IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received April 27, 2019, accepted June 10, 2019, date of publication June 20, 2019, date of current version July 10, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2924045

A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures

VIKAS HASSIJA[1], VINAY CHAMOLA[2], VIKAS SAXENA[1], DIVYANSH JAIN[1], PRANAV GOYAL[1], AND BIPLAB SIKDAR[3], (Senior Member, IEEE)

[1]Department of CSE and IT, Jaypee Institute of Information Technology, Noida 201309, India
[2]Department of EEE, Birla Institute of Technology and Science (BITS), Pilani 333031, India
[3]Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583

Corresponding author: Vinay Chamola (vinay.chamola@pilani.bits-pilani.ac.in)

This work was supported in part by the National Research Foundation, Prime Minister's Office, Singapore, through its Corporate Laboratory@University Scheme, in part by the National University of Singapore, and in part by Singapore Telecommunications Ltd.

ABSTRACT The Internet of Things (IoT) is the next era of communication. Using the IoT, physical objects can be empowered to create, receive, and exchange data in a seamless manner. Various IoT applications focus on automating different tasks and are trying to empower the inanimate physical objects to act without any human intervention. The existing and upcoming IoT applications are highly promising to increase the level of comfort, efficiency, and automation for the users. To be able to implement such a world in an ever-growing fashion requires high security, privacy, authentication, and recovery from attacks. In this regard, it is imperative to make the required changes in the architecture of the IoT applications for achieving end-to-end secure IoT environments. In this paper, a detailed review of the security-related challenges and sources of threat in the IoT applications is presented. After discussing the security issues, various emerging and existing technologies focused on achieving a high degree of trust in the IoT applications are discussed. Four different technologies, blockchain, fog computing, edge computing, and machine learning, to increase the level of security in IoT are discussed.

INDEX TERMS Internet of Things (IoT), IoT security, blockchain, fog computing, edge computing, machine learning, IoT applications, distributed systems.

I. INTRODUCTION

The pace of connecting physical devices around us to the Internet is increasing rapidly. According to a recent Gartner report, there will be around 8.4 billion connected things worldwide in 2020. This number is expected to grow to 20.4 billion by 2022 [1]. The use of IoT applications is increasing in all parts of the world. The major driving countries in this include western Europe, North America, and China [1]. The number of machine to machine (M2M) connections is expected to grow from 5.6 billion in 2016 to 27 billion in 2024 [1]. This leap in numbers itself declares IoT to be one of the major upcoming markets that could form a cornerstone of the expanding digital economy. The IoT industry is expected to grow in terms of revenue from $892 billion in 2018 to $4 trillion by 2025 [2]. M2M connections cover a broad range of applications like smart cities, smart environment, smart grids, smart retail, smart farming, etc. [3]. Figure 1 shows the past, present and future architecture of IoT. In future, the devices are not only expected to be connected to the Internet and other local devices but are also expected to communicate with other devices on the Internet directly. Apart from the devices or things being connected, the concept of social IoT (SIoT) is also emerging. SIoT will enable different social networking users to be connected to the devices and users can share the devices over the Internet [4].

With all this vast spectrum of IoT applications comes the issue of security and privacy. Without a trusted and interoperable IoT ecosystem, emerging IoT applications cannot reach high demand and may lose all their potential. Along with the security issues faced generally by the Internet, cellular networks, and WSNs, IoT also has its special security challenges such as privacy issues, authentication issues, management issues, information storage and so on. Table 1 summarizes various factors due to which securing IoT environment is

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

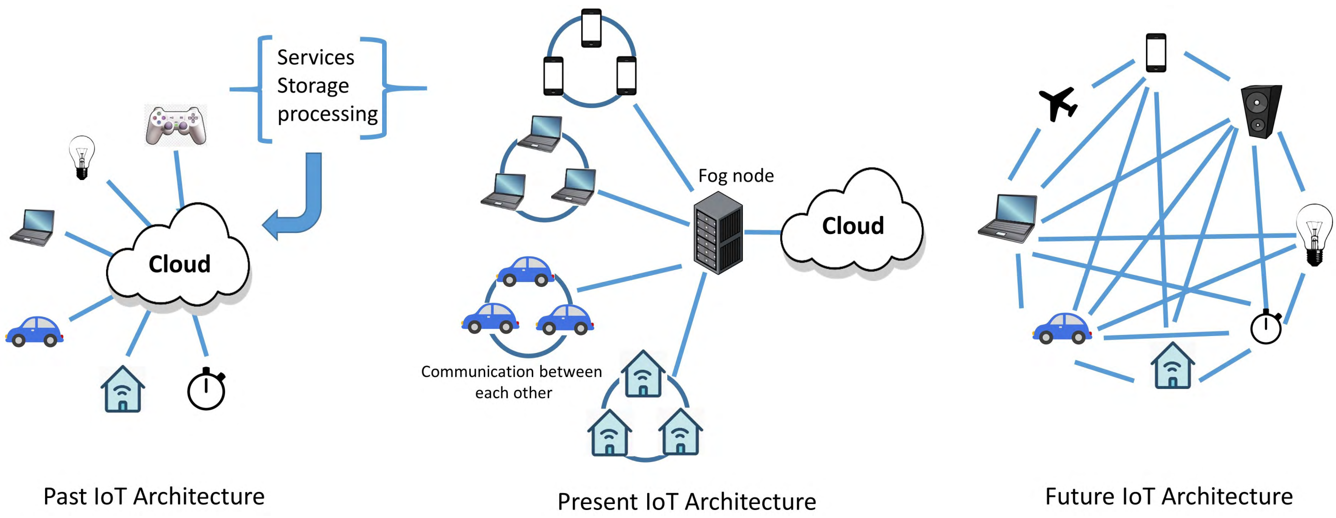


FIGURE 1. Present and future architecture of IoT.

TABLE 1. Comparison of security of IT devices and IoT devices.

Widespread IT Security	IoT security
Widespread IT has devices which is resource rich	IoT devices need to be carefully provisioned with security measures
Widespread IT is based on resource rich devices	IoT system are composed of devices having limitation in terms of their software and hardware
For wide security and lower capabilities complex algorithm are implemented	only lightweight algorithms are preferred
Homogeneous technology is responsible for high security	IoT with heterogeneous technology produce large amount of heterogeneous data increasing the attack surface

much more challenging than securing normal information technology (IT) devices. Due to all these issues and vulnerabilities, the IoT applications create a fertile ground for different kinds of cyber threats. There have been various security and privacy attacks on the already deployed IoT applications worldwide. Mirai attack in the last quarter of 2016 was estimated to infect around 2.5 million devices connected to the Internet and launch distributed denial of service (DDoS) attack [5]. After Mirai, Hajime and Reaper are the other big botnet attacks launched against a large number of IoT devices [5]. IoT devices, being low powered and less secure, provide a gateway to the adversaries for entering into home and corporate networks, thereby giving easy access to the user's data. Also, the domain of IoT is expanding beyond mere things or objects. There have been various successful attempts to implant IoT devices into the human body to monitor the live condition of various organs [6]. Attackers can target such devices to track the location of a particular individual or falsify data. Such an attack has not taken place yet in real life but can be highly dangerous, if such devices are compromised.

Cyber Physical Systems (CPS) is another area benefitting from the growth of IoT. In CPS physical objects in the environment are monitored, and actions are taken based on the physical changes. Since CPS encompass assets of critical importance (e.g., power grids, transportation systems), security vulnerabilities in such systems have serious consequences. However, security challenges for CPS have their unique characteristics and are outside the scope of this paper.

In any IoT ecosystem or environment, there are four important layers. The first layer includes the use of various sensors and actuators to perceive the data or information to perform various functionalities. Based on that, in the second layer, a communication network is used to transmit the collected data. Most of the evolving IoT applications deploy the third layer, called a middleware layer, to act as a bridge between the network and application layer. Finally, on the fourth layer, there are various IoT based end-to-end applications like smart grids, smart transport, smart factories, etc. All of these four layers have security problems specific to them. Apart from these layers, various gateways connect these layers and help in the data movement. There are certain security threats specific to these gateways as well.

In this paper, a detailed survey of IoT security solutions in the existing literature is presented. First of all, the fundamental constraints to achieve high levels for security in IoT

TABLE 2. Related surveys on IoT security.

Year	Author	Contributions
2016	Arsalan Mosenia et al., [7]	A brief discussion of vulnerabilities faced by the edge side layer of IoT
2017	Yu wei et al., [8]	Survey on using Edge Computing to secure IoT
2017	Jie Lin ea al., [9]	Discussion on relationship between IoT and Fog Computing
2017	Y yang et al., [10]	A brief discussion on most relevant limitations of IoT devices
2017	L chen , S. Thombre et al., [11]	security issues specific to location-based services in IoT
2017	A H Ngu, V. Metsis et al., [12]	Security issues related to the IoT middle ware
2018	I Farris, T Taleb et al., [13]	Security mechanism for IoT security like SDN and NFB
2019	Ikram Ud din, M. Guizani et al,. [14]	Trust Management Techniques for Internet of Things

applications are presented. The goal of this paper is to highlight the major existing and upcoming solutions for IoT security. Specifically, the four major classes of IoT security solutions namely: (1) blockchain based solutions; (2) fog computing based solutions; (3) machine learning based solutions and (4) edge computing based solutions are highlighted. Table 3 gives a list of acronyms related to IoT used in this paper.

A. RELATED SURVEYS AND OUR CONTRIBUTIONS

There are various existing surveys on IoT security and privacy issues. Yuchen *et al.* [10] have summarized various security issues in IoT applications. Authors of [11] have discussed the security issues specific to location-based services in IoT. The authors target the particular problems related to localization and positioning of the IoT devices. Anne et al. in [12] focus mainly on the security issues related to IoT middleware and provide a detailed survey of related existing protocols and their security issues. M. Guizani et al. in [14] have surveyed various trust management techniques for IoT along with their pros and cons. Security mechanisms for IoT security such as software defined networking (SDN) and network function virtualization (NFV) are discussed in [13]. In [8] the authors have compared edge computing with traditional cloud systems to secure IoT systems. Jie Lin et al. in [9] have discussed the relationship between IoT and fog computing. Some of the security issues related to fog computing have also been discussed. Authors of [7] have discussed vulnerabilities faced by IoT in brief. Table 2 summarizes the main contributions of the previous comprehensive surveys on IoT security. Although there are several works in this direction, they are specific to certain limited aspects of IoT. This calls the need for a detailed survey on all the existing and upcoming security challenges in IoT applications. This paper will help the reader to get a detailed idea of the state-of-the-art in IoT security and will give them a general understanding of the area. The main contributions of this work are as follows:

1. A classification of different IoT applications and specific security and privacy issues related to those applications.
2. A detailed explanation of different threat sources in different layers of IoT.
3. Detailed and realistic recommendations to improve the IoT infrastructure to facilitate secure communications.
4. Review on the proposed countermeasures to the security issues in IoT.
5. An assessment of the open issues, challenges and future research directions for developing secure IoT applications.

TABLE 3. 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	Decentalized Autonomous Organizations
DDoS	Distributed denial of service
GPS	Global Positioning System
HAN	Home Area Network
IIoT	Industrial Internet of Things
IOE	Internet of Everything
IoT	Internet of Things
M2M	Machine to Machine
MCC	Mobile Cloud Computing
MEC	Mobile Edge Computing
MLP	Multi-Layer Perceptron
MQTT	Message Queuing Telemetry Transport
NFC	Near Field Communication
NFV	Network Function Virtualization
P2P	peer to peer
QoS	Quality of Service
RFID	Radio Frequency Identification
RSN	RFID sensor Networks
SDN	Software-Defined Networking
SHA	Secure Hash Algorithm
SIoT	Social Internet of Things
SMQTT	Secure Message Queue Telemetry Transport
STD	Security Trust and Decentralization
WSN	Wireless Sensor Networks
XMPP	Extensible Messaging and Presence Protocol
XSS	cross-site scripting

B. ORGANIZATION

The organization of the rest of the paper is as follows: Section II describes various application areas of IoT where high security is required. Section III discusses various sources of threats in an IoT environment. In section IV various constraints and requirements to be considered while developing a secure IoT application are reviewed. Four major IoT security approaches, i.e., blockchain, fog computing, machine learning, and edge computing are presented in Section V, VI, VII, and VIII, respectively. Section IX describes various open issues, challenges and upcoming research opportunities in IoT security and finally, Section X concludes the paper.

II. SECURITY CRITICAL APPLICATION AREAS OF IoT

Security is highly critical in almost all IoT applications that have already been deployed or are in the process of deployment. The applications of IoT are increasing very rapidly and penetrating most of the existing industries. Although operators support these IoT applications through existing networking technologies, several of these applications need more stringent security support from technologies they use. In this section various security critical IoT applications are discussed.

1. **Smart Cities:** Smart cities involve extensive use of emerging computation and communication resources for increasing the overall quality of life of the people [15]. It includes smart homes, smart traffic management, smart disaster management, smart utilities, etc. There is a push to make cities smarter, and governments worldwide are encouraging their development through various incentives [16]. Although the use of smart applications is intended to improve the overall quality of life of the citizens, it comes with a threat to the privacy of the citizens. Smart card services tend to put the card details and purchase behavior of the citizens at risk. Smart mobility applications may leak the location traces of the users. There are applications using which parents can keep track of their child. However, if such applications are hacked, then the safety of the child can come to risk.
2. **Smart Environment:** Smart environment includes various IoT applications such as fire detection in forests, monitoring the level of snow in high altitude regions, preventing landslides, early detection of earthquakes, pollution monitoring, etc. All these IoT applications are closely related to the life of human beings and animals in those areas. The government agencies involved in such fields will also be relying on the information from these IoT applications. Security breaches and vulnerability in any area related to such IoT applications can have serious consequences. In this context, both false negatives and false positives can lead to disastrous results for such IoT applications. For example, if the application starts detecting earthquakes falsely, then it will lead to monetary losses for the government and businesses. On the other hand, if the application is not able to predict the earthquake, then it will lead to the loss of both property and life. Therefore, smart environment applications have to be highly precise, and security breaches and data tampering must be avoided.
3. **Smart Metering and Smart Grids:** Smart metering includes applications related to various measurements, monitoring, and management. The most common application of smart metering is smart grids, where the electricity consumption is measured and monitored. Smart metering may also be used to address the problem of electricity theft [17]. Other applications of smart metering include monitoring of water, oil and gas levels in storage tanks and cisterns. Smart meters are also used to monitor and optimize the performance of solar energy plants by dynamically changing the angle of solar panels to harvest the maximum possible solar energy. There also exist some IoT applications that use smart meters to measure the water pressure in water transport systems or to measure the weight of goods. However, smart metering systems are vulnerable to both physical and cyber-attacks as compared to analog meters that can be tampered only by physical attacks. Also, smart meters or advanced metering infrastructure (AMI) are intended to perform functions beyond generic energy usage recording. In a smart home area network (HAN) all electric equipment at home are connected to smart meters and the information collected from these equipments can be used for load and cost management. Intentional intrusion in such communication systems by the consumer or an adversary may modify the collected information, leading to monetary loss for the service providers or consumers [18].
4. **Security and Emergencies:** Security and emergencies is another important area where various IoT applications are being deployed. It includes applications such as allowing only authorized people in restricted areas etc. Another application in this domain is the detection of leakage of hazardous gases in industrial areas or areas around chemical factories. Radiation levels can also be measured in the areas around nuclear power reactors or cellular base stations and alerts can be generated when the radiation level is high. There are various buildings whose systems have sensitive data or that house sensitive goods. Security applications can be deployed to protect sensitive data and goods. IoT applications that detect various liquids can also be used to prevent corrosion and break downs in such sensitive buildings. Security breaches in such applications can also have various serious consequences. For example, the criminals may try to enter the restricted areas by attacking the vulnerabilities in such applications. Also, false radiation level alarms can have serious immediate and long term impacts. For example, if infants are exposed to high levels of radiation, then it may lead to serious life threatening diseases in long term.

5. **Smart Retail:** IoT applications are being extensively used in the retail sector. Various applications have been developed to monitor the storage conditions of the goods as they move along the supply chain. IoT is also being used to control the tracking of products in the warehouses so that restocking can be done optimally. Various intelligent shopping applications are also being developed for assisting the customers based on their preferences, habits, allergies to certain components, etc. Mechanisms to provide the experience of online shopping to offline retailers using augmented reality techniques have also been developed. Various companies in retail have faced security issues in deploying and using various IoT applications. Some of these companies include Apple, Home Depot, JP Morgan Chase and Sony [19]. Adversaries may try to compromise the IoT applications associated with storage conditions of the goods and may try to send wrong information about the products to the users in order to increase the sale. If security features are not implemented in smart retail, attackers may steal debit and credit card information, phone numbers, email-addresses, etc. of the customers which can lead to monetary losses for the customers and retailers.
6. **Smart Agriculture and Animal Farming:** Smart agriculture includes monitoring soil moisture, controlling micro-climate conditions, selective irrigation in dry zones, and controlling humidity and temperature. Usage of such advanced features in agriculture can help in achieving high yields and can save farmers from monetary losses. Control of temperature and humidity levels in various grain and vegetable production can help in preventing fungus and other microbial contaminants. Controlling the climate conditions can also help in increasing the vegetable and crop yield and quality. Just like crop monitoring, there are IoT applications to monitor the activities and the health condition of farm animals by attaching sensors to the animals. If such applications are compromised, then it may lead to the theft of animals from the farm and adversaries may also damage the crops.
7. **Home Automation:** Home automation is one of the most widely used and deployed IoT applications. This includes applications such as those for remotely controlling electrical appliances to save energy, systems deployed on windows and doors to detect intruders, etc. Monitoring systems are being applied to track energy and water supply consumption, and users are being advised to save cost and resources. Authors in [20] have proposed the use of logic based security algorithms to enhance security level in homes. Intrusions are detected by comparing the user actions at key locations of the home with normal behavior of the user in these locations. However, attackers may gain unauthorized access of the IoT devices in the home and try to harm the users. For instance, cases of home burglaries have increased rapidly after the deployment of various home automation systems [20]. There have also been various cases in the past where the adversaries try to analyze the type and volume of Internet traffic to/from the smart home for judging the behavior and presence of the residents.

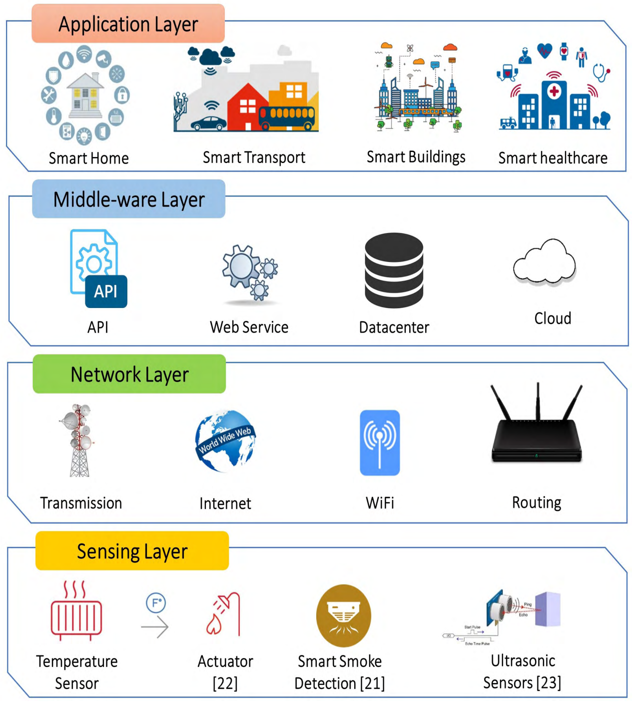


FIGURE 2. Layers in IoT system.

III. SOURCES OF SECURITY THREATS IN IoT APPLICATIONS

As discussed in Section I, any IoT application can be divided into four layers: (1) sensing layer; (2) network layer; (3) middleware layer; and (4) application layer. Each of these layers in an IoT application uses diverse technologies that bring a number of issues and security threats. Figure 2 shows various technologies, devices, and applications at these four layers. This section discusses various possible security threats in IoT applications for these four layers. Figure 3 shows the possible attacks on these four layers. The special security issues associated with the gateways that connect these layers are also discussed in this section.

A. SECURITY ISSUES AT SENSING LAYER

The sensing layer mainly deals with physical IoT sensors and actuators. Sensors sense the physical phenomenon happening around them [21]–[23]. Actuators, on the other hand, perform a certain action on the physical environment, based on the sensed data. There are various kinds of sensors for sensing different kinds of data, e.g., ultrasonic sensors, camera sensors, smoke detection sensors, temperature and humidity sensors, etc. There can be mechanical, electrical, electronic or chemical sensors used to sense the physical environment. Various sensing layer technologies are used in

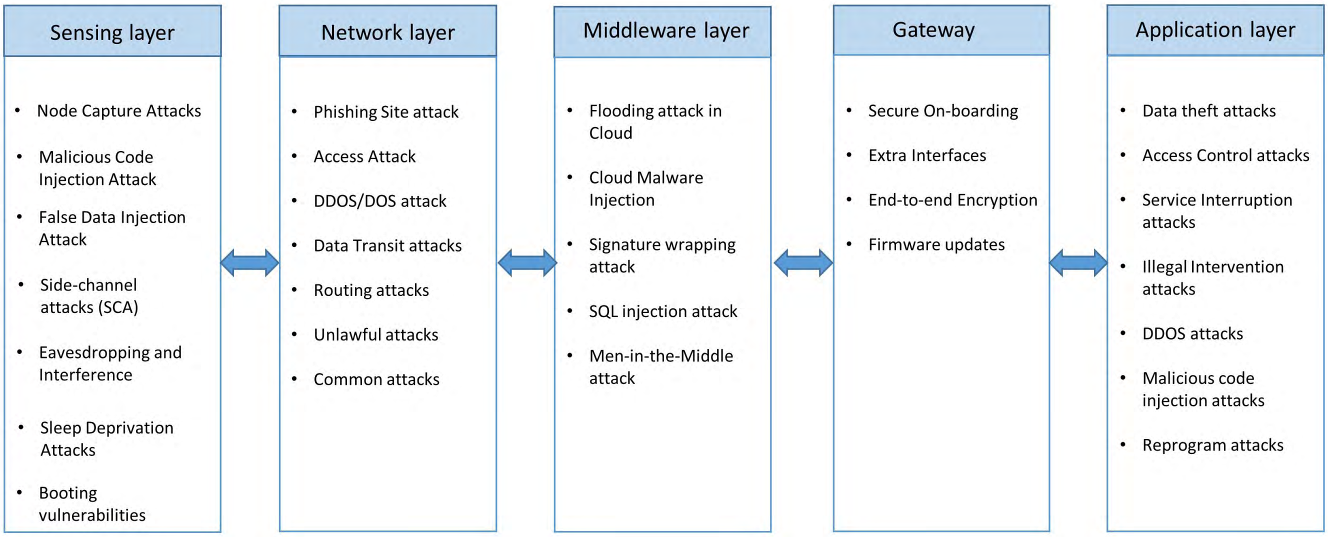


FIGURE 3. Types of attacks on IoT.

different IoT applications like RFID, GPS, WSNs, RSNs, etc. Major security threats that can be encountered at the sensing layer are as follows:

1. **Node Capturing:** IoT applications comprise of several low power nodes such as sensors and actuators. These nodes are vulnerable to a variety of attacks by the adversaries. The attackers may try to capture or replace the node in the IoT system with a malicious node. The new node may appear to be the part of the system but is controlled by the attacker. This may lead to compromising the security of the complete IoT application [24].
2. **Malicious Code Injection Attack:** The attack involves the attacker injecting some malicious code in the memory of the node. Generally, the firmware or software of IoT nodes are upgraded on the air, and this gives a gateway to the attackers to inject malicious code. Using such malicious code, the attackers may force the nodes to perform some unintended functions or may even try to access the complete IoT system.
3. **False Data Injection Attack:** Once the node is captured, the attacker may use it to inject erroneous data onto the IoT system. This may lead to false results and may result in malfunctioning of the IoT application. The attacker may also use this method to cause a DDoS attack.
4. **Side-Channel Attacks (SCA):** Apart from direct attacks on the nodes, various side-channel attacks may lead to leaking of sensitive data. The microarchitectures of processors, electromagnetic emanation and their power consumption reveal sensitive information to adversaries. Side channel attacks may be based on power consumption, laser-based attacks, timing attacks or electromagnetic attacks. Modern chips take care of various countermeasures to prevent these side-channel attacks while implementing the cryptographic modules.
5. **Eavesdropping and Interference:** IoT applications often consist of various nodes deployed in open environments [25]. As a result, such IoT applications are exposed to eavesdroppers. The attackers may eavesdrop and capture the data during different phases like data transmission or authentication.
6. **Sleep Deprivation Attacks:** In such type of attacks the adversaries try to drain the battery of the low-powered IoT edge devices. This leads to a denial of service from the nodes in the IoT application due to a dead battery. This can be done by running infinite loops in the edge devices using malicious code or by artificially increasing the power consumption of the edge devices.
7. **Booting Attacks:** The edge devices are vulnerable to various attacks during the boot process. This is because the inbuilt security processes are not enabled at that point. The attackers may take advantage of this vulnerability and try to attack the node devices when they are being restarted. As edge devices are typically low powered and at times go through sleep-wake cycles, it is thus essential to secure the boot process in these devices.

B. SECURITY ISSUES AT NETWORK LAYER

The key function of the network layer is transmitting the information received from the sensing layer to the computational unit for processing. The major security issues that are encountered at the network layer are as follows.

1. **Phishing Site Attack:** Phishing attacks often refer to attacks where several IoT devices can be targeted by a minimal effort put by the attacker. The attackers expect

that at least few of the devices will become a victim of the attack. There is a possibility of encountering phishing sites in the course of users visiting web pages on the Internet. Once the user's account and password are compromised, the whole IoT environment being used by the user becomes vulnerable to cyber attacks. The network layer in IoT is highly vulnerable to phishing sites attacks [26].

2. **Access Attack:** Access attack is also referred to as advanced persistent threat (APT). This is a type of attack in which an unauthorized person or an adversary gains access to the IoT network. The attacker can continue to stay in the network undetected for a long duration. The purpose or intention of this kind of attack is to steal valuable data or information, rather than to cause damage to the network. IoT applications continuously receive and transfer valuable data and are therefore highly vulnerable to such attacks [27].
3. **DDoS/DoS Attack:** In this kind of attacks, the attacker floods the target servers with a large number of unwanted requests. This incapacitates the target server, thereby disrupting services to genuine users. If there are multiple sources used by the attacker to flood the target server, then such an attack is termed as DDoS or distributed denial of service attack. Such attacks are not specific to IoT applications, but due to the heterogeneity and complexity of IoT networks, the network layer of the IoT is prone to such attacks. Many IoT devices in IoT applications are not strongly configured, and thus become easy gateways for attackers to launch DDoS attacks on the target servers. The Mirai botnet attack as discussed in Section I used this vulnerability and blocked various servers by constantly propagating requests to the weakly configured IoT devices [28].
4. **Data Transit Attacks:** IoT applications deal with a lot of data storage and exchange. Data is valuable, and therefore it is always the target of hackers and other adversaries. Data that is stored in the local servers or the cloud has a security risk, but the data that is in transit or is moving from one location to another is even more vulnerable to cyber attacks. In IoT applications, there is a lot of data movement between sensors, actuators, cloud, etc. Different connection technologies are used in such data movements, and therefore IoT applications are susceptible to data breaches.
5. **Routing Attacks:** In such attacks, malicious nodes in an IoT application may try to redirect the routing paths during data transit. Sinkhole attacks are a specific kind of routing attack in which an adversary advertises an artificial shortest routing path and attracts nodes to route traffic through it. A worm-hole attack is another attack which can become serious security threat if combined with other attacks such as sinkhole attacks. A warm-hole is an out of band connection between two nodes for fast packet transfer. An attacker can create a warm-hole between a compromised node and a device on the internet and try to bypass the basic security protocols in an IoT application.

C. SECURITY ISSUES AT MIDDLEWARE LAYER

The role of the middleware in IoT is to create an abstraction layer between the network layer and the application layer. Middleware can also provide powerful computing and storage capabilities [29]. This layer provides APIs to fulfill the demands of the application layer. Middleware layer includes brokers, persistent data stores, queuing systems, machine learning, etc. Although the middleware layer is useful to provide a reliable and robust IoT application, it is also susceptible to various attacks. These attacks can take control of the entire IoT application by infecting the middleware. Database security and cloud security are other main security challenges in the middleware layer. Various possible attacks in the middleware layer are discussed as follows.

1. **Man-in-the-Middle Attack:** The MQTT protocol uses publish-subscribe model of communication between clients and subscribers using the MQTT broker, which effectively acts as a proxy. This helps in decoupling the publishing and the subscribing clients from each other and messages can be sent without the knowledge of the destination. If the attacker can control the broker and become a man-in-the-middle, then he/she can get complete control of all communication without any knowledge of the clients.
2. **SQL Injection Attack:** MIddleware is also susceptible to SQL Injection (SQLi) attacks. In such attacks, attacker can embed malicious SQL statements in a program [30], [31]. Then, the attackers can obtain private data of any user and can even alter records in the database [32]. Open Web Application Security Project (OWASP) has listed SQLi as a top threat to web security in their OWASP top 10 2018 document [33].
3. **Signature Wrapping Attack:** In the web services used in the middleware, XML signatures are used [34]. In a signature wrapping attack, the attacker breaks the signature algorithm and can execute operations or modify eavesdropped message by exploiting vulnerabilities in SOAP (Simple Object Access Protocol) [35].
4. **Cloud Malware Injection:** In cloud malware injection, the attacker can obtain control, inject malicious code or can inject a virtual machine into the cloud. The attacker pretends to be a valid service by trying to create a virtual machine instance or a malicious service module. In this way, the attacker can obtain access to service requests of the victim's service and can capture sensitive data which can be modified as per the instance.
5. **Flooding Attack in Cloud:** This attack works almost the same as DoS attack in the cloud and affects the quality of service (QoS). For depleting cloud resources, the attackers continuously send multiple requests to a service. These attacks can have a big impact on cloud systems by increasing the load on the cloud servers.

D. SECURITY ISSUES AT GATEWAYS

Gateway is a broad layer that has an important role in connecting multiple devices, people, things and cloud services. Gateways also help in providing hardware and software solutions for IoT devices. Gateways are used for decrypting and encrypting IoT data and translating protocols for communication between different layers [36]. IoT systems today are heterogeneous including LoraWan, ZigBee, Z-Wave and TCP/IP stacks with many gateways in between. Some of the security challenges for IoT gateway are discussed below.

1. **Secure On-boarding:** When a new device or sensor is installed in an IoT system, it is imperative to protect encryption keys. Gateways act as an intermediary between the new devices and the managing services, and all the keys pass through the gateways. The gateways are susceptible to man-in-the-middle attacks and eavesdropping to capture the encryption keys, especially during the on-boarding process.
2. **Extra Interfaces:** Minimizing the attack surface is an important strategy that needs to be kept in mind while installing the IoT devices [37]. Only the necessary interfaces and protocols should be implemented by an IoT gateway manufacturer. Some of the services and functionalities should be restricted for end-users to avoid backdoor authentication or information breach.
3. **End-to-End Encryption:** True end-to-end application layer security is required to ensure the confidentiality of the data [38]. The application should not let anyone other than the unique recipient to decrypt the encrypted messages. Although Zigbee and Zwave protocols support encryption, this is not end-to-end encryption, because, in order to translate the information from one protocol to another, the gateways are required to decrypt and re-encrypt the messages. This decryption at the gateway level makes the data susceptible to data breaches.
4. **Firmware updates:** Most IoT devices are resource constrained, and therefore they do not have an user interface or the computation power to download and install the firmware updates. Generally, gateways are used to download and apply the firmware updates. The current and new version of the firmware should be recorded, and validity of the signatures should be checked for secure firmware updates.

E. SECURITY ISSUES AT APPLICATION LAYER

The application layer directly deals with and provides services to the end users. IoT applications like smart homes, smart meters, smart cities, smart grids, etc. lie in this layer. This layer has specific security issues that are not present in other layers, such as data theft and privacy issues. The security issues in this layer are also specific to different applications. Many IoT applications also consist of a sub-layer between the network layer and application layer, usually termed as an application support layer or middleware layer. The support layer supports various business services and helps in intelligent resource allocation and computation. Major security issues encountered by the application layer are discussed below.

1. **Data Thefts:** IoT applications deal with lot of critical and private data. The data in transit is even more vulnerable to attacks than data at rest, and in IoT applications, there is a lot of data movement. The users will be reluctant to register their private data on IoT applications if these applications are vulnerable to data theft attacks. Data encryption, data isolation, user and network authentication, privacy management, etc. are some of the techniques and protocols being used to secure IoT applications against data thefts.
2. **Access Control Attacks:** Access control is authorization mechanism that allows only legitimate users or processes to access the data or account. Access control attack is a critical attack in IoT applications because once the access is compromised, then the complete IoT application becomes vulnerable to attacks.
3. **Service Interruption Attacks:** These attacks are also referred to as illegal interruption attacks or DDoS attacks in existing literature. There have been various instances of such attacks on IoT applications. Such attacks deprive legitimate users from using the services of IoT applications by artificially making the servers or network too busy to respond.
4. **Malicious Code Injection Attacks:** Attackers generally go for the easiest or simplest method they can use to break into a system or network. If the system is vulnerable to malicious scripts and misdirections due to insufficient code checks, then that would be the first entry point that an attacker would choose. Generally, attackers use XSS (cross-site scripting) to inject some malicious script into an otherwise trusted website. A successful XSS attack can result in the hijacking of an IoT account and can paralyze the IoT system.
5. **Sniffing Attacks:** The attackers may use sniffer applications to monitor the network traffic in IoT applications. This may allow the attacker to gain access to confidential user data if there are not enough security protocols implemented to prevent it [39].
6. **Reprogram Attacks:** If the programming process is not protected, then the attackers can try to reprogram the IoT objects remotely. This may lead to the hijacking of the IoT network [40].

IV. IMPROVEMENTS AND ENHANCEMENTS REQUIRED FOR UPCOMING IoT APPLICATIONS

Personal computers (PC) and smartphones have a number of security features built into them, e.g., firewalls, anti-virus softwares, address space randomization, etc. These safety shields are, in general, missing in various IoT devices that are already in the market. There are various security challenges that the IoT applications are facing currently. A well-defined framework and standard for an end-to-end IoT application is not yet available. An IoT application is not a standalone application, and it is an assembled product which includes work from many individuals and industries. At every layer starting from sensing to the application, several diverse products and technologies are being used. These include a large number of sensors and actuators at the edge nodes. There are multiple communication standards like cellular network, WiFi, IEEE 802.15.4, Insteon, dash7, Bluetooth, etc. A handshake mechanism is required between all these standards. Apart from this, various connectivity technologies are being used at different levels in the same IoT application like Zigbee, 6LOWPAN, wireless HART, Z-Wave, ISA100, Bluetooth, NFC, RFID, etc. Over and above this, the generic HTTP protocol cannot be used in the application layer. HTTP is not suitable for resource-constrained environments because it is heavy-weight and thus incurs a large parsing overhead. Therefore, at the application layer also there are many alternate protocols that have been deployed for IoT environments. Some of them are MQTT, SMQTT, CoAP, XMPP, AMQP, M3DA, JavascriptIoT, etc.

Due to the intense diversity of protocols, technologies, and devices in an IoT application, the significant trade-offs are between cost effectiveness, security, reliability, privacy, coverage, latency, etc. If one metric for improvement is optimized, it may result in the degradation of other metric. For example, imposing too many security checks and protocols in all data transactions in IoT applications may end up increasing the cost and latency of the application, thereby, making it unsuitable for the users.

A typical IoT application consists of a big chain of connected devices, technologies, domains, and geographies. Even if one of the device or technology or their combination is left weak, then that may be the cause of a security threat for the entire application. The chain is considered to be as strong as the weakest link. There has been a large increase in the number of weak links in IoT applications recently. For example, even basic IoT applications such as smart bulbs and smart door locks can be used as a weak link in a smart home IoT application to extract the user's WiFi password [41] and [42].

The large number of IoT devices being deployed around the world to make it smart generates a large amount of environment and user-related data. A lot of private information can be inferred from this data, and that can be another cause of threat for an individual and society at large [7]. As a result, significant improvements and enhancements in the current IoT application structure and framework are required to make it reliable, secure and robust. In this regard:

1. Rigorous penetration testing for IoT devices is necessary to quantify the level of risk involved in deploying these devices in different applications. Based on the risk involved, a priority list can be made and the devices can be deployed appropriately in different applications.
2. Encryption techniques are being used in IoT system at different layers and protocols. However, there are various levels of encrypt, decrypt, and re-encrypt cycles in the complete system. These cycles make the system vulnerable to attacks. End to end encryption would be a promising solution to prevent different attacks.
3. Authenticate-always protocols need to be implemented. Whenever a device wants to interact with another device, an authentication process should be implemented. Digital certificates can be a promising solution to provide seamless authentication with bound identities that are tied to cryptographic protocols.
4. Any IoT security framework being implemented should be tested and confirmed for scalability. The security protocols should not be working only for a limited set of users. The real threats start coming only when the application becomes public and starts being used widely in the public domain. Therefore, proper strategy and planning are required.
5. A mechanism based on encryption techniques like RSA, SHA256, or hash chains is required to secure the user and environment data from being captured. IoT devices need to be designed in a way that they can transmit the sensed data in a secure and encrypted way. This will help in gaining the trust of the individuals, government agencies and industries in IoT applications.
6. Since the IoT devices and applications are growing rapidly, an approach needs to be designed to handle the cost and capacity constraints that are expected to be encountered shortly. A paradigm shift from a centralized approach to some decentralized approach might be needed, where devices can automatically and securely communicate with each other. This can help in reducing the cost of managing the applications and can reduce the issues of capacity constraints [43].
7. Since most of the IoT applications use cloud services for data storage and retrieval, the risks caused by the cloud should also be considered. Cloud is a public platform used by multiple users and there may be malicious users on the cloud who can be the cause of threat for IoT related data. The data should be stored as ciphertext in the cloud and the cloud should not be allowed to decrypt any ciphertext. This can further enhance data security and can save us from the generic risks of using cloud services [44].
8. Apart from the challenges from outside entities, there are various scenarios where the sensors in an IoT application start collecting or sending erroneous data. These errors might be easy to handle in case of a centralized architecture but can become a bottleneck in case of an autonomous decentralized architecture. Faulty reading or transmitting of data can lead to undesirable results. Thus, mechanism needs to be identified to validate the data flow, especially in case of a distributed architecture [45].
9. Since the ultimate goal of all IoT applications is to create an autonomous system that needs minimum human interventions, the use of some artificial

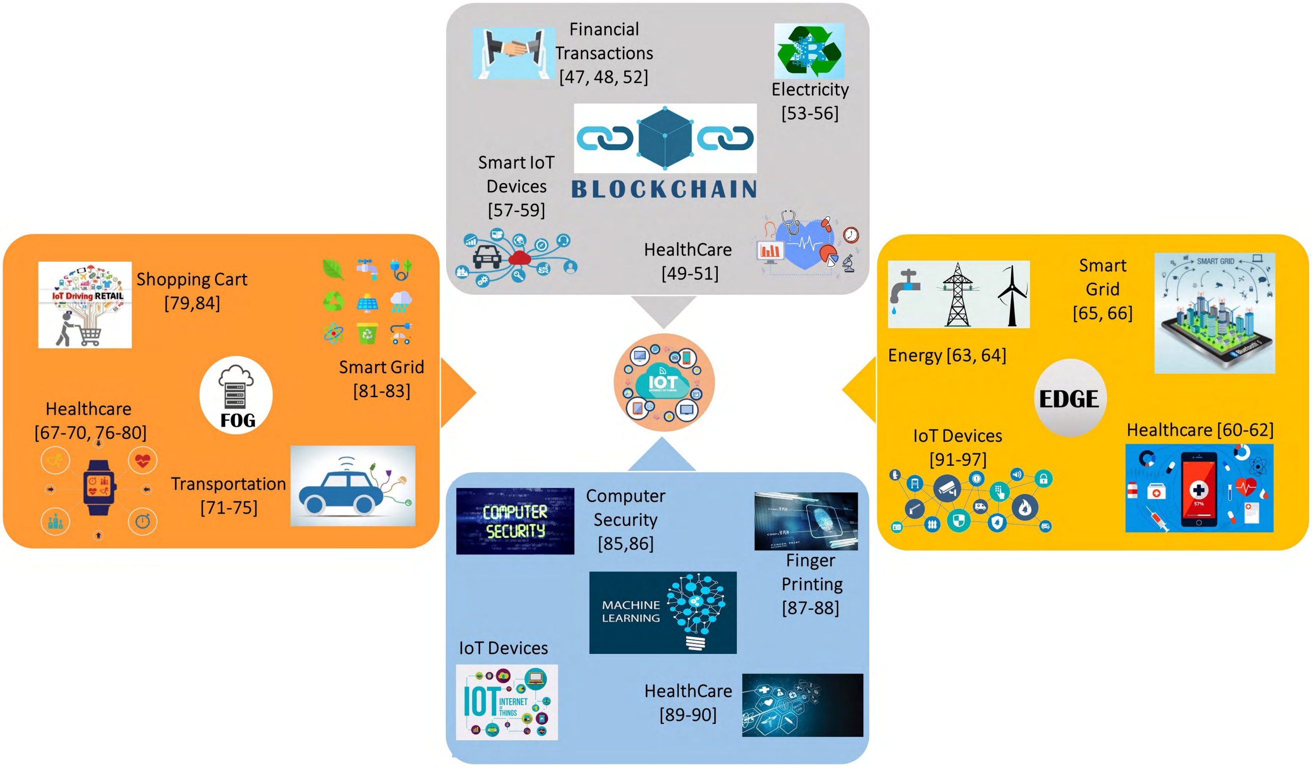


FIGURE 4. **Research papers addressing IoT security using various security techniques.**

intelligence (AI) based techniques or algorithms to secure IoT devices might be useful. This can help in reducing the analysis and communication load on IoT environment [46].

There are various techniques and approaches in the existing literature for securing IoT environments and applications. These solutions may be divided into four categories: (1) blockchain based solutions; (2) fog computing based solutions; (3) machine learning based solutions and (4) edge computing based solutions. Figure 4 shows various works in different domains that have used the above-mentioned solutions for securing the IoT environments [47]–[97]. In the following sections, these solutions are described in detail.

V. IoT SECURITY USING BLOCKCHAIN

Blockchain and IoT are important technologies that will have a high impact on the IT and communication industry. These two technologies focus on improving the overall transparency, visibility, level of comfort and level of trust for the users. The IoT devices provide real-time data from sensors and blockchain provides the key for data security using a distributed, decentralized and shared ledger [108].

The basic idea behind the blockchain is simple: it is a distributed ledger (also called replicated log files). The entries in the blockchain are chronological and time-stamped. Each entry in the ledger is tightly coupled with the previous entry using cryptographic hash keys. A Merkle tree is used to store the individual transactions and the root hash of the tree is stored in the blockchain. In the figure, $T1, T2, T3, \cdots, Tn$ represent the individual transactions. The transactions are cryptographically hashed and stored on the leaf nodes of the tree as Ha, Hb, Hc and so on. The hash of the child nodes are concatenated and a new root hash is generated. The final root hash (e.g., $H1$ and $H2$) is stored on the blockchain. Just the root hash can be verified in order to make sure that all the transactions associated with that root hash are secure and have not been tampered with. Even if a single transaction is changed, all the hash values on that particular side of the tree will change. The ledger maintainer or the miner verifies the logs or transactions and generates a key that enables the latest transaction to become the part of complete ledger. This process makes the latest entries available to all the nodes in the network. Due to the presence of cryptographic hash keys in each block, it is too time-consuming and difficult for the adversaries to tamper with the blocks [109].

The miners do not have any personal interest in the transactions, and they are mining just to earn their incentives. The miners do not know the identity of the owners of the transactions. Over and above, there are multiple miners working on the same set of transactions, and there is a strong competition between them to add the transactions to the blockchain. All these unique features empower the blockchain to be a strong, tamper-proof, distributed and open data structure for IoT data [110]. Figure 5 shows the complete flow of a transaction from being initialized to being committed to the distributed chain. There are various platforms and

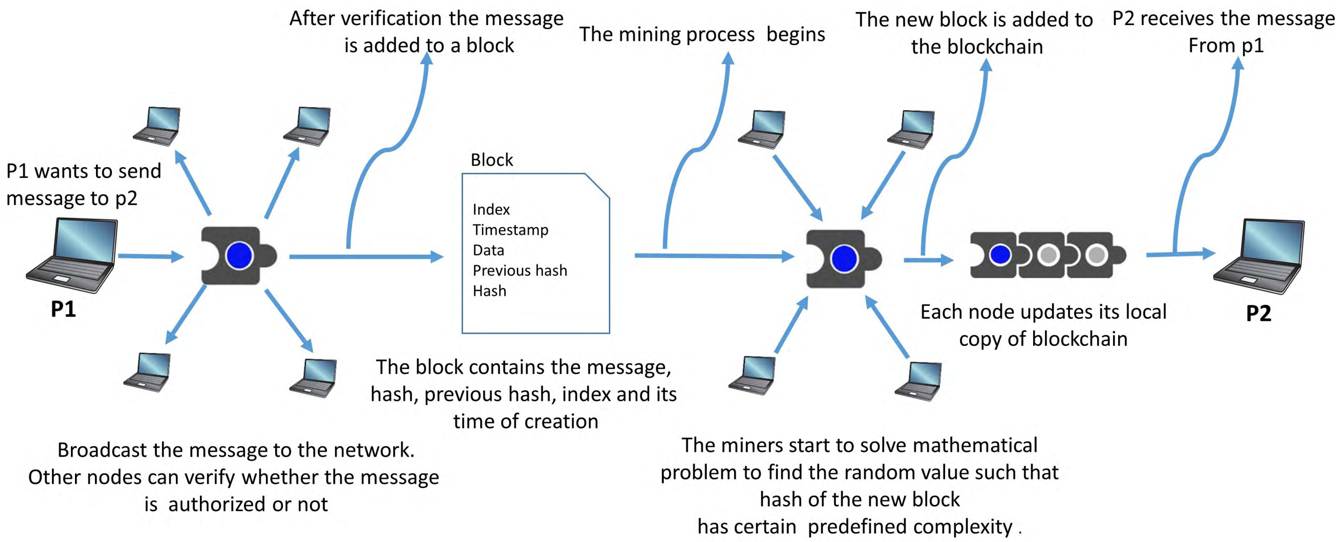


FIGURE 5. Working process of blockchain.

frameworks being developed in academia and industry that support the creation and maintenance of blockchain. Some examples of such platforms are Ethereum, Hyperledger fabric, Ripple, etc. [111].

A. PERMISSIONED AND PERMISSION-LESS BLOCKCHAIN

There are two types of blockchain architectures based on the type of data being added and the nature of application using blockchain. In permission-less blockchain, there is no specific permission required for a user to become the part of the blockchain network or to become a miner. Anyone can join or leave this network of permission-less blockchain. The best example of permission-less blockchains is Bitcoin. Although the throughput of transactions is not very high, the permission-less blockchains can support a large number of nodes in the network.

On the other hand, the permissioned blockchains have a defined set of rules to participate in the blockchain network. The miners are also the authorized persons and the blocks are allowed to be added to the chain only after their validation. The blockchain of Ripple and Hyperledger are two prime examples of permissioned blockchain. The permissioned concept of blockchain improves the overall throughput of transactions as compared to permission-less blockchains. Figure 6 shows the sample architecture of a blockchain and the way every block is connected to all the previous blocks based on cryptographic hashing.

B. BENEFITS OF BLOCKCHAIN IN IoT

The usage of blockchain has many advantages in IoT applications. Table 4 gives a summary of some specific challenges in IoT security and their possible solutions using blockchain. Various security issues faced by IoT applications have already been discussed in Section III. The key benefits of using blockchain in IoT applications are discussed below.

1. **Data coming from IoT devices can be stored in Blockchain:** The IoT applications include a large variety of devices connected to each other. These devices are further connected and controlled by other devices. This setup is further connected to the cloud to enable IoT applications to be used from any location. Due to this large space for data movement, blockchain is a promising solution to store the data and prevent it from being misused. Irrespective of the layer in an IoT application, blockchain can act as a suitable solution to store and transmit data.
2. **Distributed nature of blockchain allowing secure data storage:** Since the blockchain architecture is distributed in nature, it can avoid the risk of being a single point of failure as is faced by various IoT applications based on the cloud. Irrespective of the distance between the devices, the data generated by them can be easily stored on the blockchain in a secure manner [112].
3. **Data encryption using the hash key and verified by miners:** In blockchain, only the 256-bit hash key for the data can be stored, rather than storing the actual data. The actual data can be stored on the cloud and the hash key can be mapped with the original data. If there is any change in the data, the hash of the data will change. This makes the data secure and private. The size of blockchain will also not get affected by the size of the data as only the hash values are stored in the chain. Only the intended parties, who are authorized to use that data can access the data from the cloud using the hash of the data. Every set of data being stored on blockchain is properly verified by different miners in the network, and therefore the probability of storing corrupt data from the devices reduces by using blockchain as a solution.

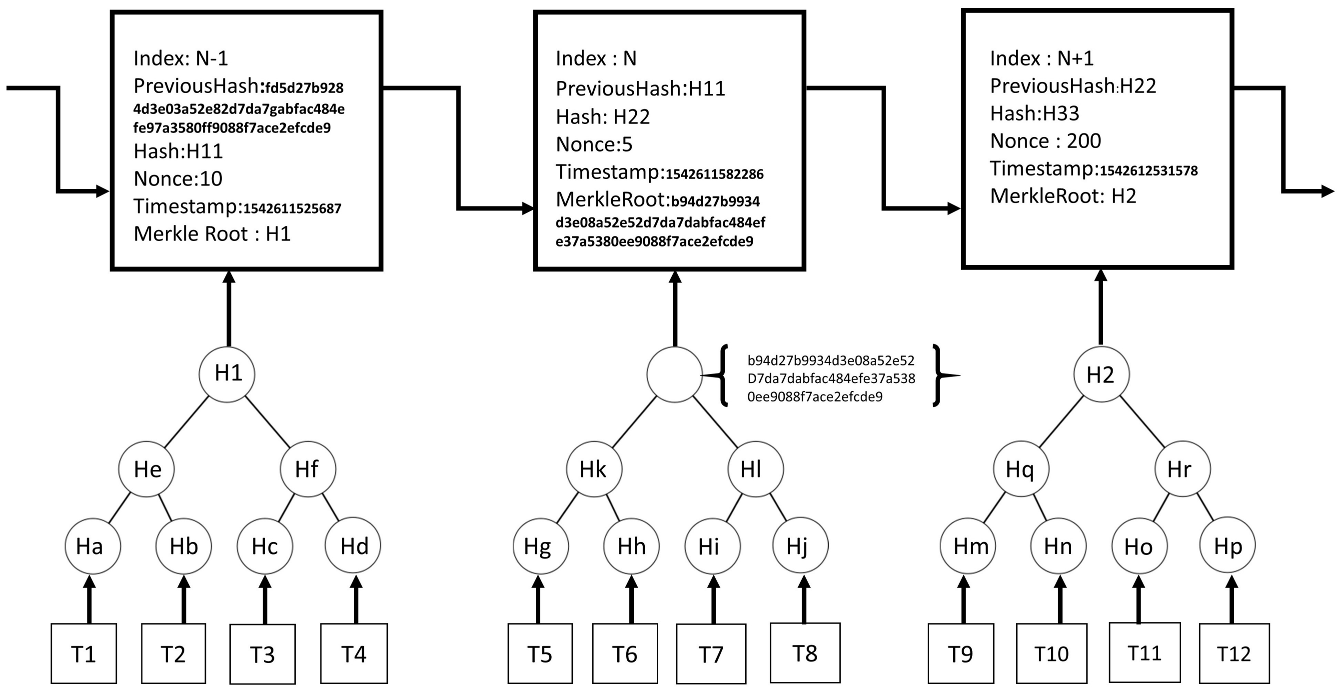


FIGURE 6. Basic blockchain architecture.

TABLE 4. Challenges in IoT and possible blockchain solution.

Challenge Towards IoT	Specification	Possible Blockchain Solution
Privacy in IoT devices	IoT devices are vulnerable to exposing private user data	To address such a challenge, proposed solution is to use Permissioned Blockchain that can secure the IoT devices [98], [99], [100].
Cost and traffic	To handle exponential growth in IoT devices	Moving towards decentralization using blockchian. The devices can directly connect and communicate with the peers rather than communicating via central servers [3], [101], [102].
Heavy load on cloud service and services insufficiency	Cloud services are unavailable due to attacks, bugs in software, power or other problems	Records are updated on different nodes on the network that hold same data so there is no single point of failure [103], [104].
Defective architecture	All parts of IoT devices have point of failure that affects network and the whole device	Validity of devices is verified due to blockchain. The data is also verified cryptographically to ensure that only main originator can send it [105].
Data manipulation	Data is extracted from IoT devices and after manipulating, the data it is used in some inappropriate way	Due to blockchain, devices are interlocked. If any device updates data the system rejects it [106], [107].

4. **Prevention from data loss and spoofing attacks:** In spoofing attacks on IoT applications, a new adversary node enters into the IoT network and starts imitating to be the part of the original network. By spoofing, the adversary can easily capture, observe or inject data in the network. Blockchain acts as a promising solution to prevent such attacks. Each legitimate user or device is registered on blockchain, and devices can easily identify and authenticate each other without the need for central brokers or certification authorities [113]. Being low powered in nature, IoT devices inherit the risk of losing data. There might be cases where due to

some external environmental issues the data is lost by both the sender and the receiver. Use of blockchain can prevent such losses as once the block is added in the chain there is no way to remove it [114].

5. **Blockchain to prevent unauthorized access:** Many IoT applications involve a lot of frequent communication between various nodes. The communication in blockchain takes place using the public and private keys, and therefore only the intended party or node can access the data. Even if the unintended party is able to access the data, the contents of the data will be incomprehensible as the data is encrypted with keys. Therefore, the blockchain data structure tries to handle various security issues faced by IoT applications.
6. **Proxy-based architecture in blockchain for resource-constrained devices:** Although blockchain provides various security features for a distributed environment, IoT has a specific challenge of resource constraints. Being highly resource-constrained, IoT devices cannot store large ledgers. There have been various works in this direction to facilitate the use of blockchain in IoT. Proxy-based architecture is one of the promising solutions that can help IoT devices to use blockchain. Proxy servers can be deployed in the network, to store the resources in an encrypted form. The encrypted resources can be downloaded by the client from the proxy servers [115].
7. **Elimination of centralized cloud servers:** Blockchain can enhance the security of IoT systems because it ultimately eliminates the centralized cloud servers and makes the network peer-to-peer. Centralized cloud servers are the prime target of the data thieves. Using blockchain, the data will be distributed among all the nodes of the network and will be encrypted using a cryptographic hash function.

C. MERKLE TREE

Merkle tree is an add-on that can be added to the blockchain data structure to enhance the security of IoT devices. This can also help in reducing the overall number of blocks being added in the chain. A Merkle tree is like a binary tree where every node contains two child nodes except the leaf nodes. The leaf nodes contain the data or transactions, and the roots are the hash values of the data on the leaf nodes [116]. Based on the size of the tree, multiple transactions can be combined to generate a single root hash. Rather than treating each transaction as a block, each root hash can be considered as a block in the chain. This can help us in reducing the number of blocks. Also, due to multiple levels of hashing, at every level in the tree, the security of the data is enhanced [117]. IoT devices involve a lot of small communications among each other and therefore using Merkle tree along with blockchain can be a promising solution [118].

D. IOTA

IOTA is another upcoming and highly promising solution to secure IoT. IOTA is also a DLT (Distributed Ledger Technology) as blockchain. IOTA is specially designed for resource-constrained IoT devices. Every incoming request in the network is required to validate the previous two requests. Using this process of cumulative validations, IOTA can provide a high level of security at the device or edge level. The tip selection algorithm is used for request verification. A cumulative weight is created for all requests. Higher the weight of a device in the network, more secure the device is. IOTA uses a tangle data structure as compared to the chain data structure in blockchain [119].

VI. IoT SECURITY USING FOG COMPUTING

A. EVOLUTION OF FOG FROM CLOUD

IoT and cloud computing are two independent technologies which have many applications. IoT has provided users with a large number of smart devices and applications. Similarly, a cloud provides a very effective solution to store and manage data which can be accessed from anywhere and is widely used by many organizations. IoT is generating an unprecedented amount of data, which puts a lot of strain on the Internet infrastructure. The integration of cloud and IoT has introduced an era of new opportunities and challenges for processing, storing, managing and securing data more effectively. Industry and research groups have tried to solve some issues faced by the IoT by integrating it with the cloud. The benefits of this integration are not enough to address all the issues faced by IoT. Therefore, the concept of fog computing was introduced by Cisco in 2012. Fog computing complements cloud computing rather than replacing it.

B. FOG COMPUTING ARCHITECTURE

The main task of fog computing is to handle the data generated by IoT devices locally for better management and thus requires an architecture consisting of different layers. It has two frameworks that are Fog-Device framework and Fog-Cloud-Device framework [120]. The former framework consists of device and fog layer and the latter framework consists of device, fog and cloud layer. The arrangement of layers is done based on their storing and computational powers. The communication between different layers is done using wired (e.g., optical fiber, Ethernet) or wireless communication (e.g., WiFi, Bluetooth, etc.). In Fog-Device framework, the fog nodes provide various services to a user without involving cloud servers. However, in Fog-Cloud-Device framework the simple decisions are taken at the fog layer, whereas, the complex decisions are taken on cloud [121]. The architecture of Fog-Cloud-Device framework is shown in Figure 7. The authors of [122] have considered the fog computing architecture theoretically and mathematically while comparing the performance of fog computing paradigm

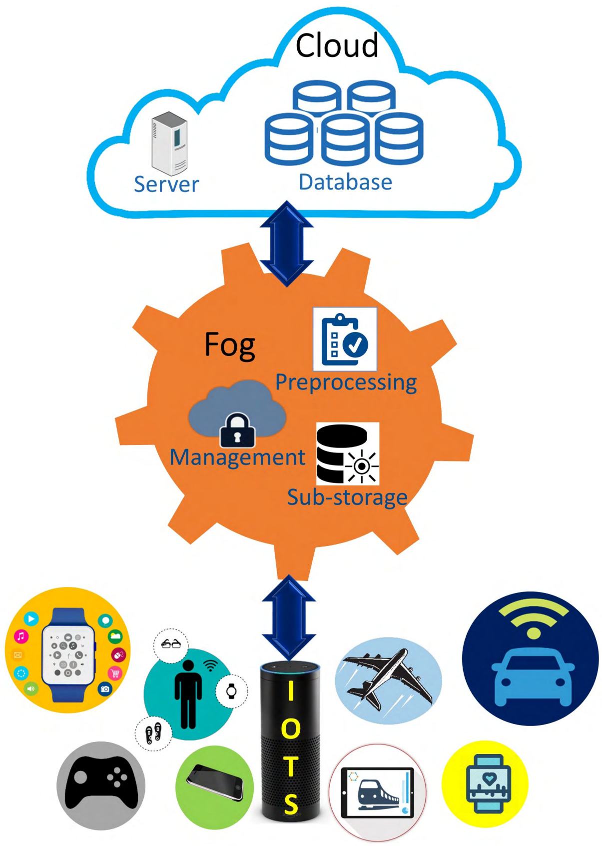


FIGURE 7. Fog computing architecture.

with traditional cloud computing framework based on service latency and energy consumption. Fog computing reduces the data traffic between cloud and network edge by 90% and average response time for a user by 20% when compared with cloud-only model [123]. Authors in [124] have discussed the definition and concept of fog computing in-depth, comparing it with similar concepts such as mobile-edge computing (MEC) and mobile cloud computing (MCC). Authors in [124] have also introduced some applications like real-time video analytics and augmented reality (AR), mobile big data analytics, and content delivery and caching for fog computing.

C. ADVANTAGES OF FOG OVER CLOUD

IoT devices generate large volumes of data every day. Moving this data to the cloud in real-time for analysis is not feasible. Therefore, the concept of fog computing has been developed. Figure 7 shows the placement and functionality of fog layer in an IoT application. Fog computing refers to extending cloud computing and its services to the edge of the network. Fog computing is a decentralized infrastructure for analysis of data and computing and can be used to store and process time-sensitive data efficiently and quickly. Its main goal is to enhance security, prevent data thefts, minimize the data stored on the cloud and to increase the overall efficiency of IoT applications. The latency in fog computation is less than cloud computation because the fog layer is placed much closer to the devices than the cloud. Only the selected and important data is sent to the cloud for long-term storage. Fog computing applications include smart vehicles, smart homes, smart agriculture, health-care, smart traffic lights, smart retail, software-defined networks, etc. Sending the immense amount of data generated by IoT devices to the cloud for processing and analyzing would be costly and time-consuming. Along with minimizing network bandwidth requirements, fog computing also reduces the frequency of two-way communication between IoT devices and the cloud [125].

In fog architecture, the data is collected at devices called fog nodes which can analyze 40 percent of it [126]. It offloads traffic from the core network minimizing the latency of IoT devices. A fog node can be any device like a router, switch, or a video surveillance camera which has computing, storage, and network connectivity. These fog nodes can be installed anywhere like on a factory floor or in a vehicle, provided it has a network connection. Data is directed to the fog node, aggregation node or cloud based on its time-sensitivity. Fog nodes make the communication in IoT application secure by providing cryptographic computations. Mere sensors and IoT devices do not always have the necessary inbuilt resources for that purpose [127].

D. SOLUTIONS PROVIDED BY FOG COMPUTING TO OVERCOME IoT SECURITY THREATS

In regard to the attacks discussed in Section III, the solution that fog computing provides or can provide to overcome those security threats are discussed below.

1. **Man-in-the-middle attack:** Fog acts as a security layer between end-user and cloud or IoT system. All threats or attacks on the IoT systems need to pass through the fog layer in between, and this layer can identify and mitigate unusual activities before they are passed to the system.
2. **Data transit attacks:** Data storage and management is much better if performed on the secure fog nodes, as compared to the IoT devices. Data will be better protected if it is stored on the fog nodes as compared to storing the data on the end-user devices. Fog nodes also help in making the user data more available.
3. **Eavesdropping:** Using fog nodes, the communication takes place between the end-user and the fog node only, rather than routing the information through the entire network. The chances of an adversary trying to eavesdrop reduces a lot because the traffic on the network is reduced.
4. **Resource-constraint issues:** Most of the IoT devices are resource constrained and the attackers take advantage of this fact. They try to damage the edge devices and use them as the weak links to enter the system. Fog nodes can support the edge devices and can prevent them from being affected by such attacks. A nearby fog node can perform the more sophisticated security functions necessary for protection.

TABLE 5. Characteristics and solutions provided by fog computing.

Characterstics	Solutions Provided By Fog
Decentralization	Verifiable computation [128]–[130] Server-aided exchange [131], [132] Big data analytics [133]–[137]
Data dissemination	Designing protocol [138] Sharing data securely [139]–[143] Searching data securely [144], [145]
Real-time services	Identity recognition [146]–[151] Access management [152], [153] Intrusion detection [154]–[159]
Transient storage	Recovery from attacks [160] Data distribution [161] Identifying and protecting sensitive data [162]

5. **Incident response services:** Fog nodes can be programmed to provide real-time incident response services. Fog nodes can generate a flag to the IoT system or the end users as soon as they encounter a suspicious data or request. Fog computing allows for malware detection and problem resolution in transit. In many critical applications, it might not be possible to stop the entire system to resolve malware incidences. Fog nodes can help in such resolutions while the system is up and running.

E. SECURITY CHALLENGES AND SOLUTIONS IN FOG LAYER

Although fog layer provides various features and security aspects for IoT applications, the movement of data and computation to fog layer creates new vulnerabilities [120]. Therefore, before implementing fog-assisted IoT applications, these security and privacy goals of fog computing are required to be studied. In this section, various features provided by fog layer, privacy and security challenges faced, and proposed solutions to overcome them are discussed. Table 5 summarizes these issues and proposed solutions.

1. **Real-Time Services:** Fog computing tends to provide a near real-time service in the IoT systems by performing computation near the data generation points.
   - Intrusion detection: Policy violations and malicious activities on fog nodes and IoT devices will not be discovered if no proper intrusion detection mechanism is implemented. The attacks might not impact the whole architecture of fog computing, but the attacker can control the local services. Attacks targeting local services can be detected by fog nodes by collaborating with their adjacent nodes. By observing program behavior and host file systems, the attack on the cloud can be detected [163].
   - Identity authentication: There are various entities involved in the process of offering and accessing real-time services like fog nodes, service providers and users. Trusting all the entities involved is an arduous task, and creates security challenges for IoT services and user's data. Accessibility of services should be given only to authentic and credible users; otherwise, attackers may compromise the server and exploit services and user privacy. Therefore, to prevent attackers from illegitimately accessing services, identity authentication mechanisms are needed. To provide secure services, some efficient identity authentication mechanisms have been proposed in the past [146]–[149], [164], [165].
2. **Transient Storage:** Users can store and maintain their data on fog nodes temporarily with the help of transient storage. On the one hand, it helps in managing data easily on local storage, but on the other hand, it creates new challenges and security issues, especially for maintaining data privacy.
   - Identifying and protecting sensitive data: Data stored in IoT devices may include social events, traffic conditions, personal activities, temperature and so on. Some of the data might be personal or sensitive while some data may be made public. Furthermore, for different users, the same data has different security levels. Therefore, it is important to identify and protect the sensitive data from the large volume of information.
   - Sharing data securely: To provide security, data uploaded on fog nodes is first encrypted. No one other than its owner can read that data once it is encrypted. This creates a problem for data sharing. To overcome this challenge, some cryptographic techniques such as key-aggregate encryption, proxy re-encryption, and attribute-sharing, have been proposed in [166].
3. **Data Dissemination:** The data cannot be transferred to the fog node without encryption, due to security issues.

Due to this movement of encrypted data to the fog node, many desirable features are sacrificed such as sharing, searching, and aggregation.

- Searching data securely: As discussed in transient storage, data is encrypted before uploading. However, once it is encrypted, searching or retrieving on the ciphertext becomes difficult for owners as well as other entities. In order to retrieve the information from encrypted text, search-able encryption and its privacy levels are defined in [145]. A dynamic symmetric search-able scheme is introduced in [167].
- Data aggregation: Fog nodes might need to aggregate the data in certain cases to prevent data leakage and reduce communication overhead. It is important to develop secure aggregation algorithms to prevent data thefts. Various homomorphic encryption schemes, such as BGN encryption [168] and Paillier encryption [169], have been proposed to achieve secure data aggregation.

4. **Decentralized Computation:** The data stored on the fog nodes can be processed and analyzed for better results. However, such computations have several threats and risks associated with them. For example, attackers can not only control the analyzed results, but can also expose processed data.
   - Server-aided computation: Tasks which cannot be executed by IoT devices themselves are computed with the help of fog nodes. However, this can lead to exposure of data to attackers, if the fog nodes which received data from IoT are already compromised. Server-aided computation is one such method whose aim is to provide secure computation [131].
   - Verifiable computation: Users rely on the fog nodes to compute their data. There must be a secure mechanism to verify the computation results coming from the fog node. Authors in [170], [171] have proposed certain multi-user mechanisms that help with verifiable computation.

VII. IoT SECURITY USING MACHINE LEARNING

The area of machine learning (ML) has attracted significant interest over recent years. Many domains are using ML for their development, and it is being used for IoT security as well. ML appears to be a promising solution to protect IoT devices against cyber attacks by providing a different approach for defending against attacks as compared to other traditional methods.

A. SOLUTIONS PROVIDED BY ML TO OVERCOME SECURITY THREATS

In regard to the attacks discussed in Section III, the solutions provided by ML to overcome these security threats are discussed below.

1. **DoS Attack:** DoS attacks on IoT devices or originating from IoT devices are a serious concern. One approach to prevent such attacks is to use a Multi-Layer Perceptron (MLP) based protocol that secures networks against DoS attacks [172]. The authors of [173] have proposed a particle swarm optimization and back propagation algorithm to train a MLP that helps in enhancing the security of wireless networks. ML techniques help in increasing the deduction accuracy and securing IoT devices vulnerable to DoS attacks.
2. **Eavesdropping:** Attackers may eavesdrop on messages during data transmission. To provide protection from such attacks, ML techniques such as Q-learning based offloading strategy [174] or non-parametric Bayesian techniques [175] can be used. Schemes such as Q-learning and Dyna-Q are ML techniques that may also be used to protect devices from eavesdropping. Evaluation of these schemes via experiments and reinforcement learning is presented in [176].
3. **Spoofing:** Attacks from spoofers can be avoided by using Q-learning [176], Dyna-Q [176], Support Vector Machines (SVM) [177], Deep Neural Network (DNN) model [178], incremental aggregated gradient (IAG) [46], and distributed FrankWolfe (dFW) [179] techniques. These techniques not only increase the detection accuracy and classification accuracy but also help in reducing the average error rate and false alarm rate.
4. **Privacy Leakage:** Collection of personal information such as health data, location, or photos puts the user's privacy at stake. Privacy-preserving scientific computations (PPSC) [180] should be employed for preventing privacy leakage. A commodity integrity detection algorithm (CIDA) which is based on the Chinese remainder theorem (CRT) is another technique that has been proposed to develop IoT application trust [181].
5. **Digital Fingerprinting:** Digital fingerprinting is one of the upcoming and promising solutions to secure IoT systems and to help the end users gain sufficient trust in the applications. Fingerprints are being widely used to unlock smartphones, approve payments, unlock the car and home doors, etc. Due to its low cost, reliability, acceptability and high-security level, digital fingerprinting is emerging as a dominant bio-metric identification method [182]. Apart from the benefits of digital fingerprinting, there are various challenges to efficiently use this technique in IoT, such as fingerprint classification, image enhancement, feature matching, etc. Various machine learning based algorithms have been developed to provide some non-traditional solutions to overcome these challenges [183], some of which are discussed below.
   - Support Vector Machine: SVM is a training algorithm for non-linear and linear classifications, principal component analysis, text categorization, speaker identification, and regression.

It maximizes the gap between the decision boundary and training patterns. Authors of [184] have discussed the use of SVM in digital fingerprinting in detail. They have also compared it with other traditional models. A feature vector is built based on pixel values of the fingerprint, and it is used to train the SVM. Various patterns behind the fingerprint are analyzed, and then the matching of a fingerprint is done based on patterns identified.
- Artificial Neural Networks: ANN is one of the most commonly used algorithms in the machine learning. It offers many advantages like fault tolerance, adaptive learning, and generalization. In [185] a framework has been proposed for using ANN to identify fingerprints digitally. The digital values of various features in the fingerprint like minutiae, ridge ending, and bifurcation is applied as the input to the neural network for training purpose using back propagation algorithm of ANN. The verification of the fingerprint is done based on the previous experiential values stored in the database.

The fundamental need in IoT is to secure all the systems and devices that are connected to the network. The role of ML is to use and train algorithms to detect anomalies in IoT devices or to detect any unwanted activity taking place in IoT system to prevent data loss or other issues. Therefore, ML provides a promising platform to overcome the difficulties faced in securing IoT devices. Further contributions in this field are required to maintain the growth of IoT.

VIII. IoT SECURITY USING EDGE COMPUTING

Edge and fog computing are both extensions of cloud computing which is widely used by various organizations. Cloud, fog and edge may appear similar but they constitute different layers of IoT applications. The main difference between cloud, fog and edge computing is the location of intelligence and power computation. The cloud is deployed at a much larger scale that needs to process huge amount of data and is situated at comparatively more distance from its users [186]. To overcome the problems faced by cloud computing, edge computing is used as a solution where a small edge server is placed between the user and the cloud/fog. Some processing activity is performed at the edge server, rather than the cloud. Edge computing architecture consists of edge devices, cloud server and fog nodes as shown in Figure 8 [187].

In an edge computing framework the computation and analysis power is provided at the edge itself. The devices in an application can create a network among themselves and can cooperate among each other to compute the data [63]. Consequently, a lot of data can be saved from going outside the device, either to cloud or to fog nodes, and this can enhance the security of the IoT application. Edge computing also helps in providing low communication cost by preventing the need of moving all the data to the cloud [66].

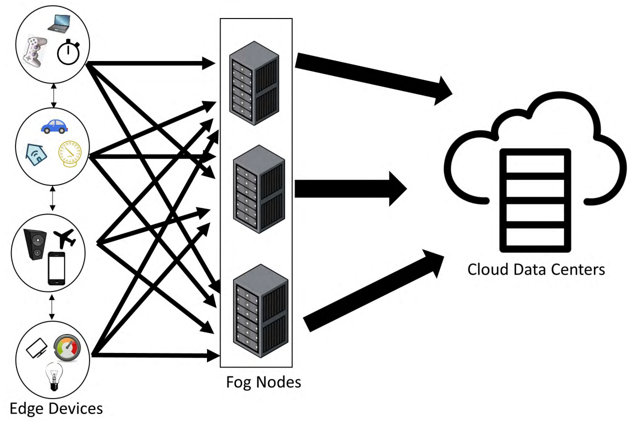


FIGURE 8. Edge computing architecture.

A. USING EDGE COMPUTING TO SECURE AND IMPROVE IoT

In regard to the attacks discussed in Section III, the solutions that edge computing provides or can provide to overcome these security threats are discussed below.

1. **Data Breaches:** In edge computing, all the data is stored and processed within the device or local network. There is no movement of the data from the data originator to the processor. This prevents the data from being in transit and thereby prevents the risk of data thefts and data breaches. In fog computing there is some movement of data from a device to fog layer and adversaries can take advantage of this movement [188].
2. **Data Compliance Issues:** Many countries have strict regulatory acts to prevent data movement outside their boundaries, e.g., European Union's GDPR (General Data Protection Regulation). Using edge computing, organizations can keep the data within their borders and ensure compliance with data sovereignity laws [189].
3. **Safety Issues:** With the increase in the deployment of cyber-physical systems, security and safety are considered as integral issues. If there is even a little delay in responses, then that may lead to physical safety issues. For example, if the sensors in a car predict that a crash is about to happen, then the airbags have to be deployed immediately. If the sensors completely rely on sending all the data to the cloud and waiting for the response from the cloud to perform any action, then that may be too late to prevent injuries or loss of life. Surveillance cameras can also be empowered using edge computing and they can themselves analyze the anomalies and can send the summarized and suspected data to the data centers to achieve faster response times.
4. **Bandwidth Issues:** IoT application generate a lot of data at very high rate. Most of this data is raw and of relatively low-value. Sending all the data to the cloud involves a lot of bandwidth cost as well, along with the

security challenges of data movement. If edge computing is used, then a lot of data cleaning and aggregation can be done at the edge nodes and only the summarized data, if required, needs to be sent to the cloud [190].

B. CHALLENGES IN EDGE LAYER

Although edge computing provides various features to increase the security and performance of IoT applications, there are various challenges associate with completely relying on the edge layer for all computation. Edge devices include sensors, RFID devices, actuators, tags, and embedded devices. The edge layer is highly susceptible to attacks in an IoT system. If the edge layer is compromised, then the entire system may be compromised. MQTT and COAP are the most popular protocols for the edge layer. Both these protocols do not use any security layer by default. Although the option to add an optional security layer in the form of TLS for MQTT and DTLS for COAP is present, it creates additional overhead in terms of processing and bandwidth. Issues specific to edge devices include sleep deprivation attacks, battery draining attacks, and outage attacks. Edge devices are typically resource constrained, and the most important resource they rely upon is the battery backup. The foremost and easiest way to attack the edge devices is to somehow deplete the battery of an edge device. For example, an attacker might force the edge device to do some power hungry or infinite loop computation [191].

The process of striking a balance between storing and processing data on edge or cloud is very important. Keeping too much data on edge may also lead to overwhelming of the edge devices and may impact the entire application.

IX. OPEN ISSUES, CHALLENGES, AND FUTURE RESEARCH DIRECTIONS

There are some performance and security issues in the use of blockchain, fog computing, edge computing and machine learning for IoT security that are yet to be solved. This section discusses some of these issues.

The security of blockchain depends on its method of implementation and the use of software and hardware in that implementation. Since all the transactions made by users in blockchain are public, there is a possibility that private information of users can be revealed. Also, as the number of miners increases, the size of blockchain also increases continuously. This increases the cost of storage and reduces the speed of distribution over the whole network, giving rise to issues like scalability and availability of blockchain [192].

Since fog computing is a nontrivial extension of cloud computing, some of the issues such as security and privacy will continue to persist [120]. Therefore, before implementing fog-assisted IoT applications, these security and privacy goals of fog computing are required to be studied. Some of the challenges and research issues on security and privacy in IoT environments and the solutions provided by fog computing are discussed in [127].

There are many machine learning algorithms in existence. Therefore, it is imperative to select a proper algorithm suitable for the application. Selecting a wrong algorithm would result in producing ''garbage'' output and will lead to loss of effort, effectiveness and accuracy. Similarly, choosing the wrong data set will lead to ''garbage'' input producing incorrect results. The success of a machine learning solution depends on these factors as well as diversity in selecting data. If the data is not clustered and classified, the prediction accuracy will be lower. Also, the historical data may contain many ambiguous values, outliers, missing values, and meaningless data. IoT applications are creating a huge amount of data, and therefore it is a difficult task to clean and preprocess that data accurately. Various features like attribute creation, linear regression, multiple regression, removing redundancies and compressing data are required to effectively use machine learning for securing the IoT.

In case of edge computing, data security and user privacy are the main concerns. An user's private data can be leaked and misused if a house that is deployed with IoT devices is subjected to cyber attacks. For example, a person's presence or absence at home can be revealed simply by observing the electricity or water usage data. Since the data is computed at the edge of data resource (e.g., home), therefore, the user has to be aware of some of the measures like securing WiFi connections. Secondly, data at edge should be owned fully by the user, and he/she should have control on which data to be shared.

Some of the future research directions in this field are:

- The edge devices are most resource constrained devices in the IoT and are therefore uniquely vulnerable to attacks. Penetration studies show that while it takes very little power to implement best practice security for the edge nodes, they are still highly vulnerable to a variety of malicious attacks.
- The gateways between different layers in the IoT system need to be secured. Gateways provide an easy entry point for the attackers into the IoT system. End to end encryption, rather than specific encryption techniques for specific protocols would be a promising solution to secure the data passing through the gateways. The data should be decrypted only at the intended destination and not at the gateways for protocol translation.
- Inter-fog sharing of resources is one of the areas where further work needs to be done. As of now, when the fog layer is unable to process the requests due to heavy load, the requests are forwarded to the cloud. There can be resource sharing between neighboring fog layers to prevent unwanted requests to be transferred to the cloud.
- The current blockchain architecture is highly limited in terms of the number of nodes in permissioned networks and in terms of throughput in permissionless networks. Various consensus algorithms are being designed to support high throughput along with a large number of nodes or users.
- Fog layer can be made more intelligent using various ML and AI techniques. Fog layer must be able to decide the duration for which the data in the fog should be

retained and when the data should be discarded or shifted to the cloud for prolonged storage.

- More efficient and reliable consensus mechanisms can be designed to reach consensus among the nodes along with preventing rampant use of computation power. The current consensus algorithms are highly resource hungry and less efficient.
- The tamper-proof feature of blockchain is ending up into a collection of a lot of garbage data and addresses. There is a lot of invalid data that is never deleted like the addresses of the destructed smart contracts. This affects the performance of the overall application and better ways need to be designed to efficiently handle the garbage data in the blockchain.
- Data analysis in near real-time and in the proximity of the IoT node is crucial for successful deployment of IoT applications. Various ML-based algorithms can be designed to analyze the data in the node itself to prevent the data transit for analysis. This can further enhance the security of the application by preventing data movement.

X. CONCLUSION

In this survey, we have presented various security threats at different layers of an IoT application. We have covered the issues related to the sensing layer, network layer, middleware layer, gateways, and application layer. We have also discussed the existing and upcoming solutions to IoT security threats including blockchain, fog computing, edge computing, and machine learning. Various open issues and issues that originate from the solution itself have also been discussed. The state-of-the-art of IoT security has also been discussed with some of the future research directions to enhance the security levels is IoT. This survey is expected to serve as a valuable resource for security enhancement for upcoming IoT applications.

REFERENCES

[1] R. Kandaswamy and D. Furlonger. *Blockchain-Based Transformation*. Accessed: Jun. 5, 2018. [Online]. Available: https://www.gartner.com/en/doc/3869696-blockchain-based-transformation-a-gartner-trend-insight-report/

[2] Gsma. *Safety, Privacy and Security*. Accessed: Jan. 29, 2019. [Online]. Available: https://www.gsma.com/publicpolicy/resources/safetyprivacy-security-across-mobile-ecosystem/

[3] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[4] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018.

[5] Flashpoint. *Mirai Botnet Linked to Dyn DNS DDoS Attacks*. Accessed: Dec. 18, 2018. [Online]. Available: https://www.flashpoint-intel.com/blog/cybercrime/mirai-botnet-linked-dyn-dns-ddos-attacks/

[6] G. Yang, M. Jiang, W. Ouyang, G. Ji, H. Xie, A. M. Rahmani, P. Liljeberg, and H. Tenhunen, "IoT-based remote pain monitoring system: From device to cloud platform," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 6, pp. 1711–1719, Nov. 2018.

[7] 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. 2017.

[8] 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.

[9] 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.

[10] 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.

[11] L. Chen, S. Thombre, K. Järvinen, E. S. Lohan, A. Alén-Savikko, H. Leppäkoski, M. Z. H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala, J. Lindqvist, L. Ruotsalainen, P. Korpisaari, and H. Kuusniemi, "Robustness, security and privacy in location-based services for future IoT: A survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2017.

[12] 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. 2017.

[13] 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., 2019.

[14] 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, 2019.

[15] A. Gharaibeh, 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.

[16] 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, 1st Quart., 2018.

[17] 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, 2019.

[18] 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.

[19] 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.

[20] 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.

[21] Bridgera. *IoT System | Sensors and Actuators*. Accessed: Feb. 9, 2019. [Online]. Available: https://bridgera.com/IoT-system-sensors-actuators/

[22] Smarthomeblog. *How to Make Your Smoke Detecter Smarter*. Accessed: Feb. 9, 2019. [Online]. Available: https://www.smarthomeblog.net/smart-smoke-detector/

[23] Tictecbell. *Sensor d'Ultrasons*. Accessed: Feb. 11, 2019. [Online]. Available: https://sites.google.com/site/tictecbell/Arduino/ultrasons/

[24] 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.

[25] 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.

[26] APWG. *Phishing Activity Trends Report*. Accessed: Feb. 12, 2019. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q4_2017.pdf

[27] 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.

[28] 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.

[29] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "A survey of middleware for Internet of Things," in *Recent Trends in Wireless and Mobile Networks*. Springer, 2011, pp. 288–296.

[30] Q. Zhang and X. Wang, "SQL injections through back-end of RFID system," in *Proc. Int. Symp. Comput. Netw. Multimedia Technol.*, Jan. 2009, pp. 1–4.

[31] R. Dorai and V. Kannan, "SQL injection-database attack revolution and prevention," *J. Int. Commercial Law Technol.*, vol. 6, no. 4, p. 224, 2011.

[32] 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.

[33] Acunetix. *Insecure Deserialization*. Accessed: Feb. 9, 2019. [Online]. Available: https://www.acunetix.com/blog/articles/owasp-top-10-2017/
[34] 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.
[35] WS-Attacks. *Attack Subtypes*. Accessed: Feb. 9, 2019. [Online]. Available: https://www.ws-attacks.org/XML_Signature_Wrapping
[36] C. Fife. *Securing the IoT Gateway*. Accessed: Feb. 9, 2019. [Online]. Available: https://www.citrix.com/blogs/2015/07/24/securing-the-IoT-gateway/
[37] 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.
[38] 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.
[39] 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.
[40] 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.
[41] M. Kumar. *How to Hack WiFi Password from Smart Doorbells*. Accessed: Jan. 13, 2016. [Online]. Available: http://thehackernews.com/2016/01/doorbell-hacking-wifi-pasword.html
[42] A. Chapman. *Analysing the Attack Surface*. Accessed: Feb. 1, 2016. [Online]. Available: http://www.contextis.com/resources/blog/hacking-internet-connected-light-bulbs
[43] N. Kshetri, "Can blockchain strengthen the Internet of Things?" *IT Prof.*, vol. 19, no. 4, pp. 68–72, 2017.
[44] 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.
[45] 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.
[46] 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.
[47] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[48] T. Swanson. (Apr. 2015). *Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems*. [Online]. Available: https://www.ofnumbers.com/2015/04/06/consensus-as-a-service-a-brief-report-on-the-emergence-of-permissioned-distributed-ledger-systems/
[49] 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.
[50] 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.
[51] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, and F. Sallabi, "Softwarization of Internet of Things infrastructure for secure and smart healthcare," 2018, *arXiv:1805.11011*. [Online]. Available: https://arxiv.org/abs/1805.11011
[52] D. Wilson and G. Ateniese, "From pretty good to great: Enhancing PGP using bitcoin and the blockchain," in *Proc. Int. Conf. Netw. Syst. Secur.* Springer, 2015, pp. 368–375.
[53] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin," in *Proc. 18th Int. Conf. Intell. Next Gener. Netw.*, Feb. 2015, pp. 184–191.
[54] 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.
[55] Ó. Blanco-Novoa, T. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "An electricity price-aware open-source smart socket for the Internet of energy," *Sensors*, vol. 17, no. 3, p. 643, 2017.
[56] 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.
[57] 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.
[58] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2017, pp. 464–467.
[59] 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.
[60] T. Muhammed, R. Mehmood, A. Albeshri, and I. Katib, "Ubehealth: A personalized ubiquitous cloud and edge-enabled networked healthcare system for smart cities," *IEEE Access*, vol. 6, pp. 32258–32285, 2018.
[61] 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.
[62] 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.
[63] 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.
[64] 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.
[65] 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 (ICII)*, Oct. 2018, pp. 99–108.
[66] 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.
[67] 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, 2017.
[68] 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.
[69] 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.
[70] 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.
[71] 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.
[72] 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.
[73] T. H. Luan, L. Gao, Z. Li, Y. Xiang, G. Wei, and L. Sun, "Fog computing: Focusing on mobile users at the edge," 2015, *arXiv:1502.01815*. [Online]. Available: https://arxiv.org/abs/1502.01815
[74] O. T. T. Kim, N. D. Tri, N. H. Tran, and C. S. Hong, "A shared parking model in vehicular network using fog and cloud environment," in *Proc. 17th Asia–Pacific Netw. Oper. Manage. Symp. (APNOMS)*, Aug. 2015, pp. 321–326.
[75] 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.
[76] 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*. Springer, 2017, pp. 281–321.

[77] 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.
[78] 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*, 2015, pp. 43–48.
[79] W. Shi and S. Dustdar, "The promise of edge computing," *Computer*, vol. 49, no. 5, pp. 78–81, 2016.
[80] 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 Int. Conf. Comput. Inf. Technol.*, Oct. 2015, pp. 356–363.
[81] 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.
[82] M. A. A. Faruque and K. Vatanparvar, "Energy management-as-a-service over fog computing platform," *IEEE Internet Things J.*, vol. 3, no. 2, pp. 161–169, Apr. 2016.
[83] 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.
[84] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016.
[85] 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.
[86] P. K. Chan and R. P. Lippmann, "Machine learning for computer security," *J. Mach. Learn. Res.*, vol. 7, pp. 2669–2672, Dec. 2006.
[87] 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, Jun. 2019.
[88] 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.
[89] C. Mercer. *How Machine Learning Will Change Society*. [Online]. Available: https://www.techworld.com/picture-gallery/tech-innovation/5-ways-machine-learning-will-change-society-3666674
[90] 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.
[91] 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.
[92] M. N. Aman, K. C. Chua, and B. Sikdar, "Secure data provenance for the Internet of Things," in *Proc. ACM Int. Workshop IoT Privacy, Trust, Secur.*, 2017, pp. 11–14.
[93] M. N. Aman, B. Sikdar, K. C. Chua, and A. Ali, "Low power data integrity in IoT systems," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 3102–3113, Aug. 2018.
[94] 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. 2018.
[95] 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.
[96] 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.
[97] 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.
[98] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.
[99] P. Lv, L. Wang, H. Zhu, W. Deng, and L. Gu, "An IoT-oriented privacy-preserving publish/subscribe model over blockchains," *IEEE Access*, vol. 7, pp. 41309–41314, Jan. 2019.
[100] U. Javaid, M. N. Aman, and B. Sikdar, "BlockPro: Blockchain based data provenance and integrity for secure IoT environments," in *Proc. 1st Workshop Blockchain-Enabled Netw. Sensor Syst.*, 2018, pp. 13–18.
[101] K. Valtanen, J. Backman, and S. Yrjölä, "Blockchain-powered value creation in the 5G and smart grid use cases," *IEEE Access*, vol. 7, pp. 25690–25707, Feb. 2019.
[102] U. Javaid, A. K. Siang, M. N. Aman, and B. Sikdar, "Mitigating loT device based DDoS attacks using blockchain," in *Proc. 1st Workshop Cryptocurrencies Blockchains Distrib. Syst.*, 2018, pp. 71–76.
[103] K. R. Ozyilmaz and A. Yurdakul, "Designing a blockchain-based IoT with ethereum, swarm, and lora: The software solution to create high availability with minimal security risks," *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, pp. 28–34, Mar. 2019.
[104] V. Sharma, "An energy-efficient transaction model for the blockchain-enabled Internet of vehicles (IoV)," *IEEE Commun. Lett.*, vol. 23, no. 2, pp. 246–249, Feb. 2019.
[105] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2018.
[106] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the Internet of Things," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 12–18, Dec. 2018.
[107] U. Javaid, M. N. Aman, and B. Sikdar, "DrivMan: Driving trust management and data sharing in VANETS with blockchain and smart contracts," in *Proc. IEEE Veh. Technol. Conf.*, May 2019, pp. 1–6.
[108] D. Miller, "Blockchain and the Internet of Things in the industrial sector," *IT Prof.*, vol. 20, no. 3, pp. 15–18, 2018.
[109] H. Orman, "Blockchain: The emperors new PKI?" *IEEE Internet Comput.*, vol. 22, no. 2, pp. 23–28, Mar. 2018.
[110] 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.
[111] R. Henry, A. Herzberg, and A. Kate, "Blockchain access privacy: Challenges and directions," *IEEE Secur. Privacy*, vol. 16, no. 4, pp. 38–45, Jul./Aug. 2018.
[112] 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.
[113] B. Dickson. *How Blockchain Can Change the Future of IoT*. Accessed: Apr. 27, 2019. [Online]. Available: https://venturebeat.com/2016/11/20/how-blockchain-can-change-the-future-of-IoT/
[114] 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.
[115] O. Alphand, M. Amoretti, T. Claeys, S. Dall'Asta, A. Duda, G. Ferrari, F. Rousseau, B. Tourancheau, L. Veltri, and F. Zanichelli, "IoTchain: A blockchain security architecture for the Internet of Things," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6.
[116] 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.
[117] 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.
[118] 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.
[119] Oodles. *Will IOTA Blockchain Solution Secure Internet of Things Ecosystem?* Accessed: Jan. 30,2019. [Online]. Available: https://blockchain.oodles.io/blog/blockchain-solution-IoTa-IoT-security/
[120] 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.
[121] 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*. Springer, 2015, pp. 251–263.
[122] 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.
[123] B. Varghese, N. Wang, D. S. Nikolopoulos, and R. Buyya. "Feasibility of fog computing," 2017, *arXiv:1701.05451*. [Online]. Available: https://arxiv.org/abs/1701.05451
[124] S. Yi, C. Li, and Q. Li, "A survey of fog computing: Concepts, applications and issues," in *Proc. Workshop Mobile Big Data*, 2015, pp. 37–42.
[125] IoT Agenda. *IoT and Big Data Analytics*. Accessed: Nov. 3, 2018. [Online]. Available: https://internetofthingsagenda.techtarget.com/
[126] A. Mitra. *Smart Contracts and Blockchain*. Accessed: Nov. 3, 2018. [Online]. Available: https://www.thesecuritybuddy.com/

[127] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, ''Fog computing for the Internet of Things: Security and privacy issues,'' *IEEE Internet Comput.*, vol. 21, no. 2, pp. 34–42, Mar./Apr. 2017.
[128] 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.
[129] 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.*. Springer, 2015, pp. 144–168.
[130] K. Elkhiyaoui, M. Önen, M. Azraoui, and R. Molva, ''Efficient techniques for publicly verifiable delegation of computation,'' in *Proc. 11th ACM Asia Conf. Comput. Commun. Secur.*, 2016, pp. 119–128.
[131] 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*. Springer, 2015, pp. 156–173.
[132] 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, May 2017.
[133] 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.
[134] 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.
[135] 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.
[136] 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.
[137] 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.*, 2016, pp. 192–203.
[138] 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.
[139] 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.
[140] 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, p. 203, 2017.
[141] 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.
[142] 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.
[143] C.-C. Lee, C.-T. Li, S.-T. Chiu, and S.-D. Chen, ''Time-bound key-aggregate encryption for cloud storage,'' *Secur. Commun. Netw.*, vol. 9, no. 13, pp. 2059–2069, 2016.
[144] X. Yang, F. Yin, and X. Tang, ''A fine-grained and privacy-preserving query scheme for fog computing-enhanced location-based service,'' *Sensors*, vol. 17, no. 7, p. 1611, 2017.
[145] 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.
[146] 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.
[147] 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.
[148] 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.
[149] 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.
[150] 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.
[151] D. Pointcheval and O. Sanders, ''Short randomizable signatures,'' in *Proc. Cryptogr. Track RSA Conf.*. Springer, 2016, pp. 111–126.
[152] S. Salonikias, I. Mavridis, and D. Gritzalis, ''Access control issues in utilizing fog computing for transport infrastructure,'' in *Proc. Int. Conf. Crit. Inf. Infrastruct. Secur.* Springer, 2015, pp. 15–26.
[153] 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.
[154] J. Ni, K. Zhang, K. Alharbi, X. Lin, N. Zhang, and X. 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.
[155] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, ''A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT,'' *IEEE Access*, vol. 5, pp. 3302–3312, 2017.
[156] 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.
[157] 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.
[158] 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.
[159] 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.
[160] 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.
[161] 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.* Springer, 2016, pp. 301–319.
[162] M. Agrawal and P. Mishra, ''A comparative survey on symmetric key encryption techniques,'' *Int. J. Comput. Sci. Eng.*, vol. 4, no. 5, p. 877, 2012.
[163] 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.
[164] 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.
[165] 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.
[166] 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.
[167] 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.
[168] D. Boneh, E.-J. Goh, and K. Nissim, ''Evaluating 2-DNF formulas on ciphertexts,'' in *Proc. Theory Cryptogr. Conf.* Springer, 2005, pp. 325–341.
[169] P. Paillier, ''Public-key cryptosystems based on composite degree residuosity classes,'' in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Springer, 1999, pp. 223–238.
[170] C. Papamanthou, E. Shi, and R. Tamassia, ''Signatures of correct computation,'' in *Proc. Theory Cryptogr. Conf.* Springer, 2013, pp. 222–242.
[171] S. G. Choi, J. Katz, R. Kumaresan, and C. Cid, ''Multi-client non-interactive verifiable computation,'' in *Proc. Theory Cryptogr. Conf.* Springer, 2013, pp. 499–518.
[172] 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.
[173] 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.
[174] L. Xiao, C. Xie, T. Chen, H. Dai, and H. V. Poor, ''A mobile offloading game against smart attacks,'' *IEEE Access*, vol. 4, pp. 2281–2291, 2016.

[175] 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.

[176] 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.

[177] 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.

[178] C. Shi, J. Liu, H. Liu, and Y. Chen, "Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT," in *Proc. 18th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2017, pp. 5–11.

[179] 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.

[180] 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.

[181] 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.

[182] K. Spirina. *Biometric Authentication: The Future of IoT Security Solutions*. Accessed: Feb. 9, 2019. [Online]. Available: https://www.IoTevolutionworld.com/IoT/articles/438690-biometric-authentication-future-IoT-security-solutions.htm

[183] A. I. Awad, "Machine learning techniques for fingerprint identification: A short review," in *Proc. Int. Conf. Adv. Mach. Learn. Technol. Appl.* Springer, 2012, pp. 524–531.

[184] 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.

[185] 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.

[186] 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.

[187] 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.

[188] 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.

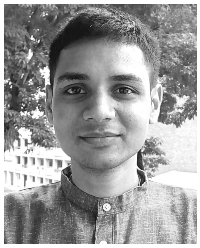
[189] L. Rosencrance. *6 Significant Issues That Edge Computing in IoT Solves*. Accessed: Jan. 26, 2019. [Online]. Available: https://internetofthingsagenda.techtarget.com/feature/6-significant-issues-that-edge-computing-in-IoT-solves

[190] 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.

[191] 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.

[192] 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.

VIKAS HASSIJA received the B.Tech. degree from Maharshi Dayanand University, Rohtak, India, in 2010, and the M.S. degree in telecommunications and software engineering from the Birla Institute of Technology and Science (BITS), Pilani, India, in 2014. He is currently pursuing the Ph.D. degree in IoT security and blockchain with the Jaypee Institute of Information and Technology (JIIT), Noida, where he is currently an Assistant Professor. He has eight years of industrial experience and has worked with various telecommunication companies, such as Tech Mahindra and Accenture. His research interests include the IoT security, network security, blockchain, and distributed computing.



VINAY CHAMOLA received the B.E. degree in electrical and electronics engineering and the master's degree in communication engineering from the Birla Institute of Technology and Science (BITS), Pilani, India, in 2010 and 2013, respectively, and the Ph.D. degree in electrical and computer engineering from the National University of Singapore, Singapore, in 2016. In 2015, he was a Visiting Researcher with the Autonomous Networks Research Group (ANRG), University of Southern California (USC), USA. He is currently a Research Fellow with the National University of Singapore. His research interests include solar-powered cellular networks, energy efficiency in cellular networks, the Internet of Things, and networking issues in cyber-physical systems.

VIKAS SAXENA received the B.Tech. degree from IET, M.J.P. Rohilkhand University, Bareilly, India, in 2000, the M.E. degree from VJTI, Mumbai, India, in 2002, and the Ph.D. degree in CSE from the Jaypee Institute of Information and Technology, Noida, India, in 2009, where he is currently a Professor and the Head of Computer Science and Information Technology Department. He has more than 17 years of experience in teaching and research. His research interests include image processing, blockchain, computer vision, software engineering, and multimedia. He has served as the Publicity Co-Chair with the International Conference IC3-2008, India, conducted by JIIT and the University of Florida, USA.

DIVYANSH JAIN is currently pursuing the B.Tech. degree with the Jaypee Institute of Information and Technology. He is currently a Summer Intern with the Birla Institute of Technology and Science (BITS), Pilani. He has completed few projects on deep learning, blockchain, and artificial intelligence. His research interests include distributed algorithms and data structures.

PRANAV GOYAL is currently pursuing the B.Tech. degree with the Jaypee Institute of Information and Technology. He is currently a Summer Intern with the Birla Institute of Technology and Science (BITS), Pilani. He has completed few projects on blockchain applications and machine leaning. His research interests include distributed computing, the IoT, and data analytics.

BIPLAB SIKDAR (S'98–M'02–SM'09) received the B.Tech. degree in electronics and communication engineering from North-Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from the IIT Kanpur, Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. His research interests include wireless MAC protocols, transport protocols, network security, and queuing theory.