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018.
- [61] A. Manzoor, P. Porambage, M. Liyanage, M. Ylianttila, and A. Gurtov, "DEMO: Mobile relay architecture for low-power IoT devices," in *Proc. IEEE 19th Int. Symp. World Wireless, Mobile Multimedia Networks (WoWMoM)*, Jun. 2018, pp. 14–16.
- [62] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Systematically evaluating security and privacy for consumer IoT devices," in *Proc. Workshop Internet Things Secur. Privacy*, Nov. 2017, pp. 1–6.
- [63] S. Dominikus and S. Kraxberger, "Secure communication with RFID tags in the Internet of Things," *Secur. Commun. Netw.*, vol. 7, no. 12, pp. 2639–2653, Dec. 2014.
- [64] M. Sain, Y. J. Kang, and H. J. Lee, "Survey on security in Internet of Things: State of the art and challenges," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2017, pp. 699–704.
- [65] A. E. Omolara, A. Alabdulatif, O. I. Abiodun, M. Alawida, W. H. Alshoura, and H. Arshad, "The Internet of Things security: A survey encompassing unexplored areas and new insights," *Comput. Secur.*, vol. 112, pp. 102494–102525, Jan. 2022, doi: [10.1016/j.cose.2021.102494](https://doi.org/10.1016/j.cose.2021.102494).
- [66] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.
- [67] L. Babun, K. Denney, Z. B. Celik, P. McDaniel, and A. S. Uluagac, "A survey on IoT platforms: Communication, security and privacy perspectives," *Comput. Netw.*, vol. 192, Jun. 2021, Art. no. 108040.
- [68] S. Ramamoorthi, B. M. Kumar, M. Mohamed Sithik, T. Thinesh Kumar, J. Ragaventhiran, and M. Islabudeen, "Enhanced security in IoT environment using blockchain: A survey," *Mater. Today, Proc.*, pp. 1–4, Apr. 2021, doi: [10.1016/j.matpr.2021.03.346](https://doi.org/10.1016/j.matpr.2021.03.346).
- [69] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet Things*, vol. 11, Oct. 2020, Art. no. 100227, doi: [10.1016/j.iot.2020.100227](https://doi.org/10.1016/j.iot.2020.100227).
- [70] M. Aboubakar, M. Kellil, and P. Roux, "A review of IoT network management: Current status and perspectives," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 7, pp. 4163–4176, Jul. 2022, doi: [10.1016/j.jksuci.2021.03.006](https://doi.org/10.1016/j.jksuci.2021.03.006).
- [71] M. A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, "A survey on the adoption of blockchain in IoT: Challenges and solutions," *Blockchain, Res. Apps.*, vol. 2, no. 2, pp. 1–49, 2021, doi: [10.1016/j.bcar.2021.100006](https://doi.org/10.1016/j.bcar.2021.100006).
- [72] D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang, and Z. Han, "Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city," *IEEE Access*, vol. 7, pp. 54508–54521, 2019.
- [73] S.-R. Oh and Y.-G. Kim, "Security requirements analysis for the IoT," in *Proc. Int. Conf. Platform Technol. Service (PlatCon)*, Feb. 2017, pp. 1–6.
- [74] ZigBee. *Brief Introduction*. Accessed: Aug. 11, 2022. [Online]. Available: Accessed: Aug. 11, 2022. [Online]. Available: http://ijariie.com/AdminUploadPdf/WIRELESS_SENSOR_WITH_DATA_LOGGER_USING_ZIGBEE_A REVIEW_ijariie4390.pdf
- [75] ZigBee. *Brief Introduction*. Accessed: Aug. 11, 2022. [Online]. Available: http://ijariie.com/AdminUploadPdf/WIRELESS_SENSOR_WITH_DATA_LOGGER_USING_ZIGBEE_A REVIEW_ijariie4390.pdf
- [76] S. D. Park. *IPv6 Over Low Power WPAN Security Analysis*. Accessed: Sep. 12, 2022. [Online]. Available: <https://datatracker.ietf.org/doc/draft-daniel-6lowpan-security-analysis/>
- [77] P. P. Ray, "A survey on Internet of Things architectures," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 30, no. 3, pp. 291–319, Jul. 2018, doi: [10.1016/j.jksuci.2016.10.003](https://doi.org/10.1016/j.jksuci.2016.10.003).
- [78] Bridgera. *IoT System, Sensors and Actuators*. Accessed: Sep. 18, 2022. [Online]. Available: <https://bridgera.com/IoT-system-sensors-actuators/>
- [79] Smarthomeblog. *How to Make Your Smoke Detector Smarter*. Accessed: Sep. 20, 2022. [Online]. Available: <https://www.smarthomeblog.net/smartsmoke-detector/>
- [80] Tictecbell. *Sensor D'ultrasons*. Accessed: Sep. 22, 2022. [Online]. Available: <https://sites.google.com/site/tictecbell/Arduino/ultrasons/>
- [81] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "A survey of middleware for Internet of Things," in *Recent Trends in Wireless Mobile Network*. Cham, Switzerland: Springer, 2011, pp. 288–296.
- [82] C. Fife. *Securing the IoT Gateway*. Accessed: Aug. 18, 2022. [Online]. Available: <https://www.citrix.com/blogs/2015/07/24/securing-the-IoTgateway/>
- [83] S. Kumar, S. Sahoo, A. Mahapatra, A. K. Swain, and K. K. Mahapatra, "Security enhancements to system on chip devices for IoT perception layer," in *Proc. IEEE Int. Symp. Nanoelectron. Inf. Syst. (iNIS)*, Dec. 2017, pp. 151–156.
- [84] C.-H. Liao, H.-H. Shuai, and L.-C. Wang, "Eavesdropping prevention for heterogeneous Internet of Things systems," in *Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2018, pp. 1–2.
- [85] APWG. *Phishing Activity Trends*. Accessed: Sep. 10, 2022. [Online]. Available: <https://docs.apwg.org/reports/apwg-trends-report-q4-2017.pdf>
- [86] C. Li and C. Chen, "A multi-stage control method application in the fight against phishing attacks," in *Proc. 26th Comput. Secur. Acad. Commun. Across Country*, 2011, p. 145.
- [87] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other Botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.
- [88] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Detection and mitigation of sinkhole attacks in wireless sensor networks," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 644–653, 2014.
- [89] M. Goyal and M. Dutta, "Intrusion detection of wormhole attack in IoT: A review," in *Proc. Int. Conf. Circuits Syst. Digit. Enterprise Technol. (ICCSDET)*, Dec. 2018, pp. 1–5.
- [90] MQTT. *The Standard for IoT Messaging*. Accessed: Sep. 20, 2022. [Online]. Available: <https://mqtt.org/>
- [91] Q. Zhang and X. Wang, "SQL injections through back-end of RFID system," in *Proc. IEEE Int. Symp. Comput. Netw. Multimedia Technol.*, Jan. 2009, pp. 1–4.
- [92] R. Dorai and V. Kannan, "SQL injection-database attack revolution and prevention," *J. Int. Commercial Law Technol.*, vol. 6, no. 4, pp. 224–231, 2011.
- [93] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 3, no. 1, pp. 70–95, Feb. 2016.
- [94] Acunetix. *Insecure Deserialization*. Accessed: Aug. 26, 2022. [Online]. Available: <https://www.acunetix.com/blog/articles/owasp-top-10-2017/>

- [95] J. Kumar, B. Rajendran, B. S. Bindhumadhava, and N. S. C. Babu, "XML wrapping attack mitigation using positional token," in *Proc. Int. Conf. Public Key Infrastruct. Appl. (PKIA)*, Nov. 2017, pp. 36–42.
- [96] WS-Attacks. *Attack Subtypes*. Accessed: Aug. 23, 2022. [Online]. Available: <https://www.ws-attacks.org/XML-Signature-Wrapping>
- [97] A. Stanciu, T.-C. Balan, C. Gerigan, and S. Zamfir, "Securing the IoT gateway based on the hardware implementation of a multi pattern search algorithm," in *Proc. Int. Conf. Optim. Elect. Electron. Equip. (OPTIM) Int. Aegean Conf. Elect. Mach. Power Electron. (ACEMP)*, May 2017, pp. 1001–1006.
- [98] S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, "A blockchain connected gateway for BLE-based devices in the Internet of Things," *IEEE Access*, vol. 6, pp. 24639–24649, 2018.
- [99] S. N. Swamy, D. Jadhav, and N. Kulkarni, "Security threats in the application layer in IoT applications," in *Proc. Int. Conf. IoT Social, Mobile, Analytics Cloud (I-SMAC)*, Feb. 2017, pp. 477–480.
- [100] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 3, pp. 355–373, 2018.
- [101] M. Kumar. *How to Hack WiFi Password From Smart Doorbells*. Accessed: Jul. 20, 2022. [Online]. Available: <http://thehackernews.com/2016/01/doorbell-hacking-wifi-password.html>
- [102] A. Chapman. *Analysing the Attack Surface*. Accessed: Sep. 18, 2022. [Online]. Available: <http://www.contextis.com/resources/blog/hackinginternetconnected-light-bulbs>
- [103] N. Kshetri, "Can blockchain strengthen the Internet of Things?" *IT Prof.*, vol. 19, no. 4, pp. 68–72, 2017.
- [104] W. Wang, P. Xu, and L. T. Yang, "Secure data collection, storage and access in cloud-assisted IoT," *IEEE Cloud Comput.*, vol. 5, no. 4, pp. 77–88, Jul. 2018.
- [105] S. Suhail, C. S. Hong, Z. U. Ahmad, F. Zafar, and A. Khan, "Introducing secure provenance in IoT: Requirements and challenges," in *Proc. Int. Workshop Secure Internet Things (SIoT)*, Sep. 2016, pp. 39–46.
- [106] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?" *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 41–49, Sep. 2018.
- [107] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
- [108] T. Swanson. (Apr. 2015). *Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems*. Accessed: Sep. 20, 2022. [Online]. Available: <https://www.ofnumbers.com/2015/04/06/consensus-as-a-service-a-brief-report-on-the-emergence-of-permissioned-distributed-ledger-systems/>
- [109] D. Wilson and G. Ateniese, "From pretty good to great: Enhancing PGP using bitcoin and the blockchain," in *Proc. Int. Conf. Netw. Syst. Secur.* Cham, Switzerland: Springer, 2015, pp. 368–375.
- [110] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere—a use-case of blockchains in the pharma supply-chain," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, May 2017, pp. 772–777.
- [111] Z. Shae and J. J. P. Tsai, "On the design of a blockchain platform for clinical trial and precision medicine," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2017, pp. 1972–1980.
- [112] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, and F. Sallabi, "Softwareization of Internet of Things infrastructure for secure and smart healthcare," *Computer*, vol. 50, no. 7, pp. 74–79, Jul. 2017.
- [113] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin," in *Proc. IEEE ICIN*, Feb. 2015, pp. 184–191.
- [114] Y. R. Kafle, K. Mahmud, S. Morsalin, and G. E. Town, "Towards an Internet of energy," in *Proc. IEEE Int. Conf. Power Syst. Technol. (POWERCON)*, Sep. 2016, pp. 1–6.
- [115] O. Blanco-Novoa, T. Fernandez-Carames, P. Fraga-Lamas, and L. Castedo, "An electricity price-aware open-source smart socket for the internet of energy," *Sensors*, vol. 17, no. 3, pp. 1–34, 2017.
- [116] T. Lundqvist, A. De Blanche, and H. R. H. Andersson, "Thing-to-thing electricity micro payments using blockchain technology," in *Proc. IEEE Global Internet Things Summit (GIoTS)*, Jun. 2017, pp. 1–6.
- [117] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.
- [118] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. 19th Int. Conf. Adv. Commun. Technol.*, Feb. 2017, pp. 464–467.
- [119] M. Samaniego and R. Deters, "Internet of smart things-IoST: Using blockchain and clips to make things autonomous," in *Proc. IEEE Int. Conf. Cogn. Comput. (ICCC)*, Jun. 2017, pp. 9–16.
- [120] T. Muhammed, R. Mehmood, A. Albeshri, and I. Katib, "UbeHealth: A personalized ubiquitous cloud and edge-enabled networked health-care system for smart cities," *IEEE Access*, vol. 6, pp. 32258–32285, 2018.
- [121] R. K. Barik, H. Dubey, and K. Mankodiya, "SOA-FOG: Secure service-oriented edge computing architecture for smart health big data analytics," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Nov. 2017, pp. 477–481.
- [122] D. Singh, G. Tripathi, A. M. Alberti, and A. Jara, "Semantic edge computing and IoT architecture for military health services in battlefield," in *Proc. 14th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2017, pp. 185–190.
- [123] Y. Li and S. Wang, "An energy-aware edge server placement algorithm in mobile edge computing," in *Proc. IEEE Int. Conf. Edge Comput. (EDGE)*, Jul. 2018, pp. 66–73.
- [124] C. Pan, M. Xie, and J. Hu, "ENZYME: An energy-efficient transient computing paradigm for ultralow self-powered IoT edge devices," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 37, no. 11, pp. 2440–2450, Nov. 2018.
- [125] M. N. Aman, K. C. Chua, and B. Sikdar, "Mutual authentication in IoT systems using physical unclonable functions," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1327–1340, Oct. 2017.
- [126] M. N. Aman, K. C. Chua, and B. Sikdar, "Secure data provenance for the Internet of Things," in *Proc. 3rd ACM Int. Workshop IoT Privacy, Trust, Secur.*, Apr. 2017, pp. 11–14.
- [127] M. N. Aman, B. Sikdar, K. C. Chua, and A. Ali, "Lowpower data integrity in IoT systems," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 3102–3113, Aug. 2018.
- [128] M. N. Aman, S. Taneja, B. Sikdar, K. C. Chua, and M. Alioto, "Token-based security for the Internet of Things with dynamic energy-quality tradeoff," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2843–2859, Apr. 2019.
- [129] M. N. Aman, M. H. Basheer, and B. Sikdar, "Two-factor authentication for IoT with location information," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3335–3351, Apr. 2018.
- [130] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 580–589, Feb. 2019.
- [131] M. N. Aman and B. Sikdar, "ATT-Auth: A hybrid protocol for industrial IoT attestation with authentication," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 5119–5131, Dec. 2018.
- [132] Y. Huang, Y. Lu, F. Wang, X. Fan, J. Liu, and V. C. Leung, "An edge computing framework for real-time monitoring in smart grid," in *Proc. IEEE Int. Conf. Ind. Internet (ICI)*, Oct. 2018, pp. 99–108.
- [133] E. Oyekanlu, C. Nelatury, A. O. Fatade, O. Alaba, and O. Abass, "Edge computing for industrial IoT and the smart grid: Channel capacity for M2M communication over the power line," in *Proc. IEEE 3rd Int. Conf. Electro-Technol. Nat. Develop. (NIGERCON)*, Nov. 2017, pp. 1–11.
- [134] I. Kotenko, I. Saenko, and A. Branitskiy, "Framework for mobile Internet of Things security monitoring based on big data processing and machine learning," *IEEE Access*, vol. 6, pp. 72714–72723, 2018.
- [135] P. K. Chan and R. P. Lippmann, "Machine learning for computer security," *J. Mach. Learn. Res.*, vol. 7, pp. 2669–2672, Dec. 2006.
- [136] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT security through authentication of wireless nodes using *in-situ* machine learning," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 388–398, Feb. 2019.
- [137] K. Merchant, S. Revay, G. Stantchev, and B. Nousain, "Deep learning for RF device fingerprinting in cognitive communication networks," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 1, pp. 160–167, Feb. 2018.

- [138] C. Mercer. *How Machine Learning Will Change Society*. Accessed: Sep. 10, 2022. [Online]. Available: <https://www.techworld.com/picturegallery/tech-innovation/5-ways-machine-learning-will-change-society-3666674>
- [139] M. Chen, Y. Hao, K. Hwang, L. Wang, and L. Wang, "Disease prediction by machine learning over big data from healthcare communities," *IEEE Access*, vol. 5, pp. 8869–8879, 2017.
- [140] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 146–152, Jun. 2017.
- [141] E. K. Markakis, K. Karras, N. Zotos, A. Sideris, T. Moysiadis, A. Corsaro, G. Alexiou, C. Skianis, G. Mastorakis, C. X. Mavromoustakis, and E. Pallis, "EXEGESIS: Extreme edge resource harvesting for a virtualized fog environment," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 173–179, Jul. 2017.
- [142] T. H. Luan, L. Gao, Z. Li, Y. Xiang, G. Wei, and L. Sun, "Fog computing: Focusing on mobile users at the edge," *Comput. Res. Repository*, vol. 1502.01815, pp. 1–11, 2015.
- [143] O. T. T. Kim, N. D. Tri, V. D. Nguyen, N. H. Tran, and C. S. Hong, "A shared parking model in vehicular network using fog and cloud environment," in *Proc. IEEE 17th Asia-Pacific Netw. Oper. Manage. Symp. (APNOMS)*, Aug. 2015, pp. 321–326.
- [144] S. Basudan, X. Lin, and K. Sankaranarayanan, "A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing," *IEEE Internet Things J.*, vol. 4, no. 3, pp. 772–782, Jun. 2017.
- [145] A. V. Dastjerdi and R. Buyya, "Fog computing: Helping the Internet of Things realize its potential," *Computer*, vol. 49, no. 8, pp. 112–116, Aug. 2016.
- [146] M. A. Al Faruque and K. Vatanparvar, "Energy management-as-a-service over fog computing platform," *IEEE Internet Things J.*, vol. 3, no. 2, pp. 161–169, Aug. 2016.
- [147] S. Gao, Z. Peng, B. Xiao, Q. Xiao, and Y. Song, "SCoP: Smartphone energy saving by merging push services in fog computing," in *Proc. IEEE/ACM 25th Int. Symp. Qual. Service (IWQoS)*, Jun. 2017, pp. 1–10.
- [148] W. Shi and S. Dustdar, "The promise of edge computing," *Computer*, vol. 49, no. 5, pp. 78–81, 2016.
- [149] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, pp. 637–646, 2016.
- [150] S. He, B. Cheng, H. Wang, Y. Huang, and J. Chen, "Proactive personalized services through fog-cloud computing in large-scale IoT-based healthcare application," *China Commun.*, vol. 14, no. 11, pp. 1–16, Nov. 2017.
- [151] S. K. Sood and I. Mahajan, "A fog-based healthcare framework for chikungunya," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 794–801, Oct. 2018.
- [152] F. A. Kraemer, A. E. Braten, N. Tamkittikhun, and D. Palma, "Fog computing in healthcare—A review and discussion," *IEEE Access*, vol. 5, pp. 9206–9222, 2017.
- [153] L. Gu, "Cost efficient resource management in fog computing supported medical cyber-physical system," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 1, pp. 108–119, Dec. 2017.
- [154] H. Dubey, A. Monteiro, N. Constant, M. Abtahi, D. Borthakur, L. Mahler, Y. Sun, Q. Yang, U. Akbar, and K. Mankodiya, "Fog computing in medical Internet-of-Things: Architecture, implementation, and applications," in *Handbook of Large-Scale Distributed Computing in Smart Healthcare*. Cham, Switzerland: Springer, 2017, pp. 281–321.
- [155] A. M. Rahmani, T. N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jiang, and P. Liljeberg, "Exploiting smart e-health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," *Future Gener. Comput. Syst.*, vol. 78, pp. 641–658, Jan. 2018.
- [156] Y. Cao, P. Hou, D. Brown, J. Wang, and S. Chen, "Distributed analytics and edge intelligence: Pervasive health monitoring at the era of fog computing," in *Proc. Workshop Mobile Big Data*, Jun. 2015, pp. 43–48.
- [157] W. Shi and S. Dustdar, "The promise of edge computing," *Computer*, vol. 49, no. 5, pp. 78–81, 2016.
- [158] T. N. Gia, M. Jiang, A.-M. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, "Fog computing in healthcare Internet of Things: A case study on ECG feature extraction," in *Proc. IEEE CIT*, Oct. 2015, pp. 356–363.
- [159] N. R. Nikam, P. R. Patil, R. R. Vakhariya, S. K. Mohite, and C. S. Magdum, "Data integrity: An overview," *Int. J. Recent Sci. Res.*, vol. 11, no. 6(A), pp. 38762–38767, 2020.
- [160] R. H. Weber, "Accountability in the Internet of Things," *Comput. Law Secur. Rev.*, vol. 27, no. 2, pp. 133–138, Apr. 2011, doi: [10.1016/j.clsr.2011.01.005](https://doi.org/10.1016/j.clsr.2011.01.005).
- [161] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, and U. Roedig, "Securing communication in 6LoWPAN with compressed IPsec," in *Proc. Int. Conf. Distrib. Comput. Sensor Syst. Workshops (DCOSS)*, Jun. 2011, pp. 1–8.
- [162] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, and M. A. Spirito, "DEMO: An IDS framework for Internet of Things empowered by 6LoWPAN," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 1337–1340, doi: [10.1145/2508859.2512494](https://doi.org/10.1145/2508859.2512494).
- [163] *BUTLER Project*. Accessed: Jul. 4, 2022. [Online]. Available: <http://www.iot-butler.eu>
- [164] *iCORE Project*. Accessed: Jul. 17, 2022. [Online]. Available: <http://www.iot-icore.eu>
- [165] *National Science Foundation Project*. Accessed: Aug. 10, 2022. [Online]. Available: <http://www.nsf.gov>
- [166] *EU-Japan Project*. Accessed: Sep. 5, 2022. [Online]. Available: <http://www.eurojapan-ict.org/>
- [167] *FIRE EU-Korea Project*. Accessed: Sep. 7, 2022. [Online]. Available: <http://eukorea-fire.eu/>
- [168] J. Park and R. Sandhu, "Towards usage control models: Beyond traditional access control," in *Proc. 7th ACM Symp. Access Control Models Technol. (SACMAT)*, 2002, pp. 57–64.
- [169] J. Park, *Usage Control: A Unified Framework for Next Generation Access Control*. Fairfax, VA, USA: George Mason Univ., 2003.
- [170] X. Zhang, *Formal Model and Analysis of Usage Control*. Fairfax, VA, USA: George Mason Univ., 2006. [Online]. Available: https://www.profsandhu.com/dissert/xinwen_diss.pdf
- [171] A. Cui and S. J. Stolfo, "A quantitative analysis of the insecurity of embedded network devices: Results of a wide-area scan," in *Proc. 26th Annu. Comput. Secur. Appl. Conf.*, 2010, pp. 97–106.
- [172] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks," in *Proc. 3rd ACM Workshop Wireless Secur.*, 2004, pp. 32–42.
- [173] G. Mulligan, "The 6LoWPAN architecture," in *Proc. 4th Workshop Embedded Netw. Sensors (EmNets)*, 2007, pp. 78–82.
- [174] J. W. Hui and D. E. Culler, "IP is dead, long live IP for wireless sensor networks," in *Proc. 6th ACM Conf. Embedded Netw. Sensor Syst.*, 2008, pp. 15–28.
- [175] M. Durvy, N. Finne, A. Dunkels, J. Abeillé, P. Wetterwald, C. O'Flynn, B. Leverett, E. Gnoske, M. Vidales, G. Mulligan, and N. Tsiftes, "Making sensor networks IPv6 ready," in *Proc. 6th ACM Conf. Embedded Netw. Sensor Syst.*, 2008, pp. 421–422.
- [176] S. Kent and R. Atkinson, *Security Architecture for the Internet Protocol*, document RFC2401, 1998, pp. 1–65. [Online]. Available: <http://www.ietf.org/rfc/rfc2401.txt>
- [177] S. Kent, *IP Authentication Header*, document RFC Editor 4302, Dec. 2005, pp. 1–34. [Online]. Available: <http://tools.ietf.org/html/rfc4302>
- [178] S. Kent, *IP Encapsulating Security Payload (ESP)*, document RFC Editor 4303, Dec. 2005, pp. 1–44. [Online]. Available: <http://tools.ietf.org/html/rfc4303>
- [179] R. Atkinson, *Security Architecture for the Internet Protocol*, document RFC Editor 1825, Aug. 1995, pp. 1–22. [Online]. Available: <https://www.rfc-editor.org/info/rfc1825>
- [180] I. E. Bagci, M. R. Pourmirza, S. Raza, U. Roedig, and T. Voigt, "Codo: Confidential data storage for wireless sensor networks," in *Proc. IEEE 9th Int. Conf. Mobile Ad-Hoc Sensor Syst. (MASS)*, Oct. 2012, pp. 1–6.
- [181] N. Bhatnagar and E. L. Miller, "Designing a secure reliable file system for sensor networks," in *Proc. ACM Workshop Storage Secur. Survivability*, 2007, pp. 19–24.
- [182] J. Girao, D. Westhoff, E. Mykletun, and T. Araki, "TinyPEDS: Tiny persistent encrypted data storage in asynchronous wireless sensor networks," *Ad Hoc Netw.*, vol. 5, no. 7, pp. 1073–1089, Sep. 2007.
- [183] W. Ren, Y. Ren, and H. Zhang, "HybridS: A scheme for secure distributed data storage in WSNs," in *Proc. IEEE/IFIP Int. Conf. Embedded Ubiquitous Comput.*, Dec. 2008, pp. 318–323.
- [184] N. Tsiftes, A. Dunkels, H. Zhitao, and T. Voigt, "Enabling large-scale storage in sensor networks with the coffee file system," in *Proc. Int. Conf. Inf. Proc. Sensor Netw.*, 2009, pp. 349–360.
- [185] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki—A lightweight and flexible operating system for tiny networked sensors," in *Proc. 29th Annu. IEEE Int. Conf. Local Comput. Netw.*, Jun. 2004, pp. 455–462.

- [186] D. Miller, "Blockchain and the Internet of Things in the industrial sector," *IT Prof.*, vol. 20, no. 3, pp. 15–18, 2018.
- [187] T. Aste, P. Tasca, and T. D. Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18–28, Jan. 2017.
- [188] H. Orman, "Blockchain: The emperors new PKI?" *IEEE Internet Comput.*, vol. 22, no. 2, pp. 23–28, Mar. 2018.
- [189] R. Henry, A. Herzberg, and A. Kate, "Blockchain access privacy: Challenges and directions," *IEEE Secur. Privacy*, vol. 16, no. 4, pp. 38–45, Jul. 2018.
- [190] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018.
- [191] B. Dickson, *How Blockchain Can Change the Future of IoT*. Accessed: Apr. 30, 2022. [Online]. Available: <https://venturebeat.com/2016/11/20/how-blockchain-can-change-the-future-of-IoT>
- [192] D. He, S. Chan, and M. Guizani, "Security in the Internet of Things supported by mobile edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 56–61, Aug. 2018.
- [193] O. Alphand, M. Amoretti, T. Claeys, A. Duda, G. Ferrari, F. Rousseau, B. Tourancheau, L. Veltri, and F. Zanichelli, "IoT chain: A blockchain security architecture for the Internet of Things," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6.
- [194] D. Koo, Y. Shin, J. Yun, and J. Hur, "An online data-oriented authentication based on Merkle tree with improved reliability," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Jun. 2017, pp. 840–843.
- [195] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, "A blockchain based privacy-preserving incentive mechanism in crowdsensing applications," *IEEE Access*, vol. 6, pp. 17545–17556, 2018.
- [196] M. C. Muñoz, M. Moh, and T.-S. Moh, "Improving smart grid security using Merkle trees," in *Proc. IEEE Conf. Commun. Netw. Secur.*, Oct. 2014, pp. 522–523.
- [197] Oodles, *Will IOTA Blockchain Solution Secure Internet of Things Ecosystem?* Accessed: Jun. 15, 2022. [Online]. Available: <https://blockchain.oodles.io/blog/blockchain-solution-IoTa-IoT-security>
- [198] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Securing fog computing for Internet of Things applications: Challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 601–628, 1st Quart., 2018.
- [199] V. K. Sehgal, A. Patrick, A. Soni, and L. Rajput, "Smart human security framework using Internet of Things, cloud and fog computing," in *Intelligent Distributed Computing*. Cham, Switzerland: Springer, 2015, pp. 251–263.
- [200] S. Sarkar and S. Misra, "Theoretical modelling of fog computing: A green computing paradigm to support IoT applications," *IET Netw.*, vol. 5, no. 2, pp. 23–29, 2016.
- [201] B. Varghese, N. Wang, D. S. Nikolopoulos, and R. Buyya, "Feasibility of fog computing," in *Handbook of Integration of Cloud Computing, Cyber Physical Systems and Internet of Things*. Cham, Switzerland: Springer, 2020, pp. 127–146.
- [202] IoT Agenda, *IoT and Big Data Analytics*. Accessed: Sep. 17, 2022. [Online]. Available: <https://internetofothingsagenda.techtarget.com>
- [203] R. V. Kulkarni and G. K. Venayagamoorthy, "Neural network based secure media access control protocol for wireless sensor networks," in *Proc. Int. Joint Conf. Neural Netw.*, Jun. 2009, pp. 1680–1687.
- [204] R. Oulhiq, S. Ibntahir, M. Sebgui, and Z. Guennoun, "A fingerprint recognition framework using artificial neural network," in *Proc. 10th Int. Conf. Intell. Syst., Theories Appl. (SITA)*, Oct. 2015, pp. 1–6.
- [205] K. Pavani and A. Damodaram, "Intrusion detection using MLP for MANETS," in *Proc. 3rd Int. Conf. Comput. Intell. Inf. Technol. (CIIT)*, Oct. 2013, pp. 440–444.
- [206] L. Xiao, C. Xie, T. Chen, H. Dai, and H. V. Poor, "A mobile of loading game against smart attacks," *IEEE Access*, vol. 4, pp. 2281–2291, 2016.
- [207] L. Xiao, Q. Yan, W. Lou, G. Chen, and Y. T. Hou, "Proximity-based security techniques for mobile users in wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2089–2100, Dec. 2013.
- [208] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.
- [209] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, Aug. 2016.
- [210] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?" *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 41–49, Sep. 2018.
- [211] L. Xiao, X. Wan, and Z. Han, "PHY-layer authentication with multiple landmarks with reduced overhead," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1676–1687, Mar. 2017.
- [212] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, Jun. 2014.
- [213] C. Li and G. Wang, "A light-weight commodity integrity detection algorithm based on Chinese remainder theorem," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 1018–1023.
- [214] K. Spirina, *Biometric Authentication: The Future of IoT Security Solutions*. Accessed: Jul. 9, 2022. [Online]. Available: <https://www.IoTevolutionworld.com/IoT/articles/438690-biometricauthenticationfuture-IoT-security-solutions.html>
- [215] A. I. Awad, "Machine learning techniques for fingerprint identification: A short review," in *Proc. Int. Conf. Adv. Mach. Learn. Technol. Appl.* Cham, Switzerland: Springer, 2012, pp. 524–531.
- [216] N. A. Alias and N. H. M. Radzi, "Fingerprint classification using support vector machine," in *Proc. 5th ICT Int. Student Project Conf. (ICT-ISPC)*, May 2016, pp. 105–108.
- [217] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Secure data sharing and searching at the edge of cloud-assisted Internet of Things," *IEEE Cloud Comput.*, vol. 4, no. 1, pp. 34–42, Jan. 2017.
- [218] M. Alrowaily and Z. Lu, "Secure edge computing in IoT systems: Review and case studies," in *Proc. IEEE/ACM Symp. Edge Comput. (SEC)*, Oct. 2018, pp. 440–444.
- [219] Y. Li and S. Wang, "An energy-aware edge server placement algorithm in mobile edge computing," in *Proc. IEEE Int. Conf. Edge Comput. (EDGE)*, Jul. 2018, pp. 66–73.
- [220] E. Oyekanlu, C. Nelatury, A. O. Fatade, O. Alaba, and O. Abass, "Edge computing for industrial IoT and the smart grid: Channel capacity for M2M communication over the power line," in *Proc. IEEE 3rd Int. Conf. Electro-Technol. Nat. Develop. (NIGERCON)*, Nov. 2017, pp. 1–11.
- [221] G. Premsankar, M. Di Francesco, and T. Taleb, "Edge computing for the Internet of Things: A case study," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1275–1284, Apr. 2018.
- [222] L. Rosencrance, *Significant Issues That Edge Computing in IoT Solves*. Accessed: Jan. 6, 2019. [Online]. Available: <https://internetofothingsagenda.techtarget.com/feature/6-significantissues-that-edge-computing-in-IoT-solves>
- [223] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450–465, Feb. 2018.
- [224] R. Ullah, S. H. Ahmed, and B. Kim, "Information-centric networking with edge computing for IoT: Research challenges and future directions," *IEEE Access*, vol. 6, pp. 73465–73488, 2018.
- [225] W. Gao, W. G. Hatcher, and W. Yu, "A survey of blockchain: Techniques, applications, and challenges," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2018, pp. 1–11.
- [226] V. G. Shankar, G. Somani, M. S. Gaur, V. Laxmi, and M. Conti, "AndroTaint: An efficient Android malware detection framework using dynamic taint analysis," in *Proc. ISEA Asia Secur. Privacy (ISEASP)*, Jan. 2017, pp. 1–13.
- [227] S. Alam, Z. Qu, R. Riley, Y. Chen, and V. Rastogi, "DroidNative: Automating and optimizing detection of Android native code malware variants," *Comput. Secur.*, vol. 65, pp. 230–246, Mar. 2016, doi: 10.1016/j.cose.2016.11.011.
- [228] E. Gandotra, D. Bansal, and S. Sofat, "Zero-day malware detection," in *Proc. 6th Int. Symp. Embedded Comput. Syst. Design (ISED)*, Dec. 2016, pp. 171–175.
- [229] D. Li, Z. Wang, L. Li, Z. Wang, Y. Wang, and Y. Xue, "FgDetector: Fine-grained Android malware detection," in *Proc. IEEE 2nd Int. Conf. Data Sci. Cyberspace (DSC)*, Jun. 2017, pp. 311–318.
- [230] F. Ghaffari, M. Abadi, and A. Tajoddin, "AMD-EC: Anomaly-based Android malware detection using ensemble classifiers," in *Proc. Iranian Conf. Electr. Eng. (ICEE)*, May 2017, pp. 2247–2252.
- [231] F. Tong and Z. Yan, "A hybrid approach of mobile malware detection in Android," *J. Parallel Distrib. Comput.*, vol. 103, pp. 22–31, May 2017.
- [232] H. Liang, Y. Song, and D. Xiao, "An end-to-end model for Android malware detection," in *Proc. IEEE Int. Conf. Intell. Secur. Informat. (ISI)*, Jul. 2017, pp. 140–142.

- [233] P. Palumbo, L. Sayfullina, D. Komashinskiy, E. Eirola, and J. Karhunen, "A pragmatic Android malware detection procedure," *Comput. Secur.*, vol. 70, pp. 689–701, Sep. 2017.
- [234] A. Feizollah, N. B. Anuar, R. Salleh, G. Suarez-Tangil, and S. Furnell, "AndroDialysis: Analysis of Android intent effectiveness in malware detection," *Comput. Secur.*, vol. 65, pp. 121–134, Mar. 2017.
- [235] F. Shen, J. Del Vecchio, A. Mohaisen, S. Y. Ko, and L. Ziarek, "Android malware detection using complex-flows," *IEEE Trans. Mobile Comput.*, vol. 18, no. 6, pp. 1231–1245, Jun. 2018.
- [236] H. M. Hamad and M. Al-Hoby, "Managing intrusion detection as a service in cloud networks," *Manag. Intrusion Detection Service Cloud Netw.*, vol. 41, no. 1, pp. 35–40, 2012.
- [237] S. Chandrasekhar and M. Singhal, "Efficient and scalable query authentication for cloud-based storage systems with multiple data sources," *IEEE Trans. Services Comput.*, vol. 10, no. 4, pp. 520–533, Nov. 2015.
- [238] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 76, pp. 37–48, Dec. 2016.
- [239] 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.
- [240] C. Li, Z. Qin, E. Novak, and Q. Li, "Securing SDN infrastructure of IoT-fog networks from MitM attacks," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1156–1164, Oct. 2017.
- [241] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1900–1910, May 2018.
- [242] A. Wasef and X. Shen, "EMAP: Expedite message authentication protocol for vehicular ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 12, no. 1, pp. 78–89, Jan. 2013.
- [243] C.-K. Chu, S. S. M. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 468–477, Feb. 2014.
- [244] M. Naveed, M. Prabhakaran, and C. A. Gunter, "Dynamic searchable encryption via blind storage," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 639–654.
- [245] D. Boneh, E. J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *Proc. Theory Cryptogr. Conf.* Cham, Switzerland: Springer, 2005, pp. 325–341.
- [246] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Int. Conf. Theory Appl. Cryptogr. Techn.* Cham, Switzerland: Springer, 1999, pp. 223–238.
- [247] B. Cavallo, G. Di Crescenzo, D. Kahrobaei, and V. Shpilrain, "Efficient and secure delegation of group exponentiation to a single server," in *Proc. Int. Workshop Radio Freq. Identificat., Secur. Privacy Issues*. Cham, Switzerland: Springer, 2015, pp. 156–173.
- [248] C. Papamanthou, E. Shi, and R. Tamassia, "Signatures of correct computation," in *Proc. Theory Cryptogr. Conf.* Cham, Switzerland: Springer, 2013, pp. 222–242.
- [249] S. G. Choi, J. Katz, R. Kumaresan, and C. Cid, "Multi-client noninteractive verifiable computation," in *Proc. Theory Cryptogr. Conf.* Cham, Switzerland: Springer, 2013, pp. 499–518.
- [250] G. Zhuo, Q. Jia, L. Guo, M. Li, and P. Li, "Privacy-preserving verifiable data aggregation and analysis for cloud-assisted mobile crowdsourcing," in *Proc. IEEE 35th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Apr. 2016, pp. 1–9.
- [251] S. D. Gordon, J. Katz, F.-H. Liu, E. Shi, and H.-S. Zhou, "Multi-client verifiable computation with stronger security guarantees," in *Proc. Theory Cryptogr. Conf.* Cham, Switzerland: Springer, 2015, pp. 144–168.
- [252] K. Elkhiyouri, M. Önen, M. Azraoui, and R. Molva, "Efficient techniques for publicly verifiable delegation of computation," in *Proc. 11th ACM Asia Conf. Comput. Commun. Secur.*, May 2016, pp. 119–128.
- [253] B. Cavallo, G. Di Crescenzo, D. Kahrobaei, and V. Shpilrain, "Efficient and secure delegation of group exponentiation to a single server," in *Proc. Int. Workshop Radio Freq. Identificat., Secur. Privacy Issues*. Cham, Switzerland: Springer, 2015, pp. 156–173.
- [254] T. Wang, J. Zeng, M. Z. A. Bhuiyan, H. Tian, Y. Cai, Y. Chen, and B. Zhong, "Trajectory privacy preservation based on a fog structure for cloud location services," *IEEE Access*, vol. 5, pp. 7692–7701, 2017.
- [255] L. Li, R. Lu, K.-K.-R. Choo, A. Datta, and J. Shao, "Privacy-preserving-outsourced association rule mining on vertically partitioned databases," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1847–1861, Aug. 2016.
- [256] X. Liu, R. H. Deng, Y. Yang, H. N. Tran, and S. Zhong, "Hybrid privacy-preserving clinical decision support system in fog-cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 825–837, Jan. 2018.
- [257] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 308–318.
- [258] T. Zhang and Q. Zhu, "Dynamic differential privacy for ADMM-based distributed classification learning," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 172–187, Jan. 2017.
- [259] Z. Qin, Y. Yang, T. Yu, I. Khalil, X. Xiao, and K. Ren, "Heavy hitter estimation over set-valued data with local differential privacy," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 192–203.
- [260] J. Zhang, Q. Li, X. Wang, B. Feng, and D. Guo, "Towards fast and lightweight spam account detection in mobile social networks through fog computing," *Peer-Peer Netw. Appl.*, vol. 11, no. 4, pp. 778–792, 2018.
- [261] 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.
- [262] A. Alotaibi, A. Barnawi, and M. Buhari, "Attribute-based secure data sharing with efficient revocation in fog computing," *J. Inf. Secur.*, vol. 8, no. 3, pp. 203–222, 2017.
- [263] Y. Jiang, W. Susilo, Y. Mu, and F. Guo, "Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 720–729, Jan. 2017.
- [264] Z. Yu, M. H. Au, Q. Xu, R. Yang, and J. Han, "Towards leakage-resilient fine-grained access control in fog computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 763–777, Jan. 2018.
- [265] C. Lee, S. Chiu, and S. Chen, "Time-bound keyaggregate encryption for cloud storage," *Secur. Commun. Netw.*, vol. 9, no. 13, pp. 2059–2069, 2016.
- [266] 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, pp. 1–14, 2017.
- [267] P. Rizomiliotis and S. Gritzalis, "ORAM based forward privacy preserving dynamic searchable symmetric encryption schemes," in *Proc. ACM Workshop Cloud Comput. Secur. Workshop*, 2015, pp. 65–76.
- [268] S. Chandrasekhar and M. Singhal, "Efficient and scalable query authentication for cloud-based storage systems with multiple data sources," *IEEE Trans. Services Comput.*, vol. 10, no. 4, pp. 520–533, Nov. 2015.
- [269] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 76, pp. 37–48, Dec. 2016.
- [270] J. Zhou, X. Lin, X. Dong, and Z. Cao, "PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributedm-healthcare cloud computing system," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 6, pp. 1693–1703, Jun. 2015.
- [271] D. Pointcheval and O. Sanders, "Short randomizable signatures," in *Proc. Cryptogr. Track RSA Conf.* Cham, Switzerland: Springer, 2016, pp. 111–126.
- [272] S. Saloniakas, I. Mavridis, and D. Gritzalis, "Access control issues in utilizing fog computing for transport infrastructure," in *Proc. Int. Conf. Crit. Inf. Infrastruct. Secur.* Cham, Switzerland: Springer, 2015, pp. 15–26.
- [273] J. Ni, X. Lin, K. Zhang, Y. Yu, and X. S. Shen, "Device-invisible two-factor authenticated key agreement protocol for BYOD," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Jul. 2016, pp. 1–6.
- [274] J. Ni, K. Zhang, K. Alharbi, X. Lin, N. Zhang, and X. S. Shen, "Differentially private smart metering with fault tolerance and range-based filtering," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2483–2493, Sep. 2017.
- [275] R. Lu, K. Heung, A. H. Lashkari, and A. A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.
- [276] H. Wang, Z. Wang, and J. Domingo-Ferrer, "Anonymous and secure aggregation scheme in fog-based public cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 712–719, Jan. 2018.
- [277] J. Zhou, Z. Cao, X. Dong, and X. Lin, "Security and privacy in cloud-assisted wireless wearable communications: Challenges, solutions, and future directions," *IEEE Wireless Commun.*, vol. 22, no. 2, pp. 136–144, Apr. 2015.

- [278] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "EDAT: Efficient data aggregation without TTP for privacy-assured smart metering," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.
- [279] J. Ni, X. Lin, K. Zhang, and Y. Yu, "Secure and deduplicated spatial crowdsourcing: A fog-based approach," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.
- [280] X. Liang, X. Lin, and X. S. Shen, "Enabling trustworthy service evaluation in service-oriented mobile social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 310–320, Feb. 2014.
- [281] D. J. Wu, A. Taly, A. Shankar, and D. Boneh, "Privacy, discovery, and authentication for the Internet of Things," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2016, pp. 301–319.
- [282] M. Agrawal and P. Mishra, "A comparative survey on symmetric key encryption techniques," *Int. J. Comput. Sci. Eng.*, vol. 4, no. 5, pp. 877–882, 2012.



NAQASH AZEEM KHAN (Member, IEEE) received the B.Sc. degree in electronics from the University of Haripur, Pakistan, in 2015, and the M.Sc. degree in electrical engineering from COMSATS University Islamabad, Pakistan, in 2019. He is currently a Ph.D. Scholar in the Department of Electrical and Electronic Engineering, Universiti Teknologi PETRONAS (UTP), Malaysia. Since 2022, he has been a Graduate Assistant with the Integrated Circuit Design Laboratory, where he

is currently working on the cryptography and information security techniques for the security of the Internet of Things. His research interests include information security, data encryption, the Internet of Things, network and computer security, and wireless communication. He has been serving as a reviewer for many well-reputed journals and conferences.



AZLAN AWANG (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering from Polytechnic University (now NYU Tandon School of Engineering), Brooklyn, NY, USA, in 1989 and 1990, respectively, and the joint Ph.D. degree from IMT Atlantique Télécom Bretagne and University Rennes 1, Rennes, France, in 2011. Since 2004, he has been with the Department of Electrical and Electronic Engineering, Universiti Teknologi PETRONAS (UTP),

where he is currently an Associate Professor. Prior to joining UTP, he was with Motorola Malaysia Sdn Bhd, in 1991, Schlumberger Overseas S.A., from 1992 to 1993, Alcatel Networks Systems Malaysia Sdn Bhd, from 1994 to 2001, and Universiti Teknologi MARA, from 2002 to 2003. At UTP, he has been active in research and also with the Center of Systems Engineering, Institute of Autonomous Systems. His research interests include the design of energy-efficient, cross-layer medium access control and routing protocol for vehicular *ad-hoc* networks, wireless sensor networks, and the Internet of Things. He is also a member of the IEEE-Eta Kappa Nu and Tau Beta Pi Engineering Honor Societies and a Chartered Engineer with the Engineering Council, U.K. He received one of the two best paper awards in MICC2013 (20 years of MICC, from 1993 to 2013).



SAMSUL ARIFFIN ABDUL KARIM received the Ph.D. degree in mathematics from Universiti Sains Malaysia (USM). He is currently an Associate Professor with Software Engineering Programme, Faculty of Computing and Informatics, Universiti Malaysia Sabah (UMS), Malaysia. He is also a Professional Technologists registered with the Malaysia Board of Technologists (MBOT), No. Perakuan PT21030227. He has published more than 160 papers in journals and conferences, including three edited conferences volume and 80 book chapters. His research interests include numerical analysis, machine learning, approximation theory, optimization, science, and engineering education and wavelets. He was a recipient of Effective Education Delivery Award and Publication Award (journals and conference papers), UTP Quality Day, in 2010, 2011, and 2012, respectively. He was Certified WOLFRAM Technology Associate, Mathematica Student Level. He also has published 13 books with Springer publishing, including six books with *Studies in Systems, Decision and Control* (SSDC) series, two book with Taylor and Francis/CRC Press, one book with IntechOpen, and one book with UTP Press. Recently, he has received the Book Publication Award in UTP Quality Day 2020 for book Water Quality Index (WQI) Prediction Using Multiple Linear Fuzzy Regression: Case Study in Perak River, Malaysia, that was published by SpringerBriefs in Water Science and Technology, in 2020.

• • •