IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 26, 2019, accepted December 11, 2019, date of publication December 17, 2019,
date of current version December 26, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2960412

IoMT Malware Detection Approaches: Analysis and Research Challenges

MOHAMMAD WAZID[1], (Member, IEEE), ASHOK KUMAR DAS[2], (Senior Member, IEEE), JOEL J. P. C. RODRIGUES[3,4], (Fellow, IEEE), SACHIN SHETTY[5], (Senior Member, IEEE), AND YOUNGHO PARK[6], (Member, IEEE)

[1]Department of Computer Science and Engineering, Graphic Era (Deemed to be University), Dehradun 248002, India
[2]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India
[3]PPGEE, Federal University of Piauí (UFPI), 64049-550 Teresina, Brazil
[4]Instituto de Telecomunicações, 1049-001 Lisbon, Portugal
[5] Virginia Modeling, Analysis and Simulation Center, Department of Computational Modeling and Simulation Engineering, Old Dominion University, Suffolk, VA 23435, USA
[6]School of Electronics Engineering, Kyungpook National University, Daegu 41566, South Korea

Corresponding author: Youngho Park (parkyh@knu.ac.kr)

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning under Grant 2017R1A2B1002147, in part by the Fundação para a Ciência e a Tecnologia through the UID/EEA/50008/2019 Project, in part by the Brazilian National Council for Scientific and Technological Development (CNPq) under Grant 309335/2017-5, and in part by the Office of the Assistant Secretary of Defense for Research and Engineering [OASD (R&E)] under Grant FA8750-15-2-0120.

ABSTRACT The advancement in Information and Communications Technology (ICT) has changed the entire paradigm of computing. Because of such advancement, we have new types of computing and communication environments, for example, Internet of Things (IoT) that is a collection of smart IoT devices. The Internet of Medical Things (IoMT) is a specific type of IoT communication environment which deals with communication through the smart healthcare (medical) devices. Though IoT communication environment facilitates and supports our day-to-day activities, but at the same time it has also certain drawbacks as it suffers from several security and privacy issues, such as replay, man-in-the-middle, impersonation, privileged-insider, remote hijacking, password guessing and denial of service (DoS) attacks, and malware attacks. Among these attacks, the attacks which are performed through the malware botnet (i.e., Mirai) are the malignant attacks. The existence of malware botnets leads to attacks on confidentiality, integrity, authenticity and availability of the data and other resources of the system. In presence of such attacks, the sensitive data of IoT communication may be disclosed, altered or even may not be available to the authorized users. Therefore, it becomes essential to protect the IoT/IoMT environment from malware attacks. In this review paper, we first perform the study of various types of malware attacks, and their symptoms. We also discuss some architectures of IoT environment along with their applications. Next, a taxonomy of security protocols in IoT environment is provided. Moreover, we conduct a comparative study on various existing schemes for malware detection and prevention in IoT environment. Finally, some future research challenges and directions of malware detection in IoT/IoMT environment are highlighted.

INDEX TERMS Internet of Things (IoT), Internet of Medical Things (IoMT), security, IoT malware, malware detection.

I. INTRODUCTION

The Internet of Things (IoT) is a network of physical objects such as smart machines, smart home appliances and many more. They have a uniquely assigned Internet address (IP) through which they can communicate to the external entities (i.e., user of a smart home) of the network. These devices use sensors and application programming interface (API) to connect and exchange the data over the Internet [1]–[3]. IoT device is a kind of micro-computer which is very domain-specific unlike the traditional function-specific embedded devices. According to ''Gartner report'', the number of connected devices across all technical domains will reach up to 1.0 trillion by 2025.

The associate editor coordinating the review of this manuscript and approving it for publication was Victor Hugo Albuquerque.

TABLE 1. Statistics of connected IoT devices [4].

Year	Number of connected IoT devices
1990	0.3 million
1999	90.0 million
2010	5.0 billion
2013	9.0 billion
2025	1.0 trillion

The progress information of IoT device deployment as per the decades is provided in Table 1.

Internet of Medical Things (IoMT) is an another form of IoT communication environment. It consists of medical devices, such as smart healthcare and monitoring devices (i.e., smart pacemaker, smart blood glucose meter, etc.) and applications which connect them to the healthcare IoT systems through the Internet. Medical devices are also equipped with some wireless communication technology (i.e., bluetooth, Wi-Fi) that allow the machine-to-machine communication which is a foundation for IoMT communication environment. In IoMT, the smart healthcare devices sense (monitor) the health related information of the patient and send the data to some server (for example, cloud server). Some cloud platforms, such as Amazon Web Services (AWS), may be used to store the health data and analyze the data for further decision making and health prescriptions [5]–[8].

The security issues in the IoT devices are going to increase day by day because of rapid development and deployment of IoT systems. This opens the possibility to launch various types of attacks in the IoT environment using the Internet. It becomes very serious issue in case of of IoMT that deals with the communication and controlling of smart medical devices. For example, if an attacker successfully gets the remote control over a smart medical device, he/she can threat the life of the patient (i.e., a smart pacemaker can give shock to a patient which may become the reason of his/her death). Different variations of IoT malware are constantly emerging. These emerging malwares can also affect the communication of IoMT and they can be used to control the smart medical devices.

The existing mechanisms are not sufficient for the IoT/IoMT malware detection and analysis. As we have seen recently the attacks performed by Mirai and Brickerbot botnets. These attacks produce distributed denial-of-service (DDoS) attacks in IoT environments because of the lack of strong security monitoring and protection techniques. Hence, it becomes essential to provide some strong security mechanism to detect and defend such kind of threatening attacks in IoT (especially in IoMT) [9]–[11].

The main motivation behind this survey work is as follows. These days IoT devices (i.e., smart home appliances and smart healthcare devices) become the integral part of our day to day life as they facilitate and support our activities. As we know a user of IoT device accesses the data remotely by using the Internet [3], [12], [13]. Different entities, such as IoT devices, servers and users, communicate through the Internet. However, IoT/IoMT communication environment has some security and privacy issues. Various types of attacks, such as replay, man-in-the-middle (MITM), impersonation, password guessing and denial of service (DoS) attacks, are possible in this environment. Most of the time, the hackers may use malwares to target the IoT devices to get illegal access to these devices and to control them remotely. To spread malware in IoT environment, the hackers use network of attacker systems (i.e., botnet) (for example, Mirai, Reaper, Echobot, Emotet, Gamut and Necurs are very famous these days). These types of botnet attacks are also possible in IoMT environment and can be used to hijack (control) a smart medical device remotely. This can create other life threatening situations for the people (i.e., a smart pacemaker can give shock to a patient which may become the reason of his/her death). Hence, people working in the IoT security domain come up with new ideas to protect the IoT/IoMT communication environment against these attacks. Therefore, in this work we provide a detailed study of different types of malware programs, active IoT/IoMT malwares and the available solution for these attacks.

The research contributions of this review work are given below.

- We discuss some of the architectures of IoT environment along with their applications.
- We highlight different security requirements of IoT communication environment.
- We provide various details of the malware programs (for example, symptoms of their presence and their types).
- We provide a study on recent malware attacks (i.e., Mirai, Reaper, Echobot, Emotet, Gamut and Necurs) which may happen in IoT communication environment. Such kind of malware attacks are also possible in IoMT environment.
- A taxonomy of security schemes in IoT/IoMT environment is also added which contains several security protocols, such as key management, user/device authentication, access control and intrusion detection protocols.
- Furthermore, we provide the details of various malware detection schemes in IoT communication environment. A comparative study to provide the information about the performance of the existing schemes is also added.
- Some of the future research challenges and directions on this area are also highlighted.

The rest of the paper is organised as follows. Various architectures of IoT environment along with their applications are provided in Section II. The security requirements in IoT/IoMT communication environment are highlighted in Section III. Different categories of malwares, symptoms of their existence and types are discussed in Section IV. The case study of recent malware attacks in IoT communication environment is provided in Section V. A taxonomy of security schemes in IoT/IoMT environment is also highlighted in Section VI. The details of malware detection schemes in IoT communication environment along with their comparative

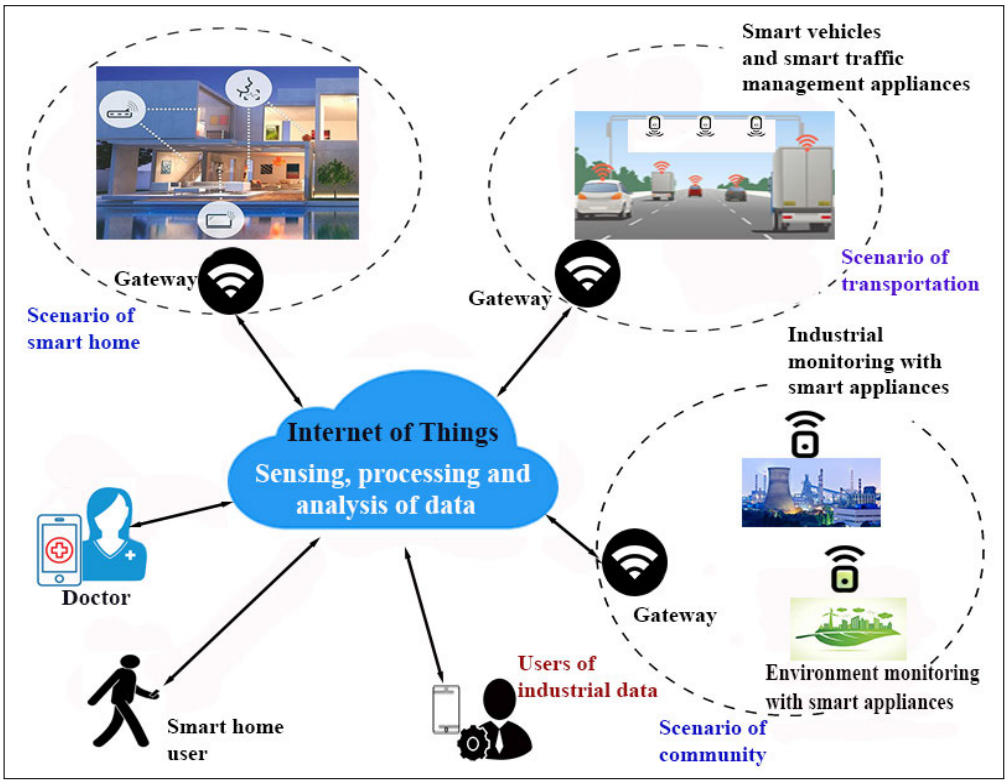

FIGURE 1. Generic architecture of IoT environment (adapted from [1]).

study are given in Section VII. Furthermore, future research challenges of malware detection in IoT/IoMT environment are provided in Section VIII. Finally, the work in concluded in Section IX.

II. OVERVIEW OF IOT COMMUNICATION ENVIRONMENT

In this section, we discuss various architectures of IoT communication environment (for example, IoT generic architecture and fog/edge based IoT architecture). Apart from that we have also discussed some of the applications of the IoT environment.

A. ARCHITECTURES OF IOT COMMUNICATION ENVIRONMENT

In the following, we have provided the details of the architectures of IoT communication environment. These architectures can be drawn on the basis of organisation and arrangement of the communicating entities.

1) GENERIC IOT ARCHITECTURE

The generic architecture of an IoT communication environment is given in Fig. 1. In this architecture, various scenarios, for example, scenario of smart home, scenario of transportation and scenario of community are provided. These scenarios consist of various smart devices, such as smart AC controller, smart TV controller, smart healthcare devices (i.e., smart pacemaker), and smart vehicles. These smart devices have unique IP addresses, and they can monitor and send the data to the servers for further processing using the gateways. Apart form that, this architecture also contains different types of users, such as a doctor who tries to access the data of smart healthcare devices using a smartphone, and a smart home user who tries to access the data of smart home appliances using the smartphone. To communicate in a secure way, a smart device and a user need to establish a session key by the help of certain number of exchanged messages which can be computed using some cryptographic operations [1], [3], [14]–[16].

2) FOG BASED IOT ARCHITECTURE

Another widely-used architecture of IoT communication environment is fog based IoT environment, in which various servers (i.e., fog servers and cloud servers) are used. The scenario of fog based IoT architecture is provided in Fig. 2. The entire architecture is divided into three layers: a) ''cloud layer'' where cloud servers are located, b) ''fog layer'' where fog servers are deployed and c) the bottom layer is ''end devices and user'' where all smart IoT devices (for example, smart pacemaker, smart vehicles, etc.) and different types of users (i.e., doctor, smart home user, etc.) are located. As we know the data produced by the smart devices is going to increase day-by-day. Therefore, the Internet infrastructure is not able to handle it properly. The combination of IoT and cloud computing was proposed to overcome this situation, but it was not sufficient to resolve the security issues. Therefore, CISCO came up with the new idea of ''Fog Computing''

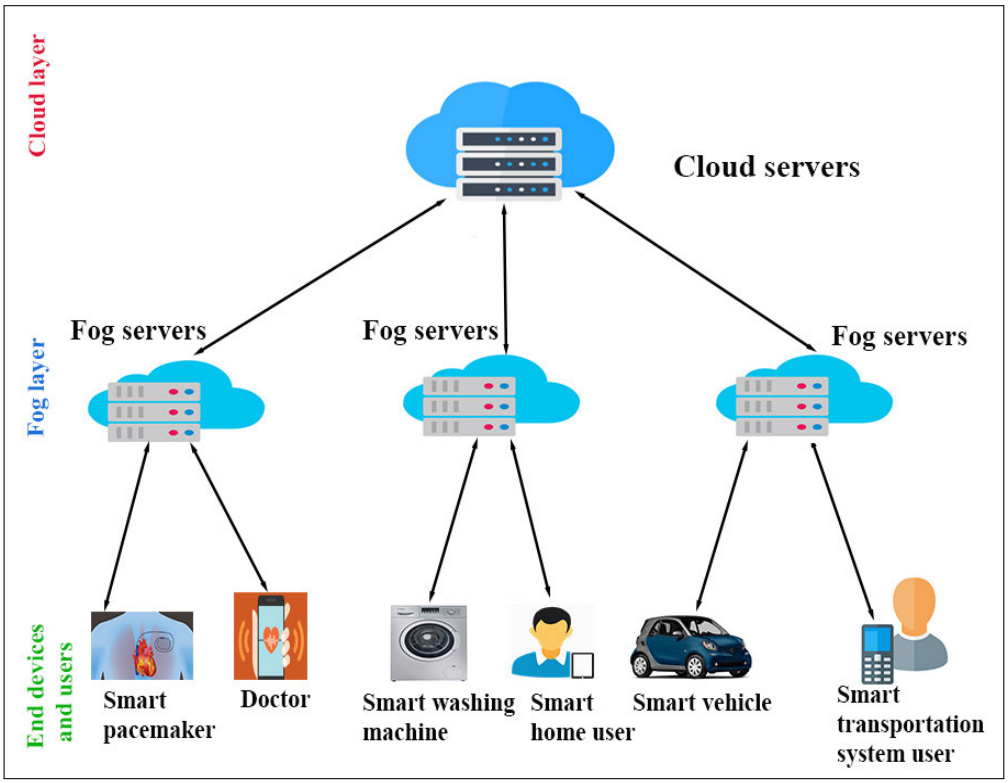

FIGURE 2. Fog based IoT architecture (adapted from [7], [17], [18]).

in 2012. Fog computing facilitates the work of cloud servers, and processes and manages the data near to IoT devices like a proxy that further reduces the end to end delay, saves the bandwidth of the network, and hence, it improves the performance. In this communication environment, the simple computing works are done by the fog nodes (servers), and the complex and computationally heavy works are done by the cloud servers. In fog based IoT environment, data analysis is performed near to the IoT devices which may be considered as a real time scenario of data analysis and is more vulnerable to various attacks and other breaches. Therefore, in such circumstances, the fog nodes confab with the adjacent nodes and then their combined accomplishment is used to find out the attacker systems by analysing the ongoing behaviour [17]–[19]. Furthermore, note that both ''generic IoT architecture'' in Fig. 1 and ''fog based IoT architecture'' in Fig. 2 can also be utilized for IoMT communication environment.

B. APPLICATIONS OF IOT/IOMT COMMUNICATION ENVIRONMENT

Various applications of IoT/IoMT communication environment are given below.

- **Wearable devices:** Health monitoring using the wearable devices is one of the hallmark applications of IoMT. Wearable devices such as ''Fit Bits'', ''heart rate monitors'' and smart-watches are very popular these days. There are also some other kind of wearable devices, such as Guardian glucose monitoring system, which was developed to treat the people suffering from diabetes. It monitors the level of glucose in the body of a patient by the help of a tiny electrode called as ''glucose sensor'' which is placed under the skin of the patient. It transmits the collected information through radio frequency to the associated monitoring device [4], [20]–[22].
- **Smart home applications:** Smart home is also one of great applications of IoT networks. A smart home is equipped with lighting, heating, cooling and other electronic devices which can be controlled remotely by using the smartphone or computing device. One of the best example of this kind of application is ''Jarvis'', which is an artificial intelligence (AI) based smart home automation system [3], [4], [15].
- **Healthcare IoT applications:** The reactive medical-based systems can be converted into proactive wellness-based systems with the help of IoT. In such a system, there are certain smart healthcare devices monitor and send the health data to the nearby node (i.e., cloud server). If a user (i.e. a doctor or a relative of a patient) is interested in the real-time access, it can be also performed by the help of IoT environment. Thus, IoT facilitates the access, processing and analysis of the valuable health data in real-time [14], [20], [22].
- **Smart cities:** These days most of the governments in many countries are working to convert their cities into smart cities. A smart city consists of components,

such as smart housing facility, smart traffic management, and many more. Each smart city has its own problems. For example, the problems that we have in Hong Kong city is much different than the New York city. Different cities have different issues (for example, limited amount of clean drinking water, increasing urban density and declined air quality index) that happen with different intensities in various cities. Therefore, these factors affect each city in a different way. Hence, the concerned organizations can use IoT environment for the analysis of these complex factors of township planning according to a specific city. The use of IoT applications can help to facilitate different challenging areas, such as drinking water management, waste water control, other waste control, housing planning, and other types of emergencies [23]–[26].

- **Smart agriculture:** The world population is going to increase day-by-day and it will reach around 10 billion in 2050. Therefore, in 2050 it will be very difficult to provide sufficient food to everybody. Hence, we need to improve our agriculture methods. We can utilize the new technologies such as ''Smart Greenhouse''. The greenhouse farming method improves the yield of the crops by controlling the environmental parameters which can harm the crops. Although the manual handling results in the production loss and energy loss, high labour cost further makes the entire process less effective. The greenhouse method utilizes the smart embedded devices which make monitoring easy and help us to control the environmental factors (i.e., temperature, humidity level, heat, etc.) inside the crop area [27]–[30].
- **Industrial Internet of Things:** The industrial Internet of Things (IIoT) is the combination of connecting machines and devices in industries (for example, electricity production, coal mining, oil, gas packaging and many more). In such kind of environment, the unplanned downtime and the system failures can cause human causality. A system embedded with the IoT aims to include smart devices, such as devices for monitoring the level of hazardous gases in a coal mining plant. These devices raise the alarm in case of any emergency situation which further helps to save the lives of the people working inside the plant [31], [32].
- **Smart retail:** The retailers have started use of IoT based solutions to make their job easy. The embedded IoT devices are used to improve the performance of overall production which further helps to increase the purchases, reduce the theft events, enable the inventory management and improve the overall consumer's shopping experience [33]–[35].
- **Smart supply chain:** The deployment of IoT devices helps in an effective management of supply chains. It provides effective supports for solving the complex problems such as tracking of goods while they are on the road or in transit. It also helps the supplier to exchange the inventory information among the intended entities. The factory equipment contains embedded sensors in the IoT enabled system which can transfer information according to the parameters (for example, pressure, temperature, and level of heat and utilization of the machinery). The deployed IoT system can also process work flow and change the equipment settings to optimize overall performance of the production and delivery [36]–[38].

III. SECURITY REQUIREMENTS IN IOT/IOMT COMMUNICATION ENVIRONMENT

In this section, we discuss different security requirements in IoT/IoMT communication environment including the general security requirements as required by other networks (i.e., smart grid and wireless sensor networks) [39]–[41]:

- *Authentication:* Authentication mechanism validates the identity of the communicating parties (identity authentication) or messages during the communication (message authentication). Before starting the secure communication, both sender and receiver mutually verify the identities. In an IoT communication environment, it involves different entities such as smart devices (i.e., IoT devices), different servers (i.e., cloud/fog servers), different users (i.e., mobile/static users), cloud service providers and gateways which require authentication among each other depending on the IoT applications.
- *Integrity:* Integrity refers to a method of ensuring that data is real and accurate. It means that the content of the received message does not contain false insertion, unauthorised deletion and modification during communication. We need to safeguard the data against any kind of unauthorized modification.
- *Confidentiality:* Confidentiality assures protection of information from being accessed by unauthorized parties. Sometimes, it is also called as ''privacy'' which assures that the exchanged messages in the channel should be protected against any kind of information disclosure attack.
- *Non-repudiation:* Non-repudiation assures that someone cannot deny the validity of something (i.e., message). It is widely used ''information security service'' which provides proof of the origin of message and the integrity of the data in that message. It makes very difficult to successfully deny who or where a message came from as well as the authenticity of that message. Digital signature mechanism offers non-repudiation (for example, in case of online transactions, it is decisive to ensure that a party to a contract (or a communication) can not deny the authenticity of his/her signature on a document). Non-repudiation can be further divided into the following two categories:
  - *Non-repudiation of origin*: It assures the genuineness of the sender, that is, the message was transmitted by the original party.

  - *Non-repudiation of destination*: It assures the genuineness of the receiver, that is, the message was received by the original party.
- *Authorization:* It is another security mechanism which is used to determine a user or device privileges (access levels) for system resources (for example, files, services, and other data applications). It is normally preceded by authentication mechanism for the identity verification of the user or device. The access rules are typically set by an authority (i.e., system administrator) which cover all the system and user resources.
- *Freshness:* It assures the freshness of information so that the previously exchanged messages should not be re-transmitted by an authorised party.
- *Availability:* Availability property assures that the information is only accessible to the authorized parties. If an attacker is not able to compromise confidentiality and the integrity of the ongoing communication, he/she may try to launch other types of attacks (for example, a denial-of-service against a web server to make the website unavailable to the legitimate users).
- *Forward secrecy:* If a device (i.e., smart IoT device) leaves an IoT communication environment, it must no longer have access to the future messages.
- *Backward secrecy:* When a new device (i.e., smart IoT device) is deployed in an IoT communication environment, it must not have any access to the messages which were already exchanged in the past.

IV. DIFFERENT CATEGORIES OF MALWARE

Malware (in short known as ''malicious software'') is a code or program file that is typically delivered over a network. It steals, infects or conducts some other malicious operations that an attacker wants to do. As per their functionality features, malware can be divided into different categories. Usually, they work to achieve following objectives [42]–[47]:

- It provides remote control to the attacker to use an infected system.
- It sends other malwares from the infected system to other targeted systems.
- It investigates the local network of the infected users' system to launch further malware attacks.
- It is used to steal the sensitive data (i.e., credit card information) from an infected system (i.e., IoT device and android phone)

A. SYMPTOMS OF MALWARE

The symptoms of malware program existence are as follows [44], [48]–[51]:

- We may get the appearance of strange programs, icons or files on the home screen of the devices.
- The programs run without permissions and out of control, re-configuring themselves. Sometimes malware reconfigure or turn off anti-virus or the deployed firewall(s).
- We may observe strange system behaviors (for example, the emails or messages being sent automatically and without someone's knowledge).
- In case of IoMT, we may also observe the malfunctioning of smart medical devices (for example, unwanted secretion of insulin from an implanted blood glucose monitoring system).

B. MALWARE TYPES

Different varieties of malware are possible, which are described below [42]–[45].

- **Spyware:** It is a type of malware which works by spying the user activity without their consent. The malicious activities like collecting keystrokes, activity monitoring, harvesting of data i.e., account's credentials, financial data- credit card numbers, are possible in the network. It may also modify the security settings of the software. It exploits through software vulnerabilities, and attaches itself with some normal program.
- **Keylogger:** It is a malicious piece of code which is used by a hacker to track the keystrokes of the users. Everything that a user types through the keyboard (for example, their login information, ID and passwords) have been recorded. A key logger attack is more powerful than brute force or dictionary attack. This malicious program first tries to get into a user's device by tricking into downloading it by clicking on a link in an email. It is one of the dangerous malwares as strong password does not provide much protection against it. Therefore, it is suggested to use multi-factor authentication (MFA) (i.e., combination of username, password, smart card as well as biometrics data).
- **Trojan Horse:** This malware masquerades itself as a normal program to trick users into downloading and installing it. It helps the hacker to get an authorized remote access to an infected system. Once the hacker gets the access to the infected system, he/she can steal the sensitive data (for instance, financial data- account number and credit card number). It can further install other malicious programs in the system to perform other malicious activities.
- **Virus:** This malicious program is capable of copying itself and spreading to other the systems. It spreads to other systems by attaching itself to different programs and then executing the code if a user starts one of these infected programs. It can be used to steal information, harm the host system and build botnets.
- **Worm:** It spreads over a network by finding out the weaknesses in the operating system. It causes harm to their host networks through bandwidth consumption and overloading of web servers. It may contain the payload to damage a host system. The hackers commonly use this to steal sensitive data, delete files or create a botnet. Worms are self-replicated in nature and they spread independently whereas viruses need some

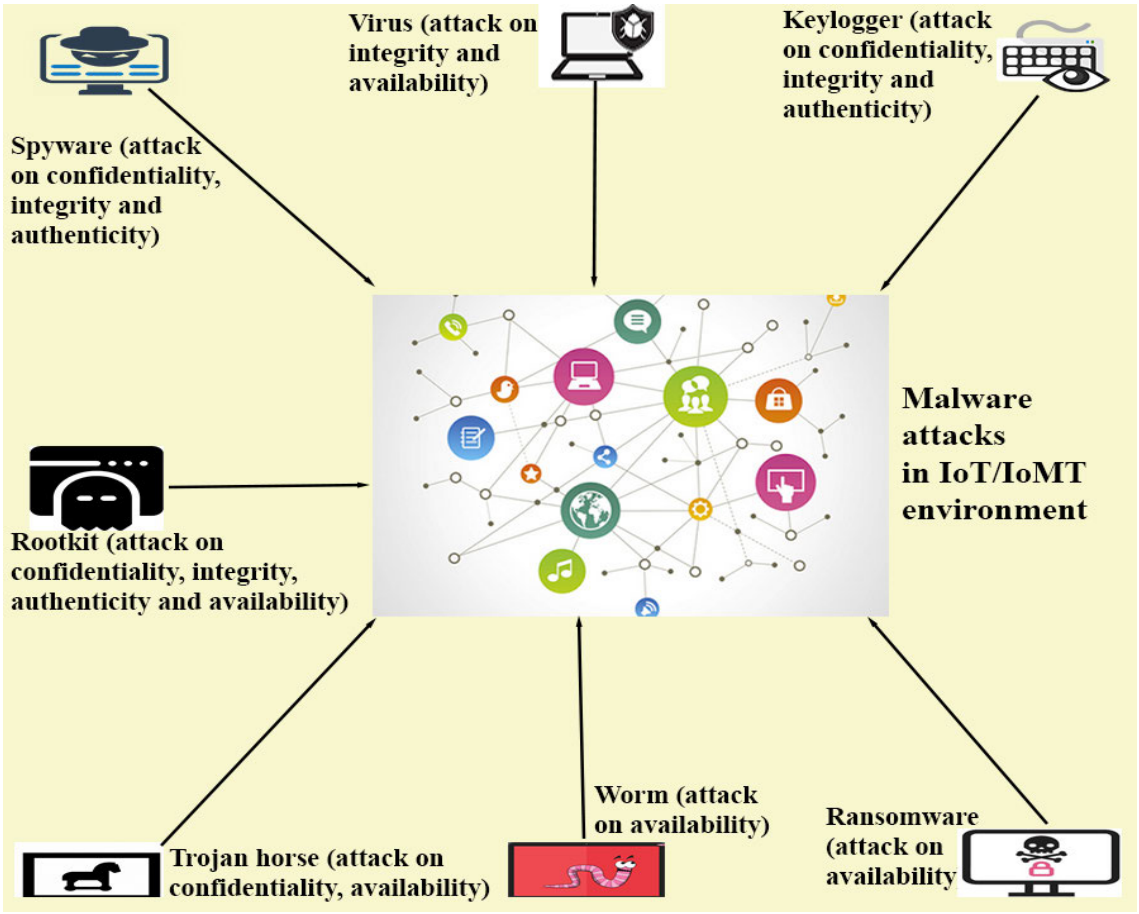

FIGURE 3. Different types of malware attacks in IoT/IoMT environment.

human involvement to spread (for example, execution of malicious a program and opening of a infected file). Worms spread through emails which contain the infected attachments.

- **Adware:** It is also called as advertising-supported program (software). It automatically delivers advertisements as per its functionality. One of the common examples of adware is pop-up advertisement on websites.
- **Ransomware:** It is a different kind of malware which essentially holds a machine (i.e., IoT device) and asks its owner to pay some money (ransom). It restricts user access to the machine (i.e., android phone) through encryption on the files of the hard drive or by locking the system. It then displays messages to force the user to pay the ransom to the owner of the malware. After that ransomware's owner provides the key to decrypt the encrypted files on the hard drive. It typically spreads through the downloaded files or through some other vulnerabilities in the system or networking software.
- **Rootkit:** It is one of the malignant kinds of malicious malwares. Hackers can use rootkit to remotely access (control) a machine (i.e., IoT device) without being detected by its user or the deployed security appliances. Once it is successfully installed in the system, the hacker can remotely execute files, steal the sensitive data, modify system configurations and alter the functionality of the security software. Its detection and prevention are very difficult because of its stealthy character. A rootkit always tries to hide its presence, and then the security appliances are not that effective for its detection and removal. Therefore, its detection depends on manual methods (for example, behaviour of the machine (behaviour based detection)), signature scanning and static analysis). We should always try to patch the existing vulnerabilities in the operating system of the machines (i.e., IoT devices).

The details of various types of malware attacks in IoT/IoMT communication environment is also provided in Fig. 3. In this figure, we highlight different types of IoT malwares such as spyware which can attack on the confidentiality, integrity and authenticity of the data or system resources, keylogger which can attack on confidentiality, integrity and authenticity of the data or system resources. Moreover, the trojan horse can attack on confidentiality, availability of the data or the system resources whereas a virus can attack on integrity and availability of the data or system resources. Furthermore, worm can attack on availability

TABLE 2. Types of malware.

Malware type	Attacks performed by an attacker
Spyware	It can attack on confidentiality, integrity and authenticity of available resources
Keylogger	It can attack on confidentiality, integrity and authenticity of various resources
Trojan horse	It can attack on confidentiality and availability of system resources
Virus	It can attack on integrity and availability of system resources
Worm	It can attack on availability of the data or other network resources
Ransomware	It can attack on availability of system resources
Rootkit	It can attack on confidentiality, integrity, authenticity and availability of the data or system resources

of the data or system resources, ransomware can attack on availability of the data or system resources. However, rootkit seems the malignant one as it may attack on confidentiality, integrity, authenticity and availability of the data or system resources [44], [48]–[51]. The summary of these malware attacks is also provided in Table 2.

V. CASE STUDY: RECENT MALWARE ATTACKS IN IOT COMMUNICATION ENVIRONMENT

Some of the active botnets which can launch various malware attacks in IoT environment are discussed below.

A. MIRAI

Attacks by Mirai botnet are still going on. Mirai is a kind of malware which provides the control of Linux operating system based network device to the remote bots. These devices can be again used as a part of botnet to perform other malicious attacks with a broader coverage. It primarily targets smart IoT devices, such as the Internet-connected consumer devices (for example, IP cameras and other smart home appliances). According to the report of Fortinet, Mirai was one of the most active botnets in 2018. Furthermore, Mirai botnets came up with some extended features and were able to turn the infected IoT devices into the ''swarms of malware proxies''. Based on the report of Fortinet, Mirai targeted the devices for both known and unknown vulnerabilities. Cryptomining shows up as a significant change in the botnet world. A hacker can use the hardware as well as electricity of victim's system to earn the cryptocurrencies by using this malware. These malicious minds are experimenting how to use IoT botnets to make money [52]–[56].

B. REAPER

Reaper is also called as *IoTroop*. In the fall of 2017, information security researchers discovered a new botnet (IoTroop) with improved functionality features. It can compromise smart IoT device very quickly as compared to the Mirai botnet. It has other severe effects as it can bring down the entire infrastructure very quickly. Mirai infectes the smart IoT devices which use default usernames and passwords. However, reaper is more severe which targets nine different vulnerabilities in the devices of different makers, such as D-Link, Netgear and Linksys. Using this botnet, the attacker could also change the malware code to make it more devastating. As per the information provided by ''Recorded Future'', it was also used to attack on some EU banks (for example, ABN Amro) [56]–[58].

C. ECHOBOT

It was discovered in the beginning of the year 2019. It is a variation of Mirai which uses twenty six malicious scripts to spread itself. Similar to other botnets, it takes the advantage of unpatched smart IoT devices and then uses these vulnerabilities to harm other applications of the enterprise (for example, weblogic of oracle). It was discovered by ''Palo Alto Networks'', and designed to create a larger botnet to execute more devastating DDoS attacks [56], [59].

D. OTHER POTENTIAL ATTACKS

Emotet, *Gamut* and *Necurs* are other existing botnets which are used to launch malware attacks in IoT communication environment. The motive behind these botnets is to discharge spam in an enormous amount to deliver the required payload. It is also used to get victims to perform some other malicious tasks.

Emotet: It is used for stealing emails from the mailboxes of the target. It can allow the attackers to craft the malicious messages to fool the recipients. Hackers can also launch this attack to abduct the credentials of SMTP, which will be helpful to take control over the email accounts of target.

Gamut: It is also specialized in spam emails and it first tries to establish a relationship with the target machine (victim). It can perform this through dating or some other kind of job offer.

Necurs: This is used to launch ransomware attack and also some other forms of digital extortions. As per the report of Cisco, it is still in the operation mode and can launch devastating attacks [56], [60].

The summary of malware attacks is provided in Table 3. Furthermore, it is noted that malware attacks discussed in Section V are also possible in IoMT environment.

VI. TAXONOMY OF SECURITY PROTOCOLS IN IOT ENVIRONMENT

In this section, we provide the details of security protocols used in IoT communication environment which provide security to the exchanged data well as to the stored data. A taxonomy of security protocols in IoT communication environment is given in Fig. 4. These security protocols are also applicable to provide the security in IoMT.

TABLE 3. Summary of malware attacks in IoT/IoMT environment.

Malware attack	Characteristics	Countermeasures
Mirai	The malware used in Mirai provides the control of Linux operating system based network device to the remote bots.	**Solution 1:** Network-based anomaly detection (N-BaIoT) to extract behavior snapshots by using deep auto-encoders [61]. **Solution 2:** IoT honeypot which operates with manual and Mirai-based attacks in which a multi-component design was implemented to get sufficient exposure to malicious traffic [54].
Reaper	It is more advanced than Mirai which could bring down the entire infrastructure very quickly. It is more severe which targeted nine different vulnerabilities in the IoT devices. Attacker could also change the malware code to make it more devastating.	**Solution 1:** It detects the botnet using the machine learning methods, a collection of algorithms in a layered hybrid method [58]. **Solution 2:** A detection method (EDIMA) was proposed which was a kind of distributed modular mechanism. It could be used for the detection of IoT malware in a large-scale network [57].
Echobot	It is a variation of Mirai which uses 26 malicious scripts for spreading.	**Solution 1:** as suggested in [61]; **Solution 2:** as suggested in [54].
Emotet	It is used for stealing emails from the mailboxes of the target. It can be launched to abduct the credentials of the "Simple Mail Transfer Protocol (SMTP)", which will be helpful to take control over the email accounts of target.	No such particular solution is available. **Solution 1:** as suggested in [61]. **Solution 2:** as suggested in [54].
Gamut	It is specialized in spam emails and first try to establish a relationship with the target machine.	No such particular solution is available. **Solution 1:** as suggested in [61]. **Solution 2:** as suggested in [54].
Necurs	It is used to launch ransomware attack and also some other form of digital extortion.	No such particular solution is available. **Solution 1:** as suggested in [61]; **Solution 2:** as suggested in [54].

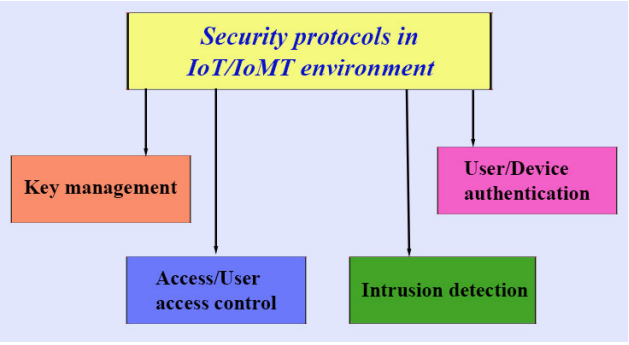

FIGURE 4. Taxonomy of security protocols in IoT/IoMT environment [39].

A. KEY MANAGEMENT

A key management protocol deals with the management, distribution and establishment of cryptographic keys among communicating entities of IoT/IoMT environment. The entire procedure is divided into several phases such as key generation, key exchange, key usage and key revocation as per the requirement. The key management mechanism uses a "cryptographic procedure" which provides the details of the key servers (i.e., trusted entity of the system), different types of users (i.e., mobile or static) and different devices (i.e., IoT devices). We should have a robust key management procedure to perform a secure communication [17], [62]–[65].

Most of the time, a key management scheme typically contains following phases:

- *Pre-deployment phase:* In this phase, a trusted party also called as trusted authority (*TA*) define various parameters for different network entities. It also does the registration of communicating entities, in an IoT environment it may include the registration of IoT devices, various types of users and other involved parties and devices. After performing the registration, the generated and registered data is stored in the memories of the devices and then the devices will be deployed in the different locations of the network.
- *Key generation and distribution:* In this phase, the trusted party of the network *TA* generates the different cryptographic keys (i.e., secret key) for various network entities. It can be further divided as per "symmetric key cryptography" and "public key cryptography" mechanisms. In a "symmetric key cryptography" technique, the entities who or which are going to start the communication should have to share a secret key which they must exchange in advance. After the successful key exchange they can start the secure communication. Most of the time the neighbor devices use their pre-loaded secrets (i.e., credentials) to establish the secret pairwise keys among them as suggested in some key pre-distribution schemes [66]–[79]). However in a "public key cryptography" technique, the key distribution of public keys is done by a trusted authority also called as public key server. In this mechanism, a communicating party generates a pair of keys and then it holds one key privately and announces the other key publicly. Most of the time *TA* generates the pair of public and private keys for a particular entity and then stores the private key in the memory of that device, make the announcement of the other key publicly so that the communicating parties can use it to communicate in a secure way.
- *Key establishment phase:* After the successful registration and deployment of various network entities (i.e., IoT device) the entities can start the process of key establishment. For this purpose first the devices compute some parameters and then they exchange these parameters with the other parties by the help of message exchange. After the receiving of these messages a communicating

party computes the secret key (i.e., session key) and then hide this inside some other message and sends to the other party. After receiving these messages, the other party also computes the secret key (i.e., session key) using the received parameters and verifies it by the help of the received messages. After the successful mutual agreement both parties establish this key for their secure communication which will happen in the future [17].

- *Key revocation and dynamic device addition phase:* It is very often in an hostile (i.e., unattended) environment for example, a war zone that some of network devices (for example, IoT sensors) may be physically captured by an enemy (physical adversary). After performing this malicious event the adversary can extract the secrets for example, private key stored in that device by the help of power analysis attacks [80]. Under these circumstances, *TA* has to deploy new devices in the deployment area. To perform this task *TA* again generates a new pair of keys (public and private) and then stores the required parameters in the memory of that device and installs that in the network. *TA* also announces the information of dynamic device addition to the other parties of the network. So that other parties can start their secure communication with this newly installed device [81].

B. USER AUTHENTICATION/DEVICE AUTHENTICATION

User authentication is a process of identification and verification of the identities of the communicating parties. Most of the time, the communicating parties (i.e., a user, smart medical device) verify their identities among each other. This process is also called as mutual authentication. In user or device authentication mechanism, one communicating entity (i.e., device or user) verifies the identity of the other communicating entity (user or device). After performing the successful mutual authentication, the communicating parties establish a session key for their future communication. Device authentication is also performed in the similar way. For the interest of simplification, we provide the details of user authentication procedure here. A user authentication protocol for IoT environment exhibits following phases [3], [31], [81]–[87], [87]:

- *System setup and pre-deployment phases:* In these phases, *TA* selects some system parameters and also does the registration of different devices (i.e., IoT device), gateway, cloud server) in the offline mode. After the successful registration, the devices are deployed in the targeted area [14].
- *User registration phase:* In this phase, a user does the registration of himself/herself in a secure way. The user can access the real-time information from a desired device (i.e., smart medical device). To perform the registration, user first chooses his/her credentials (for identity, password and biometrics information), and then sends these information to the trusted entity i.e., *TA* using a secure channel (for example, in person or through some other secure channel). After completing these steps successfully, the *TA* hands over a smart card or other some device (i.e., mobile device) to the legitimate registered user in a secure way after storing the useful data in the memory of the device [3], [81], [88].
- *Login phase:* In this phase, a registered user provides his/her credentials and biometrics to a specific device or to mobile device (i.e., smartphone). Then the device verifies the authenticity of the user. If he/she is valid user, the device computes a login request message and sends that to next communicating party (for example, a gateway) through the insecure channel.
- *Authentication and key agreement phase:* After receiving the login request message from the other entity (i.e., user), an entity preforms remaining steps as per the following details. The receiving party first verifies the authenticity of the message. If this occurs successfully, the receiving party calculates an authentication reply message containing the generated session key, and then sends it back to the previous party through the insecure channel. After receiving the message, the same entity computes the session key by the help of secrets (for example, using the short & long-term secrets) which are known and available to the receiving party. After performing successful mutual authentication between the user and the receiver (for example, a smart medical device), the parties establish a session key (secret) to secure their communication in the future.
- *Password and biomertic update phase:* It is always good to add more and more security and functionality features in a designed user authentication scheme. Therefore, in a secure and user friendly user authentication scheme, it is recommended to provide a password and biometrics update procedure. By performing the steps of this procedure, the original user can change his/her password and biometric information using his/her device (i.e., smart card) with or without communicating with the *TA*. To reduce the communication and computational overheads, it is desirable to execute this phase locally without involving the *TA*.
- *Dynamic device addition phase:* Sometimes the devices (for example, smart medical devices) get fail or may be physically stolen by an adversary because of the lack of physical security. In these circumstances, it is necessary to deploy new device in place of that device. To fulfil this work *TA* again computes the new credentials for that new device and stores them in its memory. Then that device will be installed in the required area. However, *TA* has to inform about this addition to the other parties of the network (for example, users) who want to access the real-time data from the added device.

These days two factor and three factor user authentication schemes are commonly used. These schemes provide security as per the available factors. The three factors are like user's credentials (username and password), user's smart card and user's biometrics data (i.e., fingerprints).

C. ACCESS CONTROL/USER ACCESS CONTROL

Access control is a process which limits the access of the user/device to the resources of the system or network. In this mechanism, the user/device has been granted access and privileges to different available resources. To improve the lifetime of the IoT/IoMT communication environment, it is needed to add the new devices (i.e., smart devices) in the network. This happens when devices stop their working due to battery depletion or physical capturing of those devices [80]. Moreover, an adversary can install his/her malicious device devices in the network [89], [90]. Hence, it becomes essential to differentiate between an original device and a malicious device. Therefore, we require to design secure access control schemes to stop the entry of the malicious devices in the IoT/IoMT environment [91]–[94].

The following steps need to be performed in an access control scheme:

- *Node authentication:* When a device/node (for example, smart medical device) is newly installed in the IoT/IoMT communication environment, it must authenticate itself to the other neighbor device. It provides assurance that it is an original device which is allowed to access the information from its neighbor devices.
- *Key establishment:* When a device/node (for example, smart medical device) is newly installed in the IoT/IoMT communication environment, then it should be able to establish shared secret keys with its neighbor devices to secure the future communication. This can be done properly, if this device authenticates with its neighbor devices successfully.

As per the authentication procedure, the access control schemes can be divided into two categories.

- *Certificate-based access control*: In a ''certificate-based access control scheme'', a digital certificate (for example, X.509 certificate [95]) may be stored in each deployed device by the *TA*. Then, the pre-loaded certificate is used to prove a node's identity to its neighbor nodes.
- *Certificate-less access control*: In a ''certificate-less access control scheme'', most of the time the hash-chain based process is followed.

Moreover, to provide access right only to the legitimate users for various services, the information and resources available in IoT/IoMT environment, user access control schemes are much needed.

D. INTRUSION DETECTION

An Intrusion Detection System (IDS) is used to monitor and analyze malicious activities inside a network or in a system. It detects and defends various devices (for example, smart medical devices) from the possible attacks. The deployed IDS in an IoT/IoMT environment monitors and verifies all traffic (normal and malicious), and then detects the possibility of malicious signs. If it discovers any malicious activity, the associated component takes the proper action (for example, send information to the administrators or block the of malicious IP address of that source). In IoT/IoMT environment, there are chances that an adversary may physically capture some of the devices (i.e, IoT devices). The adversary can then try to extract the sensitive information from that device by the application of power analysis attacks [80]. After that the adversary may deploy his/her malicious devices by storing the extracted information in that malicious device. These malicious devices may have some inbuilt features to launch other devastating attacks, such as some kind of routing attacks (for example, blackhole, wormhole, misdirection and sinkhole attacks) [89], [90], [96], [97]. Under the influence these attacks, the exchanged data packets may be disclosed, modified, dropped or delayed before forwarding them to the destination. This results in the severe degradation in the performance of the ongoing communication. For example, it may have increment in ''end-to-end delay'', and reduction in ''network throughput'' and ''packet delivery ratio'' [89], [97]. Furthermore, IoT environment can also be attacked through the use of the botnets in which the attacker systems may try to install malware (malicious programs) in the memory or the operating system of the IoT devices. This results in malfunctioning of the IoT/IoMT devices. Under the influence of such an attack, the devices may stop their working or they may work in an inappropriate way. Such kinds of cases are severe under some particular circumstances (for example, an implanted smart pacemaker can give shock to a patient which may become the reason of his/her death). Therefore, it becomes essential to protect the IoT communication environment from intrusion. The deep study of intrusion detection protocols in IoT environment is thus necessary [9]–[11], [14], [43], [44], [56], [98].

The functioning of an IDS is based on the following [99], [100]:

- It identifies the sign of an intruder.
- It provides information about the location (i.e., suspected IP address) of the intruder.
- It logs the information of ongoing activities.
- It tries to stop the malicious activities, if they are detected.
- It then reports the information of malicious activities to the administrator (i.e., intrusion behaviour that is either active attack or passive attack).
- It also provides information about types of the intrusion (for example, which types of attack–mirai or echobot).

On the basis of the deployment, an IDS can be divided into two classes: a) ''network based intrusion detection system (NIDS)'' which detects intrusions over a network (i.e., snort) and b) ''host based intrusion detection system (HIDS)'' which detects intrusions inside a system (i.e., malware infection in a operating system of a IoT device). Furthermore, an IDS mechanism can be divided into three categories: a) anomaly based detection, b) misuse based detection, and c) specification based detection [99], [100]. These mechanisms can be briefed as follows.

- *Anomaly based detection:* This detection mechanism works on the basis of certain statistical behavior methods. It tries to identity two different types of flows (i.e., the network traffic flow), normal flow and abnormal flow (flow under attack). If it detects any deviation from the normal behavior, it will raise an alarm. It also has certain drawback as we have to update the normal behavior database as per the changes happen in the network on regular basis. However, it has some benefits as it can detect the anomalies accurately and consistently with low false negatives and positives. Hence, it is very useful for the detection of unknown attacks. This type of detection mechanism is always very useful for the detection of new kinds of malwares in IoT environment.
- *Misuse based detection:* Sometimes it is also called the rule based or signature based detection. Signature is something that is closely associated with an anomaly (i.e., virus) and this will be generated when such an anomaly affects the system. The signatures of known attacks are used to detect such types of attacks in the future. The benefits of this mechanism are that it can detect the known anomalies accurately and efficiently along with a low false positive rate. Most of the anti-viruses (or anti-malware) installed in the systems come under the category of misuse based detection.
- *Specification based detection:* The specifications and constraints to describe the correctness of the detection process are needed to define in this mechanism. After that the behavior of the system or network as per the specifications and constraints is monitored and analyzed. It is also capable to detect the unknown attacks. It utilises the advantages of both anomaly and misuse based detection mechanisms by the help of manually defined specifications and constraints to diagnose the abnormal behavior. On the basis of its working, this mechanism seems like an anomaly based detection as it detects the attacks on the basis of deviation from the normal behaviour. At the same time, it works on the basis of manually defined set of constraints and specifications. It further induces low false positive rate as compared to the anomaly based detection mechanism. However, this mechanism has some drawbacks (for example, high time consumption because we need to define and develop the set of specifications and constraints which requires some time). The researchers working in the domain of ''malware detection'' (specially zero-day malware attack) try to propose their methods by making the use of specification based detection mechanisms as it performs their detection in an effective and efficient way along with less number of false positives and false negatives.

VII. MALWARE DETECTION SCHEMES IN IOT/IOMT COMMUNICATION ENVIRONMENT

In this section, we summarize different malware detection schemes in IoT/IoMT communication environment. Furthermore, we also provide a comparative study on malware detection schemes which can be utilized to malware detection in IoT communication environment.

A. EXISTING MALWARE DETECTION SCHEMES IN IOT/IOMT COMMUNICATION ENVIRONMENT

Various schemes of malware detection in IoT/IoMT environment are discussed below.

Kumar *et al.* [2] proposed a ''blockchain and machine learning based malware detection'' mechanism for IoT devices. The mechanism of machine learning automatically extracts the malware information using the clustering and classification algorithms and then stores the information in the blockchain. The proposed framework uses the blockchain to store the genuine information of the extracted features in a ''distributed malware database'' to improve the performance of run-time malware detection with high speed and accuracy.

Lei *et al.* [101] proposed an IoT malware detection technique named as ''EveDroid''. It is a scalable and event-aware malware detection mechanism for smart IoT devices that captures high level semantics of Android applications in IoT environment. In their mechanism, the authors introduced the concept of function clustering which automatically transforms the application programming interface calls to feature vector on the basis of semantics. This made the detection system more strong against such a malware.

Nguyen *et al.* [102] proposed a ''graph-based convolution neural network (CNN)'' mechanism for the detection of IoT botnets, which can launch malware attacks. During their experimentation, it was observed that their proposed method reliably classified the benign and IoT malware with an improved accuracy.

Dinakarrao *et al.* [103] proposed a ''HaRM malware detector'' which used the low computational cost machine learning classifier for the best utilization of the IoT resource to detect the IoT malware. They also achieved a good detection accuracy. The outcomes of the HaRM detector could be utilized to generate the estimation of infection state, which can be further used to control the spreading of malware.

Shen *et al.* [19] proposed a method for malware detection in the fog-cloud-based IoT communication environment. They selected all smart objects which could be deployed with the IDS agents (monitoring nodes). The working of monitoring nodes is to receive and forward the audit data via the border routers to the corresponding fog node. In their approach, the intrusion detection was performed by calling the IDS service provided by a cloud platform.

Su *et al.* [104] proposed a method for the detection of distributed denial-of-service (DDoS) malware in IoT environment. They extracted the malware images (for example, a one-channel gray-scale image converted from a binary code of malware) and then used a light-weight ''convolutional neural network (CNN)'' for the classification of their families. Their proposed mechanism achieved around 94.0% accuracy for the classification of goodware.

Further, note that some malware detection schemes which were discussed in this section can be also applied for the

TABLE 4. Comparison of performance of existing schemes.

Scheme	Method used	Accuracy	F1-measure
Kumar *et al.* [2]	Blockchain and machine learning based detection	98.00%	98.00%
Lei *et al.* [101]	EveDroid	N/A	99.00%
Nguyen *et al.* [102]	Graph-based convolution neural network (CNN)	92.00%	94.00%
Dinakarrao *et al.* [103]	HaRM malware detector	92.21%	N/A
Su *et al.* [104]	Light-weight convolutional neural network (CNN)	94.00%	N/A

Note: N/A: not available

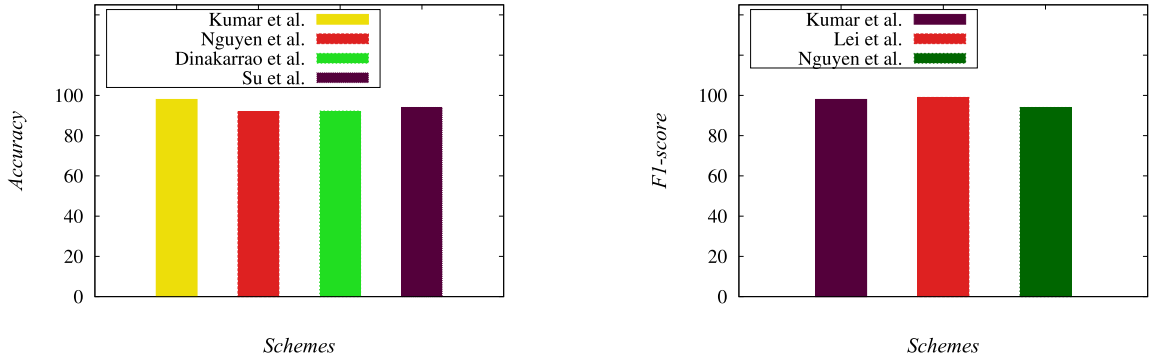

FIGURE 5. Performance comparisons of different schemes: (a) Accuracy, (b) F1-score.

detection of the IoMT malware. For that purpose, we need to do certain amendments in the detection mechanisms.

B. COMPARATIVE STUDY OF MALWARE DETECTION SCHEMES IN IOT/IOMT COMMUNICATION ENVIRONMENT

In this section, we perform a comparative analysis on the performance of various existing IoT/IoMT malware detection schemes. In these schemes, various performance parameters such as precision, recall, accuracy and F1-score are used which are explained below in Eqs. (1), (2), (3) and (4). All these parameters are computed on the basis of true positive (TP), false positive (FP), true negative (TN) and false negative (FN). If a normal program is detected as a normal program by malware detection scheme, it is called as ''true negative (TN)''; whereas if a normal program is detected as a malicious program by malware detection scheme, it is called as ''false positive (FP)''. Similarly, if a malicious program is detected as a malicious program by malware detection scheme, it is called as ''true positive (TP)''; whereas if a malicious program is detected as a normal program by malware detection scheme, it is called as ''false negative (FN)'' [2], [19], [89], [90], [96], [97], [101]–[104].

- **Precision:** It is also called as positive predicted value. It is the fraction of the correctly identified intrusion cases to the all predicted positive cases of intrusions. The formulation of precision is given by

$$\text{Precision} = \frac{TP}{TP + FP}. \tag{1}$$

- **Recall:** It is also called as true positive rate or detection rate or sensitivity. It is a fraction of correctly identified intrusion cases to the all real positive cases of intrusions. This is estimated by the following formula:

$$\text{Recall} = \frac{TP}{TP + FN}. \tag{2}$$

- **Accuracy:** It is one of the most important parameters which is measured as the all correctly identified cases. Thus, it is important to use it when all the classes are equally important. This is mathematically expressed as follows

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN}. \tag{3}$$

- **F1-score:** It is also called as F1-measure that can be computed through the harmonic mean of ''precision'' and ''recall''. It provides the exact estimate of the incorrectly classified cases than the ''accuracy'', and can be represented as

$$\text{F1-score} = \frac{2(\text{Precision} \times \text{Recall})}{\text{Precision} + \text{Recall}}. \tag{4}$$

Furthermore, the performance comparison of the schemes of Kumar *et al.* [2], Lei *et al.* [101], Nguyen *et al.* [102], Dinakarrao *et al.* [103] and Su *et al.* [104] is provided in Table 4. The schemes of Kumar *et al.* [2], Nguyen *et al.* [102], Dinakarrao *et al.* [103] and Su *et al.* [104] achieve the accuracy of 98.00%, 92.00%, 92.21% and 94.00%, respectively. However, the schemes of Kumar *et al.* [2], Lei *et al.* [101] and Nguyen *et al.* [102] achieve the F1-measure of 98.00%, 99.00% and 94%, respectively. The comparisons of accuracy and F1-scores are also provided in Fig. 5(a) and Fig. 5(b), respectively. Therefore, Kumar *et al.*'s scheme [2] achieves better accuracy, whereas Lei *et al.*'s scheme [101] archives the maximum F1-measure.

VIII. FUTURE RESEARCH CHALLENGES AND DIRECTIONS OF MALWARE DETECTION IN IOT/IOMT ENVIRONMENT

In this section, we discuss some of the future research challenges and directions of malware detection in IoT/IoMT environment.

A. FOOLPROOF SECURITY

The malware detection and prevention techniques proposed in the literature do not provide full proof security against various types of malware attacks. Moreover, some of them are attack specific and do not work for other types of attacks at the same time. Therefore, we need to design such kind of malware detection techniques for IoT/IoMT security which should be robust against multiple malware attacks at the same time. Hence, designing of such kind of techniques can be a challenging problem.

B. EFFICIENT MALWARE DETECTION TECHNIQUES

IoT/IoMT communication environment consists of resource constrained devices, such as smart IoT devices which have less computation power and storage capacity along with short battery life. Therefore, we can not use them to perform computation, communication and storage intensive operations as it requires more resources. Hence, we can not use heavy deep learning algorithms for the malware detection for IoT/IoMT devices. Therefore, we need to design malware detection and prevention mechanisms in such a way that the proposed mechanisms should exhibit less computation cost, communication cost and storage cost without compromising the security needs.

C. SCALABILITY OF MALWARE DETECTION SCHEME

IoT is a kind of large scale heterogeneous network of different communication paradigms and applications, which have their own capabilities and requirements. In that way, malware detection for IoT communication environment could be a challenging job. In such a environment, we can have the ''Electronic Health Records (EHRs)'' of certain users which are stored in an IoT-enabled cloud server for further processing. The different devices inside the ''Body Area Network (BANs)'' produce data and send that to the cloud server. Therefore, it constructs a heterogeneous network of different communicating devices. We need a specific type of malware detection mechanism which can protect all types of devices of such kind of communication environment. Hence, more deep research study is needed in this direction.

D. HETEROGENEITY OF IOT COMMUNICATION ENVIRONMENT

IoT communication environment is very different in nature as we have various of types of devices range starting from full-edged laptop systems, desktop systems, personal digital assistants end up to low powered sensing devices and RFID tags. Moreover, these devices work as per the principles of various types of communication protocols. It is also crucial to notice that these devices are different in terms of their storage capacity, computation power, communication range and underlying operating system. Henceforth, we need to design a malware detection mechanism in such a way that it can support and protect all different types of devices and underlying technologies.

E. CROSS-PLATFORM MALWARE DETECTION

The heterogeneity of IoT networks creates a problem when we plan to deploy a malware detection mechanism. This property facilitates the interconnection of various application domains. However, it also creates challenges for designing an effective malware detection mechanism. For instance, when a smart home application requires to access the data from a healthcare monitoring device, the malware detection mechanism should be compatible and strong so that application can access the data from the target network without any problem. At the same time, it is also important to notice that the data stored over the cloud requires effective malware detection and prevention mechanisms. Henceforth, in such kind of applications we need to design strong and efficient malware detection mechanism to provide an uninterrupted connectivity across different IoT platforms.

F. USE OF BLOCKCHAIN IN MALWARE DETECTION

The operations of blockchain can be used to secure various communication environments. It is because the blockchain operations are decentralized, efficient and transparent. Blockchain operations can also be utilized in efficient detection of the malware in IoT/IoMT environment. In such kind of detection method, we can create a block containing the information about the malicious programs (i.e., malware) to add in the blockchain. Since the blockchain is available to all authorized parties, these parties can have access to the information of the existing malware attacks on the system. Thus, malware detection can be performed in an effective way. Till today, very few blockchain-based malware detection schemes are proposed in the literature. Therefore, designing of blockchain based malware detection scheme can also be a future research challenge [2], [105].

IX. CONCLUSION

IoT/IoMT based applications facilitate our everyday life. However, there is also a dark side of this, because it suffers from various security and privacy issues. We have noticed that malware attacks launched by Mirai, Reaper, Echobot, Emotet, Gamut and Necurs botnets are active these days. Therefore, it becomes crucial to provide effective and efficient solutions for malware attacks occur in IoT/IoMT environment. In this review work, we have done a study of various types of malware, and their symptoms. We have also discussed some of the architectures of IoT/IoMT environment along with their applications. A taxonomy of security schemes in IoT/IoMT environment is also highlighted. Moreover, we have provided a comparative study of various existing schemes for malware detection and prevention in IoT/IoMT communication environment. Some of the future

research challenges and directions of malware detection in IoT/IoMT environment are also highlighted.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and the Associate Editor for their valuable feedback on this article which helped us to improve its quality and presentation.

REFERENCES

[1] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E.-J. Yoon, and K.-Y. Yoo, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.

[2] R. Kumar, X. Zhang, W. Wang, R. U. Khan, J. Kumar, and A. Sharif, "A multimodal malware detection technique for Android IoT devices using various features," *IEEE Access*, vol. 7, pp. 64411–64430, 2019.

[3] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Trans. Depend. Sec. Comput.*, to be published, doi: 10.1109/TDSC.2017.2764083.

[4] *10 Real World Applications of Internet of Things (IoT)*. Accessed: Oct. 2019. [Online]. Available: https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/

[5] Amazon. *Healthcare & Life Sciences*. Accessed: Oct. 2019. [Online]. Available: https://aws.amazon.com/health/

[6] A. Gatouillat, Y. Badr, B. Massot, and E. Sejdić, "Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3810–3822, Oct. 2018.

[7] X. Wang, L. Wang, Y. Li, and K. Gai, "Privacy-aware efficient fine-grained data access control in Internet of medical things based fog computing," *IEEE Access*, vol. 6, pp. 47657–47665, 2018.

[8] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical unclonable function-based robust and lightweight authentication in the Internet of medical things," *IEEE Trans. Consum. Electron.*, vol. 65, no. 3, pp. 388–397, Aug. 2019.

[9] Z. Liu, L. Zhang, Q. Ni, J. Chen, R. Wang, Y. Li, and Y. He, "An integrated architecture for IoT malware analysis and detection," in *IoT as a Service*, B. Li, M. Yang, H. Yuan, and Z. Yan, Eds. Cham, Switzerland: Springer, 2019, pp. 127–137.

[10] J. Su, D. V. Vasconcellos, S. Prasad, S. Daniele, Y. Feng, and K. Sakurai, "Lightweight classification of IoT malware based on image recognition," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Tokyo, Japan, vol. 2, Jul. 2018, pp. 664–669.

[11] V. Clincy and H. Shahriar, "IoT malware analysis," in *Proc. IEEE 43rd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Milwaukee, WI, USA, vol. 1, Jul. 2019, pp. 920–921.

[12] S. M. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, Jun. 2015.

[13] M. Wazid, A. K. Das, S. Kumari, X. Li, and F. Wu, "Provably secure biometric-based user authentication and key agreement scheme in cloud computing," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4103–4119, 2016.

[14] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos, "A novel authentication and key agreement scheme for implantable medical devices deployment," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 4, pp. 1299–1309, Jul. 2018.

[15] P. Kumar, A. Braeken, A. Gurtov, J. Iinatti, and P. H. Ha, "Anonymous secure framework in connected smart home environments," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 4, pp. 968–979, Apr. 2017.

[16] P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttila, and M. Sain, "Lightweight and secure session-key establishment scheme in smart home environments," *IEEE Sensors J.*, vol. 16, no. 1, pp. 254–264, Jan. 2016.

[17] M. Wazid, A. K. Das, N. Kumar, and A. V. Vasilakos, "Design of secure key management and user authentication scheme for fog computing services," *Future Gener. Comput. Syst.*, vol. 91, pp. 475–492, Feb. 2019.

[18] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. H. Park, "AKM-IoV: Authenticated key management protocol in fog computing-based Internet of vehicles deployment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8804–8817, Oct. 2019.

[19] S. Shen, L. Huang, H. Zhou, S. Yu, E. Fan, and Q. Cao, "Multistage signaling game-based optimal detection strategies for suppressing malware diffusion in fog-cloud-based IoT networks," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1043–1054, Apr. 2018.

[20] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and security in Internet of Things and wearable devices," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 1, no. 2, pp. 99–109, Apr./Jun. 2015.

[21] 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.

[22] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K.-K. R. Choo, and Y. Park, "Design of secure and lightweight authentication protocol for wearable devices environment," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 4, pp. 1310–1322, Jul. 2018.

[23] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4359–4373, May 2018.

[24] S. S. Alotaibi, "Registration center based user authentication scheme for smart e-governance applications in smart cities," *IEEE Access*, vol. 7, pp. 5819–5833, 2019.

[25] A. K. Tripathy, P. K. Tripathy, N. K. Ray, and S. P. Mohanty, "iTour: The future of smart tourism: An IoT framework for the independent mobility of tourists in smart cities," *IEEE Consum. Electron. Mag.*, vol. 7, no. 3, pp. 32–37, May 2018.

[26] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city," *IEEE Access*, vol. 7, pp. 18611–18621, 2019.

[27] G. Writer. *IoT Applications in Agriculture*. Accessed: Oct. 2019. [Online]. Available: https://www.iotforall.com/iot-applications-in-agriculture/

[28] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow, and M. N. Hindia, "An overview of Internet of Things (IoT) and data analytics in agriculture: benefits and challenges," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3758–3773, Oct. 2018.

[29] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E. M. Aggoune, "Internet-of-Things (IoT)-based smart agriculture: Toward making the fields talk," *IEEE Access*, vol. 7, pp. 129551–129583, 2019.

[30] F. Tseng, H. Cho, and H. Wu, "Applying big data for intelligent agriculture-based crop selection analysis," *IEEE Access*, vol. 7, pp. 116965–116974, 2019.

[31] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4900–4913, Dec. 2018.

[32] J. Li, Y. Liu, J. Xie, M. Li, M. Sun, Z. Liu, and S. Jiang, "A remote monitoring and diagnosis method based on four-layer IoT frame perception," *IEEE Access*, vol. 7, pp. 144324–144338, 2019.

[33] W. Wei, F. Liu, and S. Mei, "Energy pricing and dispatch for smart grid retailers under demand response and market price uncertainty," *IEEE Trans. Smart Grid*, vol. 6, no. 3, pp. 1364–1374, May 2015.

[34] J. Yang, J. Zhao, F. Luo, F. Wen, and Z. Y. Dong, "Decision-making for electricity retailers: A brief survey," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4140–4153, Sep. 2018.

[35] K. Nur, M. Morenza-Cinos, A. Carreras, and R. Pous, "Projection of RFID-obtained product information on a retail stores indoor panoramas," *IEEE Intell. Syst.*, vol. 30, no. 6, pp. 30–37, Nov./Dec. 2015.

[36] S. S. Kamble, A. Gunasekaran, H. Parekh, and S. Joshi, "Modeling the Internet of Things adoption barriers in food retail supply chains," *J. Retailing Consum. Services*, vol. 48, pp. 154–168, May 2019.

[37] C. Garrido-Hidalgo, T. Olivares, F. J. Ramirez, and L. Roda-Sanchez, "An end-to-end Internet of Things solution for reverse supply chain management in industry 4.0," *Comput. Ind.*, vol. 112, Nov. 2019, Art. no. 103127.

[38] M. Abdel-Basset, G. Manogaran, and M. Mohamed, "Internet of Things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems," *Future Gener. Comput. Syst.*, vol. 86, pp. 614–628, Sep. 2018.

[39] A. K. Das and S. Zeadally, "Data security in the smart grid environment," in *Pathways to a Smarter Power System*, A. Tascıkaraoglu and O. Erdinc, Eds. New York, NY, USA: Academic, 2019, ch. 13, pp. 371–395.

[40] A. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," *Future Gener. Comput. Syst.*, vol. 89, pp. 110–125, Dec. 2018.

[41] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2010.
[42] P. Yan and Z. Yan, "A survey on dynamic mobile malware detection," *Softw. Qual. J.*, vol. 26, no. 3, pp. 891–919, 2018.
[43] H. Takase, R. Kobayashi, M. Kato, and R. Ohmura, "A prototype implementation and evaluation of the malware detection mechanism for IoT devices using the processor information," *Int. J. Inf. Secur.*, 2019, doi: 10.1007/s10207-019-00437-y.
[44] A. Azmoodeh, A. Dehghantanha, and K.-K. R. Choo, "Robust malware detection for Internet of (battlefield) things devices using deep Eigenspace learning," *IEEE Trans. Sustain. Comput.*, vol. 4, no. 1, pp. 88–95, Jan./Mar. 2019.
[45] E. M. Rudd, A. Rozsa, M. Günther, and T. E. Boult, "A survey of stealth malware attacks, mitigation measures, and steps toward autonomous open world solutions," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1145–1172, 2nd Quart., 2017.
[46] M. Wazid, S. Zeadally, and A. K. Das, "Mobile banking: Evolution and threats: Malware threats and security solutions," *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, pp. 56–60, Mar. 2019.
[47] *How To Avoid The Dreaded Computer Virus*. Accessed: Oct. 2019. [Online]. Available: http://www.magellansolutions.co.uk/malware.html
[48] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, and S. Venkatraman, "Robust intelligent malware detection using deep learning," *IEEE Access*, vol. 7, pp. 46717–46738, 2019.
[49] T. Kim, B. Kang, M. Rho, S. Sezer, and E. G. Im, "A multimodal deep learning method for Android Malware detection using various features," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 773–788, Mar. 2019.
[50] W. Zhou and B. Yu, "A cloud-assisted malware detection and suppression framework for wireless multimedia system in IoT based on dynamic differential game," *China Commun.*, vol. 15, no. 2, pp. 209–223, 2018.
[51] W. Bin, L. Tianliang, Z. Kangfeng, Z. Dongmei, and L. Xing, "Smartphone malware detection model based on artificial immune system," *China Commun.*, vol. 11, no. 13, pp. 86–92, 2014.
[52] 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.
[53] G. Kambourakis, C. Kolias, and A. Stavrou, "The Mirai botnet and the IoT Zombie Armies," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Baltimore, MD, USA, Oct. 2017, pp. 267–272.
[54] H. Sinanovic and S. Mrdovic, "Analysis of Mirai malicious software," in *Proc. 25th Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM)*, Split, Croatia, 2017, pp. 1–5.
[55] H. Semic and S. Mrdovic, "IoT honeypot: A multi-component solution for handling manual and Mirai-based attacks," in *Proc. 25th Telecommun. Forum (TELFOR)*, Belgrade, Serbia, 2017, pp. 1–4.
[56] M. Korolov. *What is a Botnet? When Armies of Infected IoT Devices Attack*. Accessed: Oct. 2019. [Online]. Available: https://www.csoonline.com/ article/3240364/ what-is-a-botnet.html
[57] A. Kumar and T. J. Lim, "EDIMA: Early detection of IoT malware network activity using machine learning techniques," in *Proc. 5th World Forum Internet Things (WF-IoT)*, Limerick, Ireland, 2019, pp. 289–294.
[58] T. Kelley and E. Furey, "Getting prepared for the next botnet attack: Detecting algorithmically generated domains in botnet command and control," in *Proc. 29th Irish Signals Syst. Conf. (ISSC)*, Belfast, Ireland, 2018, pp. 1–6.
[59] I. Ilascu. *New Echobot Botnet Variant Uses Over 50 Exploits to Propagate*. Accessed: Oct. 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-echobot-botnet-variant-uses-over-50-exploits-to-propagate/
[60] Ethhack. *What's a Botnet? When Armies of Contaminated IoT Gadgets Assault*. Accessed: Oct. 2019. https://ethhack.com/2019/06/what-is-a-botnet-when-armies-of-infected-iot-devices-attack-2/
[61] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, Jul./Sep. 2018.
[62] Y.-W. Kao, K.-Y. Huang, H.-Z. Gu, and S.-M. Yuan, "uCloud: A user-centric key management scheme for cloud data protection," *IET Inf. Secur.*, vol. 7, no. 2, pp. 144–154, Jun. 2013.
[63] J. Li, X. Chen, M. Li, J. Li, P. P. C. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 6, pp. 1615–1625, Jun. 2014.
[64] P. K. Tysowski and M. A. Hasan, "Hybrid attribute- and re-encryption-based key management for secure and scalable mobile applications in clouds," *IEEE Trans. Cloud Comput.*, vol. 1, no. 2, pp. 172–186, Jul. 2013.
[65] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling cloud storage auditing with key-exposure resistance," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1167–1179, Jun. 2015.
[66] L. Eschenauer and V. D. Gligor, "A key management scheme for distributed sensor networks," in *Proc. 9th ACM Conf. Comput. Commun. Secur.*, Nov. 2002, pp. 41–47.
[67] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Symp. Secur. Privacy*, Berkeley, CA, USA, May 2003, pp. 197–213.
[68] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *Proc. 23rd Conf. IEEE Commun. Soc. (Infocom)*, vol. 1, Hong Kong, Mar. 2004, pp. 586–597.
[69] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key pre-distribution scheme for wireless sensor networks," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, Washington, DC, USA, 2003, pp. 42–51.
[70] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 740. Berlin, Germany: Springer, Aug. 1993, pp. 471–486.
[71] Y. Cheng and D. Agrawal, "Efficient pairwise key establishment and management in static wireless sensor networks," in *Proc. 2nd IEEE Int. Conf. Mobile Ad Hoc Sensor Syst.*, Washington, DC, USA, Nov. 2005, p. 550.
[72] D. Liu, P. Ning, and W. Du, "Group-based key pre-distribution in wireless sensor networks," in *Proc. ACM Workshop Wireless Secur. (WiSe)*, Sep. 2005.
[73] Q. Dong and D. Liu, "Using auxiliary sensors for pairwise key establishment in WSN," in *Proc. IFIP Int. Conf. Netw. (Networking)*, in Lecture Notes in Computer Science, vol. 4479, 2007, pp. 251–262.
[74] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Trans. Sensor Netw.*, vol. 2, no. 4, pp. 500–528, Nov. 2006.
[75] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," *Wireless Netw.*, vol. 8, no. 5, pp. 521–534, Sep. 2002.
[76] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 1, pp. 41–77, 2005.
[77] A. K. Das, "An identity-based random key pre-distribution scheme for direct key establishment to prevent attacks in wireless sensor networks," *Int. J. Netw. Secur.*, vol. 6, no. 2, pp. 134–144, 2008.
[78] A. K. Das, "ECPKS: An improved location-aware key management scheme in static sensor networks," *Int. J. Netw. Secur.*, vol. 7, no. 3, pp. 358–369, 2008.
[79] A. K. Das, "A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks," *Int. J. Inf. Secur.*, vol. 11, no. 3, pp. 189–211, Jun. 2012.
[80] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.
[81] M. Wazid, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "Secure three-factor user authentication scheme for renewable-energy-based smart grid environment," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3144–3153, Dec. 2017.
[82] D. He, N. Kumar, M. K. Khan, L. Wang, and J. Shen, "Efficient privacy-aware authentication scheme for mobile cloud computing services," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1621–1631, Jun. 2018.
[83] L. Wu, J. Wang, K. R. Choo, and D. He, "Secure key agreement and key protection for mobile device user authentication," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 319–330, Feb. 2019.
[84] D. Wang, H. Cheng, D. He, and P. Wang, "On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices," *IEEE Syst. J.*, vol. 12, no. 1, pp. 916–925, Mar. 2018.
[85] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, Feb. 2018.

[86] M. Wazid, A. K. Das, and J.-H. Lee, "User authentication in a tactile Internet based remote surgery environment: Security issues, challenges, and future research directions," *Pervasive Mobile Comput.*, vol. 54, pp. 71–85, Mar. 2019.
[87] F. Wu, L. Xu, S. Kumari, X. Li, J. Shen, K.-K. R. Choo, M. Wazid, and A. K. Das, "An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment," *J. Netw. Comput. Appl.*, vol. 89, pp. 72–85, Jul. 2017.
[88] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of drones deployment," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3572–3584, Apr. 2019.
[89] M. Wazid, A. K. Das, S. Kumari, and M. K. Khan, "Design of sinkhole node detection mechanism for hierarchical wireless sensor networks," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4596–4614, 2016.
[90] M. Wazid and A. K. Das, "A secure group-based blackhole node detection scheme for hierarchical wireless sensor networks," *Wireless Pers. Commun.*, vol. 94, no. 3, pp. 1165–1191, Jun. 2017.
[91] A. K. Das, M. Wazid, A. R. Yannam, J. J. P. C. Rodrigues, and Y. Park, "Provably secure ECC-based device access control and key agreement protocol for IoT environment," *IEEE Access*, vol. 7, pp. 55382–55397, 2019.
[92] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019.
[93] K. Riad, R. Hamza, and H. Yan, "Sensitive and energetic IoT access control for managing cloud electronic health records," *IEEE Access*, vol. 7, pp. 86384–86393, 2019.
[94] Q. Wang, D. Chen, N. Zhang, Z. Qin, and Z. Qin, "LACS: A lightweight label-based access control scheme in IoT-based 5G caching context," *IEEE Access*, vol. 5, pp. 4018–4027, 2017.
[95] (2016). *X.509: Information Technology–Open Systems Interconnection—The Directory: Public-Key and Attribute Certificate Frameworks.* [Online]. Available: https://www.itu.int/rec/T-REC-X.509
[96] M. Wazid and A. K. Das, "An efficient hybrid anomaly detection scheme using k-means clustering for wireless sensor networks," *Wireless Pers. Commun.*, vol. 90, no. 4, pp. 1971–2000, Oct. 2016.
[97] M. Wazid, P. R. Dsouza, A. K. Das, V. K. Bhat, N. Kumar, and J. J. P. C. Rodrigues, "RAD-EI: A routing attack detection scheme for edge-based Internet of Things environment," *Int. J. Commun. Syst.*, vol. 32, no. 15, p. e4024, Oct. 2019, doi: 10.1002/dac.4024.
[98] S. Challa, M. Wazid, A. K. Das, and M. K. Khan, "Authentication protocols for implantable medical devices: Taxonomy, analysis and future directions," *IEEE Consum. Electron. Mag.*, vol. 7, no. 1, pp. 57–65, Jan. 2018.
[99] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," *J. High Speed Netw.*, vol. 15, no. 1, pp. 33–51, 2006.
[100] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 266–282, 1st Quart., 2014.
[101] T. Lei, Z. Qin, Z. Wang, Q. Li, and D. Ye, "EveDroid: Event-aware Android malware detection against model degrading for IoT devices," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6668–6680, Aug. 2019.
[102] H. Nguyen, Q. Ngo, and V. Le, "IoT botnet detection approach based on PSI graph and DGCNN classifier," in *Proc. IEEE Int. Conf. Inf. Commun. Signal Process. (ICICSP)*, Singapore, Sep. 2018, pp. 118–122.
[103] S. M. P. Dinakarrao, H. Sayadi, H. M. Makrani, C. Nowzari, S. Rafatirad, and H. Homayoun, "Lightweight node-level malware detection and network-level malware confinement in IoT networks," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Florence, Italy, Mar. 2019, pp. 776–781.
[104] J. Su, D. V. Vasconcellos, S. Prasad, S. Daniele, Y. Feng, and K. Sakurai, "Lightweight classification of IoT malware based on image recognition," in *Proc. 42nd IEEE Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Tokyo, Japan, vol. 2, Jul. 2018, pp. 664–669.
[105] B. Wu, K. Xu, Q. Li, Z. Liu, Y. Hu, Z. Zhang, X. Du, B. Liu, and S. Ren, "SmartCrowd: Decentralized and automated incentives for distributed IoT system detection," in *Proc. 39th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Dallas, TX, USA, 2019, pp. 1106–1116.

MOHAMMAD WAZID (S'15–M'17) received the M.Tech. degree in computer network engineering from Graphic Era University, Dehradun, India, and the Ph.D. degree in computer science and engineering from the International Institute of Information Technology, Hyderabad, India. He is currently an Associate Professor with the Department of Computer Science and Engineering, Graphic Era University. Prior to this, he was an Assistant Professor with the Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India. He was also a Postdoctoral Researcher with the Cyber Security and Networks Lab, Innopolis University, Innopolis, Russia. His current research interests include security, remote user authentication, the Internet of Things (IoT), and cloud computing. He has published more than 60 articles in international journals and conferences in the above areas. He was a recipient of the University Gold Medal and the Young Scientist Award by UCOST, Department of Science and Technology, Government of Uttarakhand, India. He has also received the recognition of "Best Reviewer of 2019" from *ICT Express* (Elsevier) journal.

ASHOK KUMAR DAS (M'17–SM'18) received the Ph.D. degree in computer science and engineering, the M.Tech. degree in computer science and data processing, and the M.Sc. degree in mathematics from IIT Kharagpur, India. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. His current research interests include cryptography, network security, blockchain, the security in Internet of Things (IoT), the Internet of Vehicles (IoV), the Internet of Drones (IoD), smart grids, smart city, cloud/fog computing and industrial wireless sensor networks, and intrusion detection. He has authored over 200 articles in international journals and conferences in the above areas, including over 175 reputed journal articles. Some of his research findings are published in top cited journals, such as the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE TRANSACTIONS ON SMART GRID, the IEEE INTERNET OF THINGS JOURNAL, the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, the IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS (formerly the IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE), the *IEEE Consumer Electronics Magazine*, IEEE ACCESS, the *IEEE Communications Magazine*, *Future Generation Computer Systems*, *Computers & Electrical Engineering*, *Computer Methods and Programs in Biomedicine*, *Computer Standards & Interfaces*, *Computer Networks*, *Expert Systems with Applications*, and the *Journal of Network and Computer Applications*. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He is on the Editorial Board of the *KSII Transactions on Internet and Information Systems*, the *International Journal of Internet Technology and Secured Transactions* (Inderscience), and the *IET Communications*. He is a Guest Editor of *Computers & Electrical Engineering* (Elsevier) for the special issue on Big data and IoT in e-healthcare and of *ICT Express* (Elsevier) for the special issue on Blockchain Technologies and Applications for 5G Enabled IoT. He has served as a Program Committee Member in many international conferences. He has also severed as one of the Technical Program Committee Chairs of the International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, in June 2019.

JOEL J. P. C. RODRIGUES (S'01–M'06–SM'06–F'20) is currently a Professor with the Federal University of Piauí, Brazil, and a Senior Researcher with the Instituto de Telecomunicações, Portugal. He is the Leader of the Next Generation Networks and Applications Research Group (CNPq), the Director of Conference Development—the IEEE ComSoc Board of Governors, an IEEE Distinguished Lecturer, the Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, the President of the scientific council at ParkUrbis—Covilhã Science and Technology Park, the Past Chair of the IEEE ComSoc Technical Committee on eHealth, the Past Chair of the IEEE ComSoc Technical Committee on Communications Software, a Steering Committee Member of the IEEE Life Sciences Technical Community, and the Publications Co-Chair and a Member Representative of the IEEE Communications Society on the IEEE Biometrics Council. He has authored or coauthored over 800 articles in refereed international journals and conferences, three books, and one ITU-T Recommendation. He holds two patents. He is a member of the Internet Society and a Senior Member of the ACM. He is the Editor-In-Chief of the *International Journal on E-Health and Medical Communications* and an Editorial Board Member of several high-reputed journals. He has been the General Chair and the TPC Chair of many international conferences, including the IEEE ICC, IEEE GLOBECOM, IEEE HEALTHCOM, and IEEE LatinCom. He had been awarded several Outstanding Leadership and Outstanding Service Awards by the IEEE Communications Society and several best papers awards.

SACHIN SHETTY received the Ph.D. degree in modeling and simulation from Old Dominion University, in 2007. He was an Associate Professor with the Electrical and Computer Engineering Department, Tennessee State University, USA. He is currently an Associate Professor with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University. He holds a joint appointment with the Department of Modeling, Simulation and Visualization Engineering and the Center for Cybersecurity Education and Research. He has authored or coauthored over 125 research articles in journals and conference proceedings and two books. His research interests include the intersection of computer networking, network security, and machine learning. He was a recipient of the DHS Scientific Leadership Award. He has served on the Technical Program Committee of the ACM CCS, the IEEE INFOCOM, the IEEE ICDCN, and the IEEE ICCCN.

YOUNGHO PARK (M'17) received the B.S., M.S., and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, South Korea, in 1989, 1991, and 1995, respectively. From 1996 to 2008, he was a Professor with the School of Electronics and Electrical Engineering, Sangju National University, South Korea. From 2003 to 2004, he was a Visiting Scholar with the School of Electrical Engineering and Computer Science, Oregon State University, USA. He is currently a Professor with the School of Electronics Engineering, Kyungpook National University. His research interests include computer networks, multimedia, and information security.