IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 3, 2020, accepted December 25, 2020, date of publication December 28, 2020, date of current version January 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3047895

Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap

MOHAMMAD WAZID[1], (Senior Member, IEEE), ASHOK KUMAR DAS[2], (Senior Member, IEEE), SACHIN SHETTY[3], (Senior Member, IEEE), PROSANTA GOPE[4], (Member, IEEE), AND JOEL J. P. C. RODRIGUES[5,6], (Fellow, 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]Virginia Modeling, Analysis and Simulation Center, Department of Computational Modeling and Simulation Engineering, Old Dominion University, Suffolk, VA 23435, USA
[4]Department of Computer Science, University of Sheffield, Sheffield S10 2TN, U.K.
[5]PPGEE, Federal University of Piauí (UFPI), Teresina 64049-550, Brazil
[6]Instituto de Telecomunicações, 6201-001 Covilha, Portugal

Corresponding author: Ashok Kumar Das (iitkgp.akdas@gmail.com)

This work was supported in part by the Office of the Assistant Secretary of Defense for Research and Engineering [OASD (R&E), under Grant FA8750-15-2-0120, in part by the FCT/MCTES through national funds and when applicable co-funded EU funds under Project UIDB/50008/2020, in part by the Brazilian National Council for Scientific and Technological Development (CNPq) under Grant 309335/2017-5, and in part by the Ripple Centre of Excellence (CoE) Scheme, CoE in Blockchain, International Institute of Information Technology (IIIT) Hyderabad, India, under Grant IIIT/R&D Office/Internal Projects/001/2019.

ABSTRACT 5G mobile communication systems promote the mobile network to not only interconnect people, but also interconnect and control the machine and other devices. 5G-enabled Internet of Things (IoT) communication environment supports a wide-variety of applications, such as remote surgery, self-driving car, virtual reality, flying IoT drones, security and surveillance and many more. These applications help and assist the routine works of the community. In such communication environment, all the devices and users communicate through the Internet. Therefore, this communication agonizes from different types of security and privacy issues. It is also vulnerable to different types of possible attacks (for example, replay, impersonation, password reckoning, physical device stealing, session key computation, privileged-insider, malware, man-in-the-middle, malicious routing, and so on). It is then very crucial to protect the infrastructure of 5G-enabled IoT communication environment against these attacks. This necessitates the researchers working in this domain to propose various types of security protocols under different types of categories, like key management, user authentication/device authentication, access control/user access control and intrusion detection. In this survey paper, the details of various system models (i.e., network model and threat model) required for 5G-enabled IoT communication environment are provided. The details of security requirements and attacks possible in this communication environment are further added. The different types of security protocols are also provided. The analysis and comparison of the existing security protocols in 5G-enabled IoT communication environment are conducted. Some of the future research challenges and directions in the security of 5G-enabled IoT environment are displayed. The motivation of this work is to bring the details of different types of security protocols in 5G-enabled IoT under one roof so that the future researchers will be benefited with the conducted work.

INDEX TERMS Fifth generation mobile communication systems (5G), Internet of Things (IoT), security, privacy, key management, authentication, access control, intrusion detection.

I. INTRODUCTION

5G is the fifth generation mobile communication systems which promotes the mobile network to not only interconnect people, but also interconnect and control the machine and other devices (i.e., smart devices). It improves the performance and efficiency which capacitate the user experiences. 5G delivers peak rates up to 10 Gbps, ''ultra-low latency'' and ''massive capacity'' which provides the consistence and uniform service to the user. It is a wireless networking

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

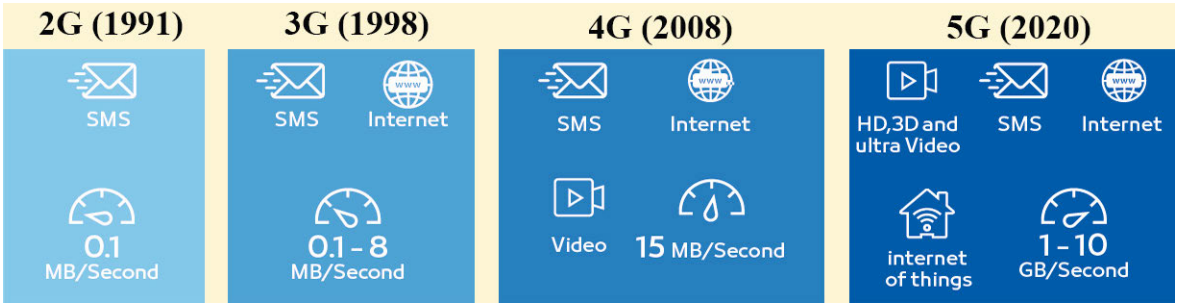

FIGURE 1. Evolution/generations of mobile communication system (adapted from [6]).

architecture which was built on the "802.11ac IEEE wireless networking standard" and aims to improve the data communication speeds by up to three times as compared to its antecedent "4G- IEEE 802.11n" [1]–[5].

A. EVOLUTION OF MOBILE COMMUNICATION SYSTEMS

The evolution of mobile communication system can be further elaborated as follows [6]:

- **Earlier Generations (1G, 2G and 3G):** 1G (First Generation) was introduced in the late 1970's. It did not have strong security mechanism, suffered from call drop problems and the data transmission speed was around 2.4 Kbps. 2G (Second Generation) supported data services like "short message service (SMS)" and "multimedia messaging service (MMS)". The data transmission speed through General Packet Radio Service (GPRS) was in between 50 Kbps to 1 Mbps. 3G (Third Generation) provided services such as web browsing, email, video downloading, picture sharing and other smartphone applications. Its data transmission stationary speed upto 2 Mbps and mobile speed upto 384 kbps. The theoretical max speed for "high speed packet access (HSPA+)" is 21.6 Mbps.
- **4G (Fourth Generation):** The motive of 4G is to provide high quality, high capacity and high speed services to the users. It provides better security along with low cost of data and voice services and Internet over IP. It supports various application such as "improved mobile web access", "gaming", "high-definition mobile TV", "IP telephony", "video conferencing", "3D television" and other novel computing environment. It uses key technologies such as "multiple input multiple output (MIMO)" and "orthogonal frequency division multiplexing (OFDM)". Some essential standards of 4G are "long term evolution (LTE)" and "worldwide interoperability for microwave access (WiMAX)". Data transfer speed upto 100 Mbps with moving device or 1 Gbps for low mobility is supported.
- **5G (Fifth Generation):** It was introduced to improve the limitations and performance of 4G. It support very good data transfer rate with low latency and high connection density. It supports device-to-device communication with better battery consumption along with good wireless coverage. The data transfer speed of 5G is approximately 35 times faster than 4G which is aimed up to 35.46 Gbps. The technologies work in the background are "massive multiple-input and multiple-output (MIMO)" and "millimeter wave mobile communications". Techniques and technologies like "small cells", "massive MIMO", "millimetre wave" and "light fidelity (Li-Fi)" are utilized to provide 10Gbps with very low latency. It supports connections approximately for 100 billion devices. Its full fledged implementation is required up to 2020 to fulfill the raised requirements of consumers [7]–[9].

The evolution of mobile communication system is also highlighted in Fig. 1 which shows the progress over the last few decades. It also includes the details of functionality features supported by various generations.

5G is designed with the forgoing four mega trends (for example, increased number of devices, traffic growth, high dependency on cloud and different 5G convergence services). Some suggestions were given by some interested companies for selecting the key performance indicators which should be used in 5G. On the basis of these suggestions, the International Telecommunication Union–Radiocommunication Sector (ITU-R) [10] selected some of the important parameters that are listed in Table 1.

TABLE 1. Key performance indicators for 5G.

Key performance indicators	Target values
Data rate (user experience)	100 Mbps to 1 Gbps
Data rate (peak)	10 Gbps to 50 Gbps
Support for Mobility	Up to 500 Kmph
Latency	1 ms
Connection density	10^6 to 10^7 per Km^2
Traffic volume density	1TB to 10TB/s/Km^2

B. BENEFITS OF 5G MOBILE COMMUNICATION SYSTEM

5G mobile communication system provides very fast speed and more reliable connections on smartphones and other mobile devices (i.e., smart vehicles) than ever before. Some of the key benefits of 5G networks are [7]–[9]:

- Provides very high data transfer rate (1-20 Gbps) which facilitates the users to download content very quickly.
- Delivers ultra low latency (1 ms) which allows users to experience less delay when requesting data from the network.
- Capacity increases as the the network expands.
- Manageable with the previous generations of mobile communication technologies.
- Effective and supportive for heterogeneous services (i.e., private network).
- Provides uniform, uninterrupted, and consistent connectivity for the various applications (i.e., communication of smart vehicles) across the world.

IoT is a communication environment of connected physical objects having unique address (i.e., IP address) which are accessible using the Internet. ''Thing'' in IoT can be a patient with smart health monitoring devices or a smart vehicle with built-in-sensors. These objects (i.e., smart devices) have assigned an IP address and using that they are able to collect and transfer data over a network without manual assistance [11]–[15]. Fifth Generation (5G) communication system has a great impact over the communication happens in IoT. 5G activates innovation across many industries (i.e., automobile sector, health sector) and provides a platform to enable the emerging technologies (for example, IoT) to become an essential part of the economy and people's daily lives.

C. ADVANTAGES AND DISADVANTAGES OF IoT COMMUNICATION

Some of the advantages and disadvantages of IoT communication are discussed below [16]–[20].

- **Advantages of IoT**
  - **Easy remote access to information:** Using the IoT communication environment the data from smart devices which are located far from our location and in real time can be accessible using the Internet and smartphone/tablet. This makes it very convenient for the working class people who can do their job work and access the smart devices (i.e., in a smart home) remotely both at the same time [14], [21].
  - **Provides better communication:** A network of interconnected devices in IoT provides a better communication environment. It increases the efficiencies by making the communication more transparent. The machine to machine communication makes the job better, efficient and produces faster results for instance, communication in industrial IoT [22].
  - **Cost-effective:** Communication among electronic devices becomes easy because of the use of IoT. This helps people to facilitates their day-to-day tasks. In such environment the transmission of data packets happen efficiently which also saves money. Such type of fast transmission of data was not possible in the past, that happens because of the advancement of communication technology (i.e., evolution of IoT) [16], [19].
  - **Automation:** Automation is biggest requirement of current time which manages day-to-day activities without any human involvement. In business, it helps to boost the quality of services and further scale downs the human involvement.
- **Disadvantages of IoT**
  - **Privacy and security:** In current tech driven time each and every device which an individual uses is connected to the Internet. This further increases the risk of leakage of sensitive information. This is the major drawback of such kind of communication. If information is not handled properly may lead to the disclosure of confidential information to the third party. Therefore, some strong authentication, access control, intrusion detection and privacy preservation protocols for IoT communication to protect against any kind of data leakage attack are required [7]–[9], [13], [14], [23]–[26].
  - **Complexity and compatibility issues:** IoT consists of different types of devices and networking protocols which are used to connect them. A single mistake in that system can affect the entire performance [27].
  - **Reduction in number of jobs:** The need for human labor reduced drastically with the task automation as machine replaces the human (labor). This further impact the employ-ability. With the emergence of IoT applications in future, there will be decline in the number of jobs available to the professionals [28]–[30].
  - **Dependability:** There is a drastic change in the technology and its applications. Technology is dominating our lifestyle and further increasing our dependability on technology (i.e., IoT applications). But at the same time it also has some drawbacks for example, if there is some vulnerability in a system then there are the possibilities that device does not work properly and can cause other serious consequences [28]–[30].

D. CONVERGENCE OF 5G AND IoT

It is an estimate that twenty billion IoT devices will be connected to a worldwide network up to 2020 which will produce enormous amount of data. Researchers have created an architecture called the 5G I-IoT paradigm, which is a merger of 5G cellular network, artificial intelligence (AI) and IoT that creates an Intelligent IoT (I-IoT) environment. Such kind of merger of three technologies provide efficient access to the users for the data generated by IoT devices which is further useful to make some sense from this generated data. The evolution of 5G networks becomes a major driving force for the growth of IoT as 5G provides extended

coverage, faster speeds along with massive bandwidth as compared to other cellular network communication system. 5G I-IoT paradigm connects IoT devices (i.e., IoT sensors) to a cloud server, where the sensory data is gathered, processed and analyzed using AI algorithms. This analysis helps the users for further decision making. It makes the users capable to take appropriate decisions relevant to their field of work (i.e., smart transportation, smart agriculture, and smart healthcare) [13], [23], [27], [36]–[38].

E. APPLICATIONS OF 5G-ENABLED IoT COMMUNICATION ENVIRONMENT

It can be convinced to everybody that 5G will be the next revolution. Some of the applications of 5G-enabled IoT communication environment are discussed below.

- **Remote surgery:** One of the tremendous advantage of 5G is its low latency feature. Because it has short time lag between a device pinging the network and getting the response whereas it was the problem with 4G LTE. Because of such characteristics of 5G network a surgeon can now perform a remote surgery and his/her physical presence is not required in the same operation theater. For example, the doctors at King's College London has demonstrated the surgery procedure in which they used a dummy patient by the help of ''virtual reality headset'' and ''special glove''. Through that they have performed remote surgery by the help of remote robotic arm [39], [40].
- **Self-driving car:** A autonomous vehicle (AV) or self-driving car is a kind of smart vehicle which has ability to sens its surroundings and safety travelling with negligible human involvement. Self-driving cars are installed with different types of sensors to get information about their surroundings. These vehicle are also inbuilt with some other important functionalities such as inertial measuring units, odometry, radar and GPS system. The equipped control systems can interpret the sensed data to identify the required navigation paths along with the existing obstacles. AVs are also capable to communicate among each other for proper decision making and to select the appropriate path to reach to a destination. All such communication facilitates through 5G mobile communication system [41]–[43].
- **Virtual reality (VR):** Its a kind of artificial environment which is created using the software and other related tools. It is presented to the user in such a way that the user suspends the originality and agrees to accept it like an actual environment. Mostly it is felt through senses for example, sound and sight. In a recently held ''mobile world congress'', it was demonstrated that ''how 5G could enhance the user's experience''. It permitted the user to do chatting in the real time with live-streaming virtual worlds [44]–[46].
- **Flying IoT (Drones):** Internet of Drones (IoD) is a ''layered network control architecture'' which is implemented to coordinate the access of unmanned aerial vehicles (i.e., drones). It is used to control the airspace and carries out navigation services between the different locations. The various services of flying IoT are like traffic surveillance, search & rescue and package delivery. These drones can communicate to the base station (server) through the Internet connection. They capture (monitor) the surroundings and transmit the data to the base station using the Internet. In order to make such kind of communication a very efficient mobile communication network is required. Therefore, 5G will be a suitable match for this [47], [48].
- **Security and surveillance:** Surveillance and analytics is another application which will be very successful with 5G connectivity. Due to the increasing threats to public safety in recent years, many governments and security agencies installing the public surveillance and security systems. Majority of public video surveillance systems still rely on wired networks. However adoption for wireless communications such as WiFi or even more the 5G system is also gaining popularity due to the easy and fast set-up with low cost. Closed circuit television (CCTV) systems (for example, cameras installed in vehicles (i.e., police cars), public transport and surveillance drones are getting popularity. The adoption of 5G communication system boost up the performance which is required for sophisticated video content analysis in real-time and the deployment of massive numbers of cameras in the targeted regions [49]–[51].
- **Transforming healthcare:** Most of the time when somebody has some illness and he/she needs some medical treatment and attention travel to a doctor's clinic or hospital. But it is very difficult for the people living in the rural area where that kind of medical facilities are not available. Moreover, travelling in illness is challenging and time-consuming. However, with the advancement of information and communications technology (ICT), latest tools and technologies for example, telehealth and remote home monitoring systems are available through which care can be received within the comfort of the homes. Remote home health monitoring system consists of health monitoring devices (i.e., implantable or wearable health devices) and other video & imaging facilities in which the communication technologies such as 5G and IoT can be utilized. These devices sens and transmit the medical information of a patient (user) to a central authority (i.e., cloud server) through which a health expert (i.e., a doctor) can also access the medical data of the patient. Doctors can suggest medicine (treatment) prescription after a short video call remotely. Such kind of remote monitoring is equipped with sophisticated imaging equipment and produces enormous amount of health sensing data which causes additional strain on the networks. This often increases the congestion and slows down the data transfer speeds, especially in a large healthcare system which may interface with huge number of patients in

a single day. Therefore, 5G mobile communication system which has very high data transfer speed along with low latency will be very helpful for such kind of healthcare system [2], [23], [52], [53].

F. EXISTING SURVEYS ON SECURITY IN 5G-ENABLED IoT ENVIRONMENT

Here, the details of the existing surveys on ''security protocols in 5G-enabled IoT environment'' are provided. This will help the readers how our work is different than the other existing works.

Granjal *et al.* (2015) [17] performed an analysis on the security protocols available to protect the communications in IoT. They also discussed the existing research proposals and challenges in IoT security for the future researchers.

Khan *et al.* [31] (2018) presented the major security issues in IoT communication. They categorized the famous security issues as per the IoT architecture. Further they discussed the security requirements, existing attacks, threats and possible solutions in IoT communication. Moreover, they explained how blockchain technology could be utilized to resolve the IoT security problems. Some of the open research problems and challenges in IoT security were also highlighted.

Das *et al.* [32] (2018) presented a survey on security protocols in IoT. They have provided the details of various types of attacks possible in IoT communication. A taxonomy of security protocols under different categories such as ''key management'', ''user authentication'', ''identity management'' and ''access control'' is provided. Few emerging research directions of the future are also highlighted.

Khan *et al.* (2019) [1] presented a survey work contained the details of core technologies which are used to implement a 5G security model. They discussed the security monitoring and management of 5G networks. The related security measures and standards of core 5G technologies were also added. Moreover, some key projects of international significance in 5G were discussed. Some future research directions were also highlighted.

Zhou *et al.* (2019) [33] identified some reasons for threats and challenges in IoT security. The eight IoT features which had the most impact on security and privacy of IoT communication were discussed. The current trends of IoT security along with the reasons and explanations were highlighted.

Noor *et al.* (2019) [34] presented the analysis of recent research in IoT security i.e., the trends and open issues. The details of the current state of IoT security research, the relevant tools, ''IoT modellers'' and ''IoT simulators'' were also provided.

Sengupta *et al.* (2020) [35] classified the attacks on the basis of objects of vulnerability. These attacks were also mapped according to the layers of generalized IoT architecture. Some countermeasures for these attacks were also provided. The features of blockchain along with its integration into the IoT applications were discussed. A taxonomy of IoT and Industrial IoT security research areas along with the countermeasures were presented. Some of the research directions of this domain were also highlighted.

The summary of the existing surveys on security in 5G-enabled IoT environment is also tabulated in Table 2.

G. MOTIVATION OF THIS WORK

5G-enabled IoT environment, suffers from different types of security and privacy related issues as it is vulnerable to various types of attacks such as ''replay'', ''man-in-the-middle'', ''impersonation'', ''password guessing'', ''physical device stealing'', ''illegal session key computation'', ''privileged-insider'', ''malware'', ''malicious routing'', many more. Hence it becomes essential to protect the infrastructure of 5G-enabled IoT environment against the different types of possible attacks. Therefore, time to time researchers proposed different types of security protocols under different types of categories like ''key management'', ''user authentication/device authentication'', ''access control/user access control'' and ''intrusion detection''. In this reviewed paper our motivation is to bring all these work under the one roof. So that the future readers will be much benefited with this work. Henceforth, the details of different types of security protocols for 5G-enabled IoT environment are provided.

H. MAIN CONTRIBUTIONS

The contributions of this work are provided below.

- The details of various types of system models i.e., network model and threat model require for 5G-enabled IoT environment are provided.
- Security requirements along with the potential attacks in 5G-enabled IoT environment are further added.
- The various categories of security protocols i.e., ''key management'', ''user authentication/device authentication'', ''access control/user access control'' and ''intrusion detection'' in 5G-enabled IoT environment are discussed.
- The analysis and comparisons of the existing security protocols in 5G-enabled IoT environment are conducted.
- Finally, some of the future research challenges and directions in the security of 5G-enabled IoT environment are highlighted.

I. ORGANIZATION OF THE PAPER

Remaining part of the paper is presented as follows. Various system models i.e., network model and threat model require for 5G-enabled IoT environment are presented in Section II. Section III consists of details of security requirements and potential attacks in 5G-enabled IoT environment. The numerous categories of security protocols i.e., ''key management'', ''user authentication/device authentication'', ''access control/user access control'' and ''intrusion detection'' in 5G-enabled IoT environment are given in Section IV. Section V consists of the details of analysis and comparisons of the existing security protocols in 5G-enabled IoT environment. Section VI contains the details of research challenges

TABLE 2. Existing surveys on security in 5G-enabled IoT environment.

Reference & Year	Details of network and threat models in IoT environment	Security and privacy issues	Security requirements and possible attacks	Categories of security protocols in IoT environment	Comparative study of different types of security protocols in IoT environment	Future research directions of security protocols in IoT environment	Key areas covered
Granjal *et al.* [17] (2015)	×	×	✓	×	×	✓	Analysis on the security protocols in IoT, existing research proposals and challenges in IoT security for the future researchers
Khan *et al.* [31] (2018)	Only network model	✓	✓	×	×	✓	Categories of security issues, discussed security requirements, existing attacks, threats and possible solutions in IoT, use of blockchain in resolving the IoT security problems, open research challenges in IoT security
Das *et al.* [32] (2018)	Only threat model	✓	✓	Details of IDS not available	Comparisons of IDS not available	✓	Provided the details of various types of attacks possible in IoT communication. A taxonomy of security protocols under different categories is provided along with few emerging research directions
Khan *et al.* [1] (2019)	Only network model	✓	✓	×	×	×	Core technologies for 5G security model, network softwarization security, 5G privacy concerns, security measures and standards of 5G technologies, key projects, future research directions
Zhou *et al.* [33] (2019)	×	✓	✓	×	×	×	Identified reasons for threats and challenges in IoT security, eight IoT features which had the most impact on security and privacy of IoT communication, current trends of IoT security along with the reasons and explanations
Noor *et al.* [34] (2019)	×	×	Only attacks	×	×	×	Analyzed the current research in the field of IoT security, details of relevant security tools, different IoT simulators and modellers
Sengupta *et al.* [35] (2020)	×	✓	✓	×	×	×	Provided countermeasures for the classified attacks, features of blockchain along with its integration into the IoT applications, a taxonomy of IoT/IIoT security research areas along with the countermeasures, some research directions
Proposed work	✓	✓	✓	✓	✓	✓	details of network model & threat model, security requirements and attacks possible, categories of security protocols, analysis and comparisons of the existing security protocols, future research challenges and directions

for the future in the security of 5G-enabled IoT environment and some directions to resolve them. The details of lessons that has been learnt from this work are available in Section VII. Section VIII contains some concluding remarks of this work.

II. SYSTEM MODELS

In an 5G-enabled IoT environment following models can be utilized.

A. NETWORK MODEL

The network model of the 5G-enabled IoT environment is given in Fig. 2. In this figure there are different types of scenarios i.e., smart farming, smart home, smart manufacturing, smart transportation system, smart healthcare and smart grid. These scenarios consists of various types of smart IoT devices such as smart vehicles, smart healthcare device (for example, connected inhalers), smart home appliances (for example, smart AC controller), smart meters, smart soil

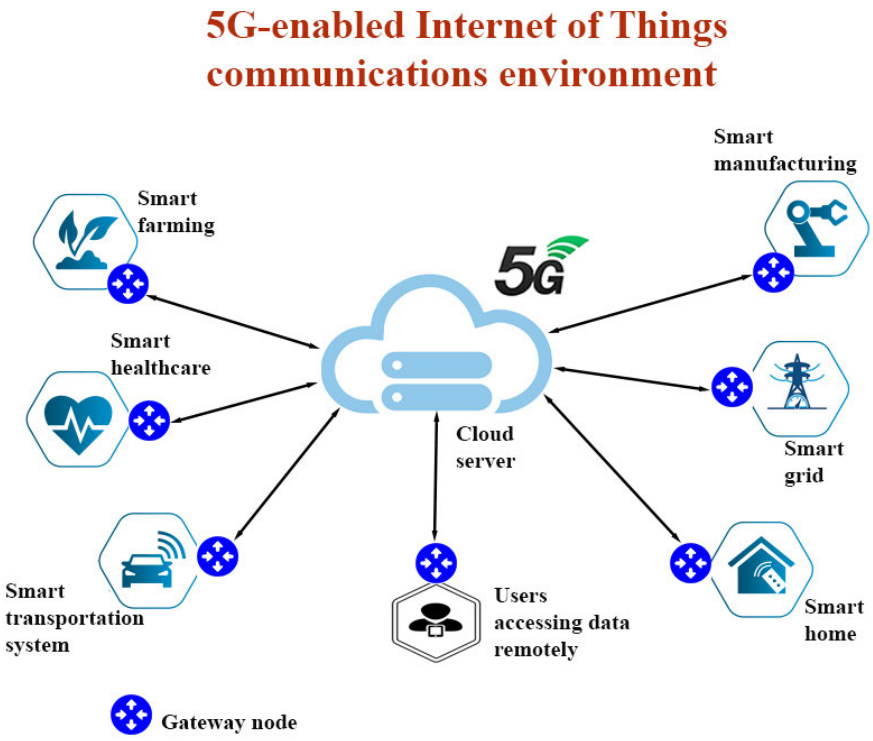

FIGURE 2. Network model of 5G-enabled IoT environment (adapted from [11]).

moisture sensor and smart industrial devices. These devices sense, monitor and control some the required functions. The smart devices send the data to some central units such as cloud servers or fog servers through specific devices (i.e., gateway nodes). In the given figure, there are also various types of users (i.e., IoT mobile app user) and they wish to access the data of the IoT devices remotely. Users can access the data of IoT devices via gateway nodes using the Internet connection. In such kind of communication environment, data generation and communication happen at the massive scale. Therefore, some strong communication infrastructure for such kind of communication environment which provides very efficient communication with very low latency is needed. Hence 5G communication infrastructure is much suitable for this environment [1]–[3], [11], [22], [23], [37], [54]–[56]. This communication environment also suffers from some ''security and privacy'' issues as it is prone to various types of attacks. The details of associated threats of such kind of communication environment are provided in Section II-B.

B. THREAT MODEL

The widely-accepted ''Dolev-Yao (DY) threat model'' [57] can be accepted in the designing of ''security protocols'' in 5G-enabled IoT environment. As information provided in Section IV, the security protocols are the collection of different types of protocols such as ''key management'', ''user authentication/device authentication'', ''access control/user access control'' and ''intrusion detection''. According to the guidelines of the DY model, two communicating entities disseminate through a open (insecure) communication medium. The terminus nodes functioning as cloud/fog servers, IoT devices are not in general trustworthy. The existing network adversary ($\mathcal{A}$) has the ability to eavesdrop, delete or update the exchanged messages as the channel is open (insecure). Another model, ''Canetti and Krawczyk's adversary model'' in short ''CK-adversary model'' [58], also the current *de facto* standard model for the designing and modeling of an ''authenticated key agreement'' security mechanism. In this model, $\mathcal{A}$ can have same capabilities like the DY model. Moreover, $\mathcal{A}$ can also accommodate the secret credentials along with the ''session states & session keys'' utilized in a session. Furthermore, $\mathcal{A}$ has the ability to physical capture some of the smart IoT devices to deduce the stored information from the devices by the application of steps of ''power analysis attack'' [59]. The obtained data can be used to launch other types of severe attacks like computation of ''identities'', ''passwords'' and ''session key''. This helps $\mathcal{A}$ to launch other attacks in the network for example, ''device impersonation attack'', ''replay attack'', ''man-in-the-middle attack'' and ''privileged-insider attack''. Apart form that $\mathcal{A}$ can reproduce new malicious devices with other attack launching functions (i.e., wormhole, blackhole) by the help of extracted information. After fabricating these malicious devices (i.e., blackhole attacker nodes) $\mathcal{A}$ directly deploys them in the target area [60]–[62]. Under the effect of discussed attacks the data packets (messages) can be lost, dropped, delayed or updated. Again it affects the performance of the communication in an 5G-enabled IoT environment.

This causes diminution in ''throughput'' and ''packet delivery ratio'' and accretion in ''end-to-end delay''.

III. SECURITY REQUIREMENTS AND POTENTIAL ATTACKS IN 5G-ENABLED IoT COMMUNICATION

Here, various ''security and privacy'' issues of 5G-enabled IoT communication are discussed. Apart from that the security requirements and the possible attacks are discussed.

A. SECURITY AND PRIVACY ISSUES IN 5G-ENABLED IoT COMMUNICATIONS

Although IoT is rapidly growing and researchers discovered the new techniques to fix the issues in IoT communication. But it still faces security and privacy issues [63]–[67].

- **Lack of robust security schemes:** IoT devices are connected with the system i.e., desktop or smartphone. In such an environment the lack of security mechanism improves the threat of leakage of personal data. The collected and transmitted data of IoT devices may be disclosed (i.e., health data collected through smart healthcare devices).
- **Openness of the network:** It is necessary to connect IoT devices with a consumer network which have connection with the other the systems. It is also possible that IoT devices comprehend with some security vulnerabilities, which may be harmful for the network of the consumers. Because it may become the entry point for the attacker to get entry into the system.
- **Privacy of sensitive data:** IoT environment consists of different types of devices, which have various types of hardware and software. Some of them may be vulnerable to different attacks i.e., replay, MITM, impersonation, password guessing, etc. Therefore, the sensitive data may be leaked through unauthorized access and manipulations. Some of these devices transmit user's personal information such as name, address, contact number, date of birth, health data and credit card. Hence it is always required to protect the communication of IoT against the possible attacks.

B. SECURITY REQUIREMENTS IN 5G-ENABLED IoT ENVIRONMENT

The essential security requirements in 5G-enabled IoT environment along with the ''general security requirements'' are provided here [68]:

- *Authentication procedure:* This procedure is used to validate the identities of the communicating devices (i.e., IoT device). Mutual verification of identities is mandatory to start a secure communication and it should be conducted in advance. In a 5G-enabled IoT environment, authentication may be happened among the smart IoT devices, various kind of servers (i.e., cloud, fog, edge servers), various kind of users, the service providers and gateway nodes.
- *Integrity property:* It provides assurance of real and accurate data. The composition of the received message should not accommodate illegal inject, unapproved modification and removal. Data should be safeguarded against unauthorized modification.
- *Confidentiality property:* This property provides protection of information against any kind of unauthorized access. In another way, it is known as ''privacy'' which protects the exchanged messages against any kind of disclosure attacks.
- *Non-repudiation property:* It assures any entity should not deny the validity of something for example, a message. It is one of important service in ''information security'' which provides proof regarding the ''origin of the message'' and ''integrity of the data'' in that message. Therefore, it is very difficult for the illegal entities to deny the ''origin of the message'' and ''authenticity of the message''. Digital signatures methods are useful for ''non-repudiation''. For example, in case of a online transactions, where it is important to assure that a party to whom the contract was made (communicated party) should not deny the originality of his/her signature on the report. It has following categories:
  - Source's non-repudiation: It provides assurance of genuineness of the sender. This concludes the message was transmitted by the genuine source.
  - Destination's non-repudiation: It provides assurance of genuineness of the receiver. This concludes the message was received by the genuine receiver.
- *Authorization procedure:* Authorization procedure is used to regulate device or user privileges (i.e., access restrictions) for network or system resources (i.e., files, data applications and services). Generally, it is anticipated by authentication procedure for the verification of identities of device or user. In general a authority (for example, a administrator) designs and implements the access rules for all available resources.
- *Freshness property:* This property provides assurance of ''data freshness''. Hence the illegal entity will not be able to re-transmit the previously exchanged messages.
- *Availability property:* It provides assurance that the information is only available to the genuine entities. If an adversary is not able to produce the attack on the confidentiality and the integrity then he/she may contend for other hazardous attacks such as distributed denial-of-service (DDoS) attack on a web server which brings down the associated websites.
- *Forward secrecy property:* If an entity (for example, smart home user, smart IoT device) leaves the communication network then it must not have any ability to access the future messages.
- *Backward secrecy property:* If an entity (for example, smart home user, smart IoT device) is just deployed in the communication network then this entity should not be able to access the previously exchanged messages.

C. POSSIBLE ATTACKS IN 5G-ENABLED IoT COMMUNICATION

An 5G-enabled IoT communication can have following potential attacks which may be performed by a passive or an active adversary [69]:

- *Eavesdropping:* It is also called as sniffing or snooping attack. It happens in case when attacker eavesdrops the exchanged messages among the communicating parties. It is one of the potential attacks in 5G-enabled IoT communication as this will help the attacker to launch further attacks.
- *Traffic analysis:* It is a another form of passive attack in which attacker does the interception and an examination of the exchanged messages to figure out what's going on there.
- *Replay attack:* It happens when a attacker intercepts the exchanged messages and then deceitfully delays or re transmits it to confound the receiving entity.
- *Man-in-the-middle attack (MITM):* In this malign activity, first attacker expropriates the transmitted messages and then attempts to update or delete the messages before forwarding them to the receiver.
- *Impersonation attack:* In this malign activity, a attacker successfully determines the identity of a genuine communicating party and then creates a message and sends that to the recipient on the behalf of the ''genuine communicating party''.
- *Denial-of-Service attack:* In this malign activity, an adversary conducts some vengeful tasks to prevent the legitimate parties from accessing the resources of the network or system (for instance, some data resource or some IoT device). There is also a variant DoS of attack, called as the ''Distributed DoS (DDoS)'' attack which is conducted through the multiple attacker systems simultaneously. Some of the examples are UDP, HTTP, TCP SYN flooding attacks. The flooded packets under these attacks consume the resources (for example, bandwidth) of the targeted system (i.e., web servers) very quickly [70]–[72]. In an 5G-enabled IoT communication the DoS attack can also preformed through other types of routing attacks for instance, sinkhole, wormhole, greyhole, blackhole and misdirection attacks. In such attacks the physically deployed attacker nodes disturb the ongoing routing process to drop, delay or modify the exchanged packets. In presence of such attacks data messages (packets) may be altered, delayed or dropped before reaching to their intended recipient. This causes increment in the ''end-to-end delay'', diminution in the ''throughput'' and also affects the other network performance parameters [60]–[62], [73].
- *Database attack:* In an 5G-enabled IoT communication, database related attacks are also feasible on the database managed through different servers i.e., fog server, cloud server. The examples are ''Structured Query Language (SQL) attack'', ''Cross-Site Scripting (XSS) attack'' and ''Cross-Site Request Forgery (CSRF)''. The existing adversary launches these attacks to harm the financial assets for example, he/she may perform illegal money transfer from a authorised user's account or may change the password of a genuine user's account.
- *Malware attack:* Sometimes an adversary executes malicious script in a remote system to perform various unauthorized activities for example, stealing, deletion, updating and encryption of important information. Malware may be of different types, for example, virus, worms, keylogger, spyware, ransomware and Trojan horses. They are also used to monitor the activities of the users without his/her consent. For the spreading of malware in IoT environment adversary can use botnet (associated and collaborated attacker systems). The botnets like Mirai, Reaper, Echobot and Necurs are active these days. These attacks may also harm the functioning of 5G-enabled IoT environment. A smart IoT device can be hijacked (controlled) remotely by making the use of malware. Sometimes it is vary risky for the people (for example, smart pacemaker probably initiates inessential electrical pulses for a patient and under such circumstances patient may die) [74]–[85].
- *Insider attack:* In this malign activity, ''a privileged-insider user'' of the trusted authority exploits the stored information to introduce other severe attacks such as session key computation, password guessing attack.
- *Physical capturing of deployed devices:* The physical monitoring of IoT devices is not possible for 24×7 hours. Therefore, sometimes adversary gets chance to capture these device physically and then tries to extract the sensitive information (i.e., identities, secret keys, etc.) from the memories of these devices. Further adversary may utilize this information to conduct other unwanted activities (for example, impersonation, password guessing, session key computation and man-in-the-middle (MITM) attacks) in an 5G-enabled IoT environment [59].

IV. CATEGORIES OF SECURITY PROTOCOLS IN 5G-ENABLED IoT COMMUNICATIONS ENVIRONMENT

As discussed earlier 5G-enabled IoT communications environment suffers from various attacks. Therefore, researcher working in this domain proposed various security protocols which can be divided into different categories for example, ''key management protocols'', ''authentication/user authentication protocols'', ''access control/user access control protocols'' and ''intrusion detection protocols'' [1], [17], [31]–[35]. In this section, some of existing security protocols of this domain under the discussed categories are briefed. The pictorial view of classification of security protocols in 5G-enabled IoT communications environment is also provided in Fig. 3.

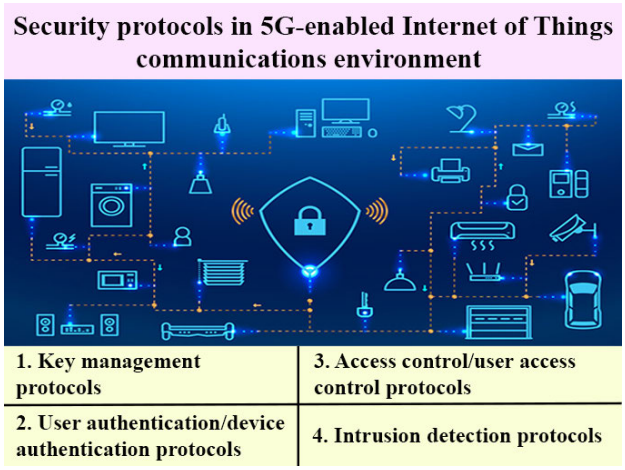

FIGURE 3. Classification of security protocols in 5G-enabled IoT communications environment.

A. KEY MANAGEMENT

A key management protocol does the generation, distribution, establishment and management of cryptographic keys among the communicating parties in an IoT environment. The defined procedure contains various steps such as ''generation of key'', ''exchange of key'', ''usage of key'' and ''revocation of key'' according to the demand. Key management protocol utilizes a ''cryptographic procedure'' that keeps the details of key servers (the trusted authority), various types of users (i.e., static or mobile) and devices involved (for example, smart IoT device). To provide secure communication strong key management practice should be followed [56], [86]–[89]. Ordinarily, a key management protocol contains some phases like ''pre-deployment phase'', ''key generation and distribution phase'', ''key establishment phase'' and ''key revocation & dynamic device addition phase'' [56], [90]–[104]. The details of different phases of key management protocols are provided in Fig. 4.

B. USER AUTHENTICATION/DEVICE AUTHENTICATION

User/device authentication is a procedure of identification and verification of the identities of the communicating entities i.e., user or device. Generally, the communicating entities user, smart IoT devices verify their identities among each other which is also known as mutual authentication. After the successful completion of ''mutual authentication'', the disseminating entities establish a session key to secure their communication. Device authentication also happens in the same way. In order to simplify this, the details of user authentication process are given. A user authentication scheme for an 5G-enabled IoT communications contains phases such as ''system setup and pre-deployment phases'', ''user registration phase'', ''login phase'', ''authentication & key agreement phase'', ''password & biometric update phase'' and ''dynamic device addition phase''. The details of these phases are provided in Fig. 5. The ''two factor'' and ''three factor'' user authentication mechanisms are very common in practice which administer security on the basis of the available factors. The three factors used in authentication methods are like user's credentials (i.e., information of used username and password), user's used device (i.e., smart card or smartphone) and user's biometrics information (i.e., his/her iris scan or fingerprints) [14], [22], [40], [48], [55], [104]–[109].

C. ACCESS CONTROL/USER ACCESS CONTROL

The access control methods put restriction on the access of the user or device to the resources of a network or system. The followed mechanism grants access and privileges to different users or devices for the various available resources. To enhance the overall lifetime of the IoT communication environment, it is required to add new devices i.e., smart IoT device in the network. That may occur in case if a device stop its working due to battery depletion or some physical stealing [59]. There are also the chances that an adversary tries to install his or her malicious device in the target area [60], [61]. For this reason, it is essential to differentiate among malicious devices and legitimate devices. Accordingly, secure access control methods to restrict the entry of pernicious entities in 5G-enabled IoT environment should be designed. Access control protocols has two categories ''certificate-based access control'' and ''Certificate-less access control''. These protocols contain phases such as ''device authentication phase'' and ''key establishment phase'' [24], [54], [110], [111]. The details of different categories and phases of access control protocols are provided in Fig. 6. However, It is important to notice that to provide the access to the genuine users for certain resources and services user access control protocols are utilized.

D. INTRUSION DETECTION

Intrusion detection protocols are deployed for the monitoring and analysis of pernicious exertions inside a system or a network. A system which does this work of ''intrusion detection'' is named as ''intrusion detection system (IDS)''. An IDS defends various devices i.e., smart IoT device against the potential attacks. The used intrusion detection technique in an 5G-enabled IoT environment monitors and verifies the different types of traffic (may be normal or malicious), and then predicts the sign of intrusions. If an intrusion is detected then the linked tool takes the required action for example, blocks the IP of malicious source or sends the information of intrusion to the administrator. Apart from that there also some possibilities that an adversary may physically steal few IoT devices. Then adversary may try to deduce the secret information (i.e., credentials, secret keys) from the stolen device through the steps of ''power analysis attacks'' [59]. Further, the adversary tries to set up his/her pernicious nodes (devices) by storing the deduced information in these nodes. These ''malicious devices'' are capable to launch some hazardous attacks i.e., routing attacks (for example, sinkhole, blackhole, misdirection, wormhole, etc.) [60]–[62], [73]. Under the effect of these potential attacks, the exchanged information may be leaked, modified, delayed or dropped

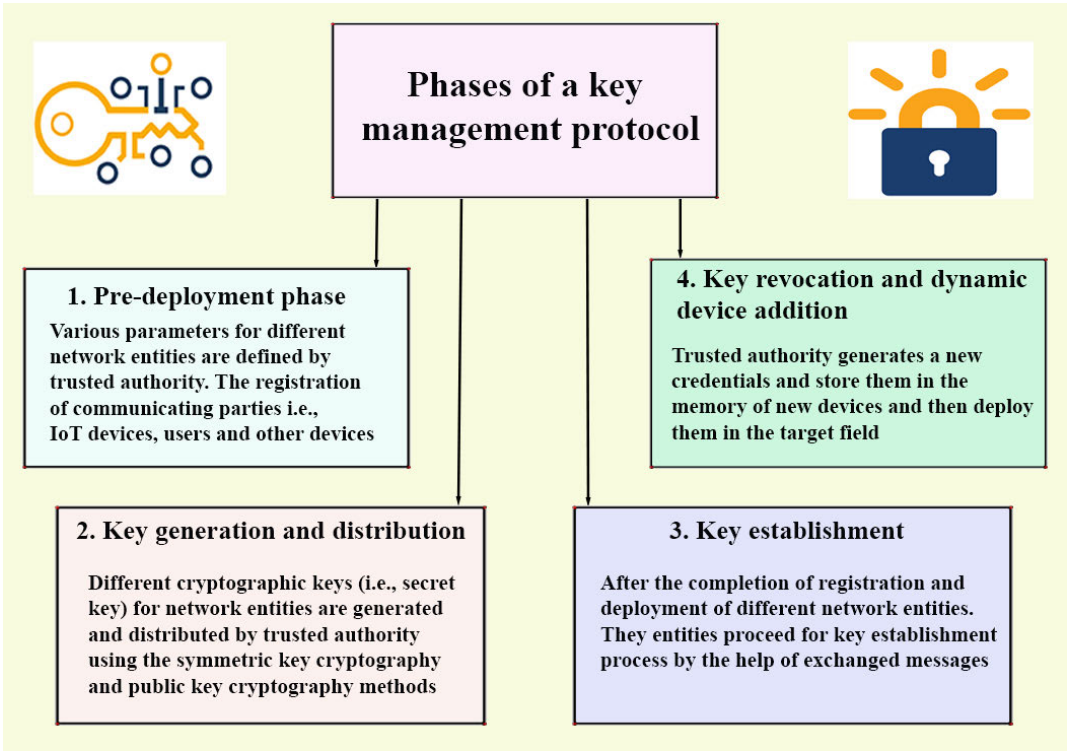

FIGURE 4. Phases of key management protocols.

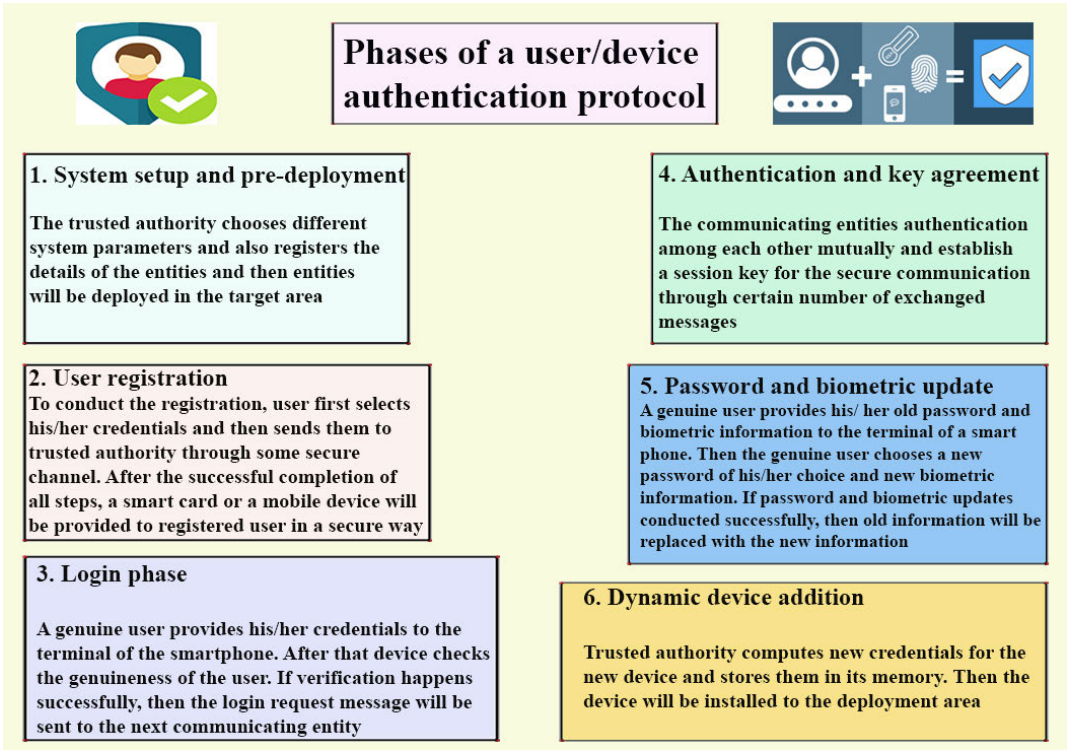

FIGURE 5. Phases of user authentication/device authentication protocols.

before forwarding them to the required destination. That causes serious deterioration in the performance of the network i.e., improvement in ''end-to-end delay'', decrement in ''network throughput'' and ''packet delivery ratio'' [61], [73]. Moreover, IoT botnets may also attack such kind of communication through which the bots make efforts to install

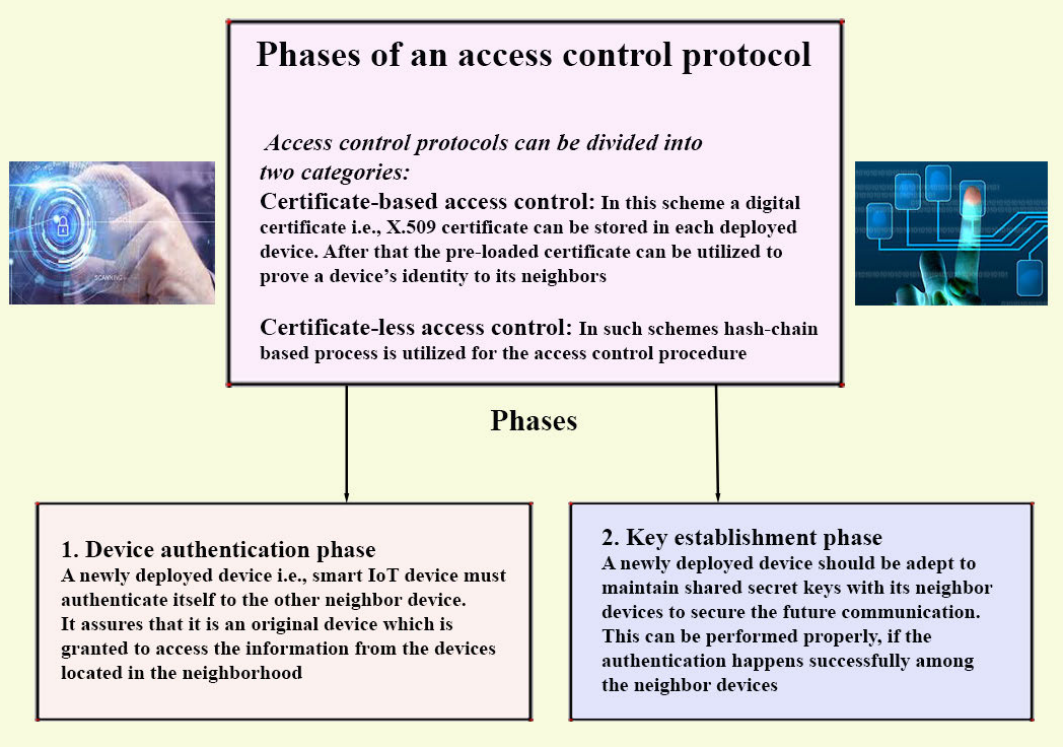

FIGURE 6. Phases of access control protocols.

malware in the operating system or in the memory of IoT devices. Under the existence of malware attacks, the IoT devices may work inaccurately or stop completely. Hence it is crucial to provide protection to the 5G-enabled IoT environment against the intrusions. Therefore, it is mandatory to study intrusion detection protocols for such an environment [12], [13], [74], [112]–[117]. IDS can be divided into two classes on the basis of the deployment: i) ''network based intrusion detection system (NIDS)'' which recognizes interventions inside a network (for example, Suricata) and ii) ''host based intrusion detection system (HIDS)'' which recognizes interventions inside a system (for example, OSSEC). Furthermore, ''intrusion detection techniques'' can be categorised as: i) ''misuse based detection'', ii) ''anomaly based detection'' and iii) ''specification based detection'' [118], [119]. Their features are available in Fig. 7.

V. EXISTING SECURITY PROTOCOLS IN 5G-ENABLED IoT COMMUNICATIONS ENVIRONMENT

As discussed in Section IV, the security protocols in 5G-enabled IoT communications environment can be divided into four categories. Here the details of some of the existing protocols belong to these categories are provided.

A. EXISTING KEY MANAGEMENT PROTOCOLS IN IoT ENVIRONMENT

The details of authentication and key management schemes is provided in the following part of this section. Li *et al.* [120] presented a identity-based hierarchical model for cloud computing. It has associated encryption and signature techniques which were used in the designing of identity-based authentication schemes for cloud computing services. It was proved that the presented method was efficient than ''secure socket layer (SSL) authentication protocol''. Li *et al.* [121] used the ''elliptic curve cryptography (ECC)'' for the designing of an authentication protocol suitable for cloud computing environment. Hu *et al.* [122] proposed methods for identity authentication, data encryption and data integrity checking. The methods were proposed to achieve confidentiality, integrity and availability properties. Mishra *et al.* [123] also proposed a authentication and key management scheme for secure multimedia communications in IoT-enabled WSNs. Later on it was observed that some of the existing schemes lacking in security and functionality features as various attacks such as ''smart card stolen'', ''impersonation'', ''password guessing'', ''replay'' and ''man-in-the middle'' attacks were possible [109]. Sharif *et al.* [124] proposed ''a lightweight authentication and key agreement scheme'' for IoT based WSNs. The formal security verification by employing the automated formal security verification software toll named as ''Automated Validation of Internet Security Protocols and Applications (AVISPA)'' [125] is also provided for [124]. Wazid *et al.* [56] proposed a ''key management and authentication'' technique for the secure communication in fog computing environment. The key management procedure was utilized for the ''smart devices and fog servers'' &

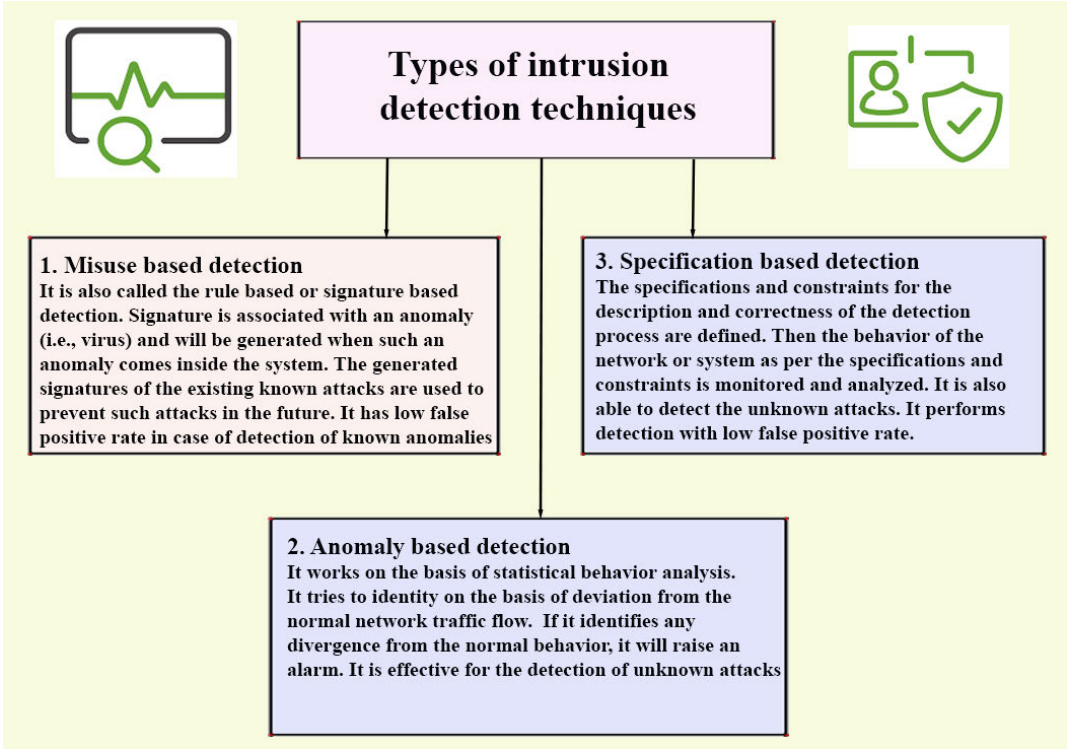

FIGURE 7. Types of intrusion detection techniques.

"fog servers and cloud servers", "pairwise key establishment" for the secure communication.

1) COMPARATIVE STUDY OF EXISTING KEY MANAGEMENT PROTOCOLS IN IoT ENVIRONMENT

The comparative study of existing key management protocols in IoT environment is provided in Table 5. The protocols of Li *et al.* [120], Li *et al.* [121], Hu *et al.* [122], Mishra *et al.* [123], Sharif *et al.* [124] and Wazid *et al.* [56] were compared and analyzed. The protocols of Li *et al.* [120], Li *et al.* [121], Hu *et al.* [122] did not support most of the required security and functionality features whereas the protocols of Mishra *et al.* [123], Sharif *et al.* [124] did not provide the support for multi-server environment. Moreover, the formal security analysis using the widely accepted Real-Or-Random (ROR) model [126] were not provided for most of the protocols. The protocol of Wazid *et al.* [56] supported most of the security and functionality features and they have also provided different types of security analysis for their protocol.

The comparison of computation cost of different protocols is given in Table 3. Suppose T_{ecm}, T_{eca}, T_{sed}, T_h, T_{fe}, T_α, T_β, T_ρ, T_χ, T_{exp}, T_{pke} and T_{pkd} represent the computational time required for "an elliptic curve point multiplication", "an elliptic curve point addition", "a symmetric encryption/decryption operation", "a cryptographic one-way hash function $h(\cdot)$ operation", "a fuzzy extraction operation (fuzzy extractor probabilistic generation function $Gen(\cdot)$ or fuzzy extractor deterministic reproduction function $Rep(\cdot)$ [127])", "identity-based encryption (IBE)", "identity-based decryption", "identity-based signature generation", "identity-based signature verification", "modular exponentiation operation", "public key encryption operation" and "public key decryption operation", respectively. The time taken for the computation of bitwise XOR operation can be considered negligible. Hence it is not considered in the performance evaluation. The evaluation results for various cryptographic operations are provided in [128]–[130]. The various experiment values as provided in [128]–[130] for T_{ecm}, T_{eca}, T_{sed} and T_h are 0.063075 s, 0.010875 s, 0.0087 s and 0.0005 s, respectively. Like [130], it is assumed that the execution time requires for a fuzzy extractor is approximately equal to an elliptic curve point multiplication time at most, which is $T_{fe} \approx T_{ecm} = 0.063075$ s. Furthermore, as depicted in [128], $T_{exp} \approx 60\ T_{sed} = 0.522$ s, and $T_{pke}/T_{pkd} \approx 100\ T_{sed} = 0.87$ s can be considered. Therefore the

TABLE 3. Comparison of computation cost- key management protocols.

Protocol	Li *et al.* [120]	Mishra *et al.* [123]	Li *et al.* [121]	Hu *et al.* [122]	Wazid *et al.* [56]	Sharif *et al.* [124]
Cost	$1T_\alpha+1T_\beta+1T_\rho+1T_\chi$	$23T_h$	$13T_h+5T_{ecm}+4T_{sed}$	$4T_{exp}+3(T_{pke}+T_{pkd})$	$35T_h+5T_{ecm}+1T_{fe}$	$33T_h$
Time (ms)	243	11.5	356.68	7308	395.95	16.5

computational time for the schemes of Li *et al.* [120], Mishra *et al.* [123], Li *et al.* [121], Hu *et al.* [122], Wazid *et al.* [56] and Sharif *et al.* [124] are 243 ms, 11.5 ms, 356.68 ms, 7308 ms, 395.95 ms and 16.5 ms, respectively. The schemes of Mishra *et al.* [123] and Sharif *et al.* [124] are efficient from the computation cost point of view.

TABLE 4. Comparison of communication cost- key management protocols.

Protocol	Li *et al.* [120]	Mishra *et al.* [123]	Li *et al.* [121]	Hu *et al.* [122]	Wazid *et al.* [56]	Sharif *et al.* [124]
No. of messages	2	4	4	3	3	6
Cost (bits)	14280	2528	4160	7168	2816	2720

TABLE 5. Comparison of functionality and security features of key management protocols in IoT environment.

Protocol /Feature	Li *et al.* [120] 2009	Li *et al.* [121] 2015	Hu *et al.* [122] 2017	Mishra *et al.* [123] 2017	Sharif *et al.* [124] 2019	Wazid *et al.* [56] 2018
$\phi\phi_1$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_2$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_3$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_4$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_5$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_6$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{T}$
$\phi\phi_7$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_8$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_9$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{T}$

Note: $\phi\phi_1$: device anonymity property; $\phi\phi_2$: privileged-insider attack; $\phi\phi_3$: replay attack; $\phi\phi_4$: man-in-the middle attack; $\phi\phi_5$: session key agreement; $\phi\phi_6$: support for multi-server environment; $\phi\phi_7$: provide formal security verification using Automated Validation of Internet Security Protocols and Applications (AVISPA) tool; $\phi\phi_8$: Session key security; $\phi\phi_9$: formal security analysis using Real-Or-Random (ROR) random oracle model
$\mathcal{F}$: insecure against a particular attack or does not support a specific feature; $\mathcal{T}$: secure against a particular attack or supports a specific feature.

The comparison of communication cost of various protocols is available in Table 4. The different sizes are assumed as "identity is 160 bits", "prime p in $E_p(a, b)$ is 160 bits" by contemplating the security of "160-bit elliptic curve cryptography (ECC)" commensurate to "1024-bit RSA" [131], "random nonce is 128 bits", "timestamp is 32 bits", "hash digest is 160 bits" (in case of "Secure Hash Algorithm (SHA-1) hash function" [132]), and "block size of a plaintext or ciphertext in symmetric encryption or decryption" (in case of "Advanced Encryption Standard (AES) [133]") is 128 bits. Public key cryptography is followed in Hu *et al.*'s scheme [122] utilizes "1024-bit RSA algorithm". Therefore the communication costs for the protocols of Li *et al.* [120], Mishra *et al.* [123], Li *et al.* [121], Hu *et al.* [122], Wazid *et al.* [56] and Sharif *et al.* [124] are 14280 bits, 2528 bits, 4160 bits, 7168 bits, 2816 bits and 2720 bits, conjointly. The protocols of Mishra *et al.* [123], Wazid *et al.* [56] and Sharif *et al.* [124] are efficient from the communication cost point of view.

B. EXISTING USER AUTHENTICATION PROTOCOLS IN IoT ENVIRONMENT

The details of user authentication protocols in IoT environment is given as follows. Porambage *et al.* [134] proposed a "certificate-based authentication scheme" in WSNs for distributed IoT applications. The developed scheme had "two-phase authentication protocol" which allowed the sensor nodes and the end-users to authenticate each other and to maintain a secure connection. Porambage *et al.* [135] presented two group key establishment protocols for secure IoT communication. The deployment conditions and requirements of the protocols were also described in terms of IoT application scenarios. The proposed protocols were also analyzed and justified in terms of performance analysis, scalability and security. Turkanovic *et al.* [136] proposed "a user authentication and key agreement scheme" for heterogeneous WSNs applicable to IoT. The presented scheme helped the remote user to establish a secure session key with a sensor node by the help of a lightweight key agreement mechanism. The presented method also ensured the "mutual authentication" among the user, sensor node and the gateway node. Their presented scheme could be adapted for the resource-constrained WSN as it only utilized "simple hash" and "XOR computations". Farash *et al.* [137] proposed a protocol for "user authentication and key agreement" for heterogeneous WSN applicable for IoT environment. Challa *et al.* [11] presented a user authentication protocol for IoT applications. The presented scheme was based on "elliptic curve cryptography (ECC)" and depended on "ECC-based digital signature". The presented scheme supported user anonymity and untraceability properties. However, this scheme needed more computation and communication costs. Wazid *et al.* [138] proposed "a lightweight authentication protocol" in cloud-based IoT environment (LAM-CIoT). Through LAM-CIoT, an authenticated user could access the data of a remote IoT sensors securely. LAM-CIoT utilized efficient "one-way cryptographic hash functions" along with "bitwise XOR operations". LAM-CIoT was also analyzed for security part by the help of formal security analysis using the widely-used "Real-Or-Random (ROR)" model, formal security verification through "Automated Validation of Internet Security Protocols and Applications (AVISPA)" tool as well as the informal security analysis. It proved the resilience of the presented protocol against possible attacks.

1) COMPARATIVE STUDY OF EXISTING USER AUTHENTICATION PROTOCOLS IN IoT ENVIRONMENT

The comparisons of functionality and security features of user authentication protocols in IoT environment is provided in Table 8. The schemes of Porambage *et al.* [134], Porambage *et al.* [135], Turkanovic *et al.* [136] and Farash *et al.* [137] did not support most of the security and functionality features. However, the scheme of

Challa *et al.* [11] and Wazid *et al.* [138] provided most of security and functionality features. But the scheme of Challa *et al.* [11] produced little more computational and communication overhead. Hence from the security, functionality features and computation & communication costs point of views the scheme of Wazid *et al.* [138] seems much better.

The computation and communication costs for the schemes of Porambage *et al.* [134], Porambage *et al.* [135], Turkanovic *et al.* [136], Farash *et al.* [137], Challa *et al.* [11] and Wazid *et al.* [138] are computed and analysed. The similar assumptions are taken as the information available in Section V-A1. The computation cost for the schemes of Porambage *et al.* [134], Porambage *et al.* [135], Turkanovic *et al.* [136], Farash *et al.* [137], Challa *et al.* [11] and Wazid *et al.* [138] are $6T_h + 4T_{ecm} + 2T_{eca}$, $18T_h + 15T_{ecm} + 4T_{eca}$, $19T_h$, $11T_h$, $12T_h + 14T_{ecm} + 1T_{fe}$ and $34T_h + 1T_{fe}$, respectively. Furthermore, time taken for the schemes of Porambage *et al.* [134], Porambage *et al.* [135], Turkanovic *et al.* [136], Farash *et al.* [137], Challa *et al.* [11] and Wazid *et al.* [138] are 79.2, 279.9, 6.08, 3.52, 260.34, 27.98 ms, respectively. Therefore, the user authentication protocols of Turkanovic *et al.* [136], Farash *et al.* [137] and Wazid *et al.* [138] performed better from computation cost point of view. The results are also reported in Table 6.

TABLE 6. Comparison of computation cost- user authentication protocols.

Protocol	Porambage *et al.* [134]	Porambage *et al.* [135]	Turkanovic *et al.* [136]	Farash *et al.* [137]	Challa *et al.* [11]	Wazid *et al.* [138]
Cost	$6T_h + 4T_{ecm} + 2T_{eca}$	$18T_h + 15T_{ecm} + 4T_{eca}$	$19T_h$	$11T_h$	$12T_h + 14T_{ecm} + 1T_{fe}$	$34T_h + 1T_{fe}$
Time (ms)	79.2	279.9	6.08	3.52	260.34	27.98

The communication cost for the schemes of Porambage *et al.* [134], Porambage *et al.* [135], Turkanovic *et al.* [136], Farash *et al.* [137], Challa *et al.* [11] and Wazid *et al.* [138] are also computed and analysed. The similar assumptions are taken as the information available in Section V-A1. The communication cost for the schemes of Porambage *et al.* [134], Porambage *et al.* [135], Turkanovic *et al.* [136], Farash *et al.* [137], Challa *et al.* [11] and Wazid *et al.* [138] are 1536, 3360, 2720, 2752, 2528 and 1696 bits, respectively. Therefore, the user authentication protocols of Porambage *et al.* [134] and Wazid *et al.* [138] performed better from communication cost point of view. The results are also reported in Table 7.

C. EXISTING ACCESS CONTROL PROTOCOLS IN IoT ENVIRONMENT

The facts of access control protocols in IoT environment are presented in the following part of this section. Li *et al.* [139] proposed an access control technique for wireless sensor networks applicable to IoT environment. They have utilized a heterogeneous signcryption scheme which allowed the party to send a message to another party in an identity-based cryptography environment. Their protocol is costly in terms of computation cost due to utilization of identity-based cryptography (IBC) and bilinear pairing mechanisms. Braeken *et al.* [140] proposed an efficient and distributed authentication protocol (eDAAAS) for the accessing of end nodes in an IoT environment of smart home. Their protocol was based on symmetric key cryptographic technique and one-way cryptographic hash function. Though this protocol had low computation cost but it had high communication cost. Furthermore, this protocol involved gateway node in the access control mechanism between the two IoT devices. Luo *et al.* [141] presented a access control protocol for WSNs applicable to IoT environment. It facilitated the communication of Internet user in an certificate less

TABLE 7. Comparison of communication cost- user authentication protocols.

Protocol	Porambage *et al.* [134]	Porambage *et al.* [135]	Turkanovic *et al.* [136]	Farash *et al.* [137]	Challa *et al.* [11]	Wazid *et al.* [138]
No. of messages	4	4	4	4	3	3
Cost (bits)	1536	3360	2720	2752	2528	1696

TABLE 8. Comparison of functionality and security features of user authentication protocols in IoT environment.

Protocol /Feature	Farash *et al.* [137] (2016)	Challa *et al.* [11] (2017)	Wazid *et al.* [138] (2019)	Porambage *et al.* [134] (2014)	Porambage *et al.* [135] (2015)	Turkanovic *et al.* [136] (2014)
$\phi\phi_1$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{T}$
$\phi\phi_2$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{F}$
$\phi\phi_3$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$	NA	NA	$\mathcal{F}$
$\phi\phi_4$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$	NA	NA	$\mathcal{F}$
$\phi\phi_5$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_6$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{F}$
$\phi\phi_7$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{T}$
$\phi\phi_8$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_9$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_{10}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_{11}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{F}$
$\phi\phi_{12}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_{13}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_{14}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{T}$
$\phi\phi_{15}$	NA	$\mathcal{T}$	$\mathcal{T}$	NA	$\mathcal{F}$	$\mathcal{F}$
$\phi\phi_{16}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{F}$
$\phi\phi_{17}$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$	NA	NA	$\mathcal{F}$
$\phi\phi_{18}$	$\mathcal{F}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{F}$	$\mathcal{T}$

Note: $\phi\phi_1$: user anonymity achievement; $\phi\phi_2$: privileged-insider attack; $\phi\phi_3$: off-line password guessing attack; $\phi\phi_4$: stolen smart card or mobile device attack; $\phi\phi_5$: denial-of-service attack; $\phi\phi_6$: user impersonation attack; $\phi\phi_7$: replay attack; $\phi\phi_8$: man-in-the middle attack; $\phi\phi_9$: mutual authentication achievement ; $\phi\phi_{10}$: provide session key agreement; $\phi\phi_{11}$: support untraceability property; $\phi\phi_{12}$: resilience against sensor node or sensing device physical capture attack; $\phi\phi_{13}$: server independent password update procedure; $\phi\phi_{14}$: sensor node or sensing device impersonation attack; $\phi\phi_{15}$: support biometric update procedure; $\phi\phi_{16}$: formal security verification through AVISPA tool; $\phi\phi_{17}$: smart card revocation process ; $\phi\phi_{18}$: known session-specific temporary information attack.
$\mathcal{F}$: insecure against a particular attack or does not support a specific feature; $\mathcal{T}$: secure against a particular attack or supports a specific feature; NA: not applicable.

cryptography environment with the smart device in an IBC environment. However, their protocol was costly in terms of computation cost because of the utilization of IBC and bilinear pairing mechanisms. Ding *et al.* [142] presented a attribute-based access control mechanism for IoT environment. The blockchain technology was utilized to record the distribution of attributes to avoid the single point failure and for data security. Riad *et al.* [143] proposed access control protocol for managing and securing the cloud-hosted electronic health records. Their protocol ensured the secrecy of patient's data in which only authorized users were able to edit or review the health data of patients. Fan *et al.* [144] presented a privacy preserving multi-authority access control protocol for fog-based IoT environment. In their protocol verifiable outsourced decryption was used to reduce the computation costs for the end user devices. A secure user revocation method was also designed. The discussed protocols [139]–[141], [143], [144] are vulnerable to the session key leakage and other attacks [145]. Das *et al.* [145] presented a certificate-based lightweight access control and key agreement protocol for IoT environment. It utilized mechanisms such as elliptic curve cryptography (ECC) and collision-resistant one-way cryptographic hash function. Various analysis i.e., formal security analysis under "Real-Or-Random (ROR) model", informal (non-mathematical) security analysis and formal security verification through "Automated Validation of Internet Security Protocols and Applications (AVISPA)" tool were provided. The conducted analysis proved the resilience of their protocol against possible attacks.

1) COMPARATIVE STUDY OF EXISTING ACCESS CONTROL PROTOCOLS IN IoT ENVIRONMENT

The comparison of functionality and security features of access control protocols in IoT environment is provided in Table 11. The protocols of Luo *et al.* [141], Li *et al.* [139], Braeken *et al.* [140] and Das *et al.* [145] (2019) were compared and analysed. The protocols of Luo *et al.* [141], Li *et al.* [139], Braeken *et al.* [140] did not provide the required security and functionality features whereas the protocol of Das *et al.* [145] provided the most of the desired security and functionality features along with less computation and communications costs. The protocol of Das *et al.* [145] will be preferable for the access control mechanism in IoT environment.

The comparison of computation costs are provided in Table 9. The protocols of Luo *et al.* [141], Li *et al.* [139], Braeken *et al.* [140] and Das *et al.* [145] are compared and analyzed. The similar assumptions are taken as the information available in Section V-A1. However, T_{bp} and T_{me} are time needed for bilinear paring operation and modular exponentiation operation. As reported in [145], time required for $T_{bp} \approx 32.71$ ms and for $T_{me} \approx 2.25$ ms. The computation costs of protocols of Luo *et al.* [141], Li *et al.* [139], Braeken *et al.* [140] and Das *et al.* [145] are $3T_{ecm} + 4T_{bp} + 4T_h + T_{eca} + T_{me}$, $3T_{ecm} + 5T_{bp} + 2T_h + 2T_{eca}$, $23T_h + 2\,T_{sed}$ and $7T_{ecm} + 6T_h + 3T_{eca}$. The corresponding time values are 173.62, 204.05, 1.40 and 94.41, respectively. The schemes of Braeken *et al.* [140] and Das *et al.* [145] performed better from the computation cost point of view.

TABLE 9. Comparison of computation cost-access control protocols.

Protocol	Luo *et al.* [141]	Li *et al.* [139]	Braeken *et al.* [140]	Das *et al.* [145]
Cost	$3T_{ecm} + 4T_{bp} + 4T_h + T_{eca} + T_{me}$	$3T_{ecm} + 5T_{bp} + 2T_h + 2T_{eca}$	$23T_h + 2T_{sed}$	$7T_{ecm} + 6T_h + 3T_{eca}$
Time (ms)	173.62	204.05	1.40	94.41

TABLE 10. Comparison of communication cost- access control protocols.

Protocol	Luo *et al.* [141]	Li *et al.* [139]	Braeken *et al.* [140]	Das *et al.* [145]
No. of messages	2	2	3	3
Cost (bits)	3040	3488	3552	3296

TABLE 11. Comparison of functionality and security features of access control protocols in IoT environment.

Protocol /Feature	Luo *et al.* [141] (2018)	Li *et al.* [139] (2016)	Braeken *et al.* [140] (2016)	Das *et al.* [145] (2019)
$\phi\phi_1$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_2$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_3$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{T}$
$\phi\phi_4$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_5$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_6$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_7$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_8$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{T}$
$\phi\phi_9$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$	$\mathcal{T}$
$\phi\phi_{10}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{T}$
$\phi\phi_{11}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{F}$	$\mathcal{T}$

$\phi\phi_1$: replay attack; $\phi\phi_2$: man-in-the-middle attack; $\phi\phi_3$: mutual authentication achievement; $\phi\phi_4$: key agreement achievement; $\phi\phi_5$: device impersonation attack; $\phi\phi_6$: malicious device deployment attack; $\phi\phi_7$: resilience against device physical capture attack; $\phi\phi_8$: formal security verification through AVISPA tool; $\phi\phi_9$: proof of formal security analysis; $\phi\phi_{10}$: whether works without involving gateway node during the access control process; $\phi\phi_{11}$: ephemeral secret leakage attack.
$\mathcal{T}$: "protocol is secure against a particular attack or it supports a specific functionality feature"; $\mathcal{F}$: "protocol is insecure against a particular attack or it does not support a specific functionality feature".

The communication costs of protocols of Luo *et al.* [141], Li *et al.* [139], Braeken *et al.* [140] and Das *et al.* [145] are 3040, 3488, 3552 and 3296, respectively (as shown in Table 10. The protocols of Braeken Luo *et al.* [141] and Das *et al.* [145] performed better from the communication cost point of view.

D. EXISTING INTRUSION DETECTION PROTOCOLS IN IoT ENVIRONMENT

The details of different intrusion detection protocols in IoT environment are provided. Wazid *et al.* [61] designed a intrusion detection mechanism for detecting and preventing

sinkhole attacker nodes in a cluster based wireless sensor network. The operations were conducted in two phases, in first phase it discovered the existence of mischievous nodes through various network performance parameters. If a node came under suspicious category then the steps of second phase confirmed the node as the sinkhole attacker node along with its types i.e., ''sinkhole message modification node'', ''sinkhole message dropping node'' and ''sinkhole message delay node''. Selvakumar *et al.* [146] presented a intrusion detection protocol on the basis of temporal reasoning method. It had utilized ''multi-class classification'' through self designed mechanism called as ''fuzzy and rough set based nearest neighborhood algorithm (FRNN)''. Wazid *et al.* [60], [62] presented a intrusion detection method for detecting blackhole attacker nodes and for ''hybrid anomaly'' in a cluster based wireless sensor network. They detected attacker nodes by the help of resource rich cluster head nodes. These proposed protocols are also applicable for the detection of intrusions in IoT environment. Jan *et al.* [147] designed a light weight intrusion detection technique for the mitigation of common type DOS attacks in IoT. From the packet transmission rate, two-three features were extracted which they were utilized for the reduction of the overall time required to classify the various flows of traffic. There were reduction in the complexity and time required by ''support vector machine (SVM)'' for the classification which results in an efficient mitigation DOS attack. Sharma *et al.* [148] designed a light weight detection technique based on behaviour rule specification for ''IoT-embedded cyber-physical systems''. The existence of intruder was detected via misbehaviour feature of an existing node. In the designed mechanism they utilized a ''profiler'' which read the module and forward this data to fuzzy analysis segment to verify the validity of behavior rules. Pajouh *et al.* [149] presented a intrusion detection mechanism for different attacks happened in IoT environment. The presented protocols used two mechanism for the reduction of dimensions and for minimizing the number of features required. The classification algorithm for example, ''KNN'' and ''naive Bayes'' were used for the detection of malign nodes. Mudgerikar *et al.* [150] presented a client system based intrusion detection protocol which utilized anomalies based detection method. It was deployed with three layers of security. But some drawbacks were there as with the increasing level of security the increment in the overhead occurred i.e., computation and communication costs. In the first component of the detection module a white list was prepared during the learning process. It separated the legitimate processes from the malicious processes. The comparisons was done on the basis of IDs of the processes. In the second module classifier was trained using the generated logs obtained through learning phase. However, it was very expensive procedure because of the use of machine learning algorithms in the resource constrained devices. Saeed *et al.* [151] presented a intrusion detection technique consisted of two phases to maintain the security in the system. The neural network was utilized in the first phase for the anomaly detection purpose. Though in the second phase a tag system was deployed for the anomaly detection. Then the anomaly detection was conducted through tag-checking method. Wazid *et al.* [73] designed an intrusion detection method to mitigate routing attacks in an edge-based IoT environment. In this technique they have used a resource rich edge node for the detection of intrusion in the network.

1) COMPARATIVE STUDY OF EXISTING INTRUSION DETECTION PROTOCOLS IN IoT ENVIRONMENT

The achievements of different intrusion detection method in IoT environment are compared. For the performance analysis purpose, there are certain parameters which need to be compared are explained as follows. The first parameter is ''detection rate (*DR*)'' (which is also called as ''true positive rate (*TPR*) or sensitivity or hit rate'') and the second one is ''false positive rate or fall out (*FPR*)''. *DR* can be formulated as ''the number of attackers detected by a intrusion detection scheme divided by the total number of attackers present in the test sample'' which is formulated as [60], [62],

$$DR = \frac{TP}{TP + FN},$$

However, *FPR* is estimated as ''the number of nodes falsely detected as attacker nodes'' which is computed as [60], [62],

$$FPR = \frac{FP}{TN + FP}.$$

The results of various intrusion detection protocols in IoT environment such as Wazid *et al.* [61], Wazid *et al.* [73], Selvakumar *et al.* [146], Wazid *et al.* [60], Jan *et al.* [147], Sharma *et al.* [148], Pajouh *et al.* [149], Mudgerikar *et al.* [150] and Saeed *et al.* [151] are provided.

The comparison of results are provided in Table 12. In the analysis following things were observed:

- The ''detection rate (DR)'' for various methods such as Wazid *et al.* [61], Wazid *et al.* [62], Wazid *et al.* [73], Selvakumar *et al.* [146], Wazid *et al.* [60], Jan *et al.* [147], Sharma *et al.* [148], Pajouh *et al.* [149], Mudgerikar *et al.* [150] and Saeed *et al.* [151] are 95.00, 98.60, 95.00, 99.87, 90.00, 97.98, 97.80, 84.86, 99.00 and 97.23 respectively.
- The ''false positive rate (FPR)'' for various methods such as Wazid *et al.* [61], Wazid *et al.* [62], Wazid *et al.* [73], Selvakumar *et al.* [146], Wazid *et al.* [60], Jan *et al.* [147], Sharma *et al.* [148], Pajouh *et al.* [149] and Saeed *et al.* [151] are 1.25, 1.20, 1.23, 0.13, 3.75, 44.48, 4.00, 4.86 and 3.48 respectively.

Computational power requirements for the methods of Wazid *et al.* [61], Wazid *et al.* [62], Wazid *et al.* [73], Wazid *et al.* [60], Selvakumar *et al.* [146], Jan *et al.* [147], Pajouh *et al.* [149], Mudgerikar *et al.* [150], Saeed *et al.* [151] and Sharma *et al.* [148] are $O(n^2)$, $O(n^2)$, $O(n^2)$, $O(n)$, $O(n)$, $O(n^3)$, $O(n)$, $O(nlog(n))$, $O(n^3)$ and $O(nlog(n))$ where n are the number nodes deployed in the target area.

TABLE 12. Accuracy comparison of existing IDS in WSN and IoT.

Scheme, Year	Detection rate (DR) %	False positive rate (FPR) %
Wazid *et al.* [61], (2016)	95.00	1.25
Wazid *et al.* [62], (2016)	98.60	1.20
Wazid *et al.* [73], (2019)	95.00	1.23
Selvakumar *et al.* [146], (2019)	99.87	0.13
Wazid *et al.* [60], (2017)	90.00	3.75
Jan *et al.* [147], (2019)	97.98	44.48
Sharma *et al.* [148], (2019)	97.80	4.00
Pajouh *et al.* [149], (2019)	84.86	4.86
Mudgerikar *et al.* [150], (2019)	99.00	N/A
Saeed *et al.* [151], (2016)	97.23	3.48

Note: N/A: not available

Apart from that it is important to notice that the scheme of Wazid *et al.* [61], Wazid *et al.* [73], Selvakumar *et al.* [146], Wazid *et al.* [60], Pajouh *et al.* [149], Mudgerikar *et al.* [150] and Saeed *et al.* [151] could be applied to achieve secuirty in WSN as well as IoT networks. However, certain amendments are required in their network model and nodes settings to achieve that objective. Methods of Wazid *et al.* [62], Selvakumar *et al.* [146] and Mudgerikar *et al.* [150] performed better with regard to true (detection) positive rate and false positive rate.

VI. FUTURE RESEARCH CHALLENGES

5G-enabled IoT communications environment supports various types of applications, such as smart home, smart transportation, smart healthcare, smart grid and smart manufacturing. This environment requires solitary requirements for example, live processing and accessing of data (i.e., environmental monitoring of an industrial plant in real-time). Such environment generates very huge data (i.e., big data) hence big data analytic process should be used on this data to identify some specific patterns from this (e.g., possibilities of an accident in a coal mine). In this environment all the devices and users communicate through the Internet. Hence it undergoes with some traditional security, privacy, and other kind of challenges. In this part of the paper some of the current challenges of this domain are discussed and further some directions for research work are highlighted.

A. SECURITY OF THE EXISTING PROTOCOLS

Most of the security protocols proposed for IoT environment insecure as they do not furnish the complete security against the possible attacks. Furthermore, some of the existing protocols works for a particular attack and do not work for multiple attacks concurrently. Hence, it is mandatory to design some security protocols which should concurrently protect multiple attacks. Therefore, designing of such kind of protocols for this domain is a challenging task which should be solved by the future researchers [27].

B. EFFICIENT DESIGN OF SECURITY PROTOCOLS

5G-enabled IoT environment contains the resource constrained devices i.e., IoT sensors which have limited computation capability, limited storage size and small battery unit. These devices are not able to execute communication, computation and storage demanding tasks which require more strength in terms of these parameters. Hence it is desirable to design security protocols to such a degree that they should need low computation power, low communication cost and small storage size without negotiating the security of the system [27], [60], [61].

C. SCALABILITY OF SECURITY PROTOCOLS

5G-enabled IoT environment is a combination of heterogeneous network of different communication mechanism and applications. These applications have their own abilities and concerns. In such situations designing of a security protocol for this kind of communication environment will be complex task. For example, in an smart healthcare communication environment, patient's electronic health records which need to be stored over a cloud server for further processing and decision making. In an body area network (BANs), there are different types of devices which generate data and then forward it to the cloud server. This constitutes a ''heterogeneous network'' of different types of communicating devices. Accordingly, some special types of security protocols which can be employed to protect various types of devices of 5G-enabled IoT environment should be designed. Therefore, more research work is needed in this area.

D. PRIVACY OF STORED DATA

The privacy of data concerns with the proper handling of information over the various resource i.e., consent, notice, and regulatory obligations. 5G-enabled IoT environment is also utilized in ''information sensitive'' operations (like smart healthcare). In this privacy-demanding environment, the health monitoring smart devices are used around/inside the body of a patient to monitor his/her health conditions. Then the sensed and collected health data is sent to cloud server(s) for further storage and processing. Usually, this type of communication environment can be affected by different potential attackers [23], [60], [62]. This may cause the leakage of data at transit and the data maintained over the servers. Consequently, it is important to sustain the privacy of the data at transit and also to the stored data. Hence new efficient protocols are much needed to maintain the privacy of data. Thenceforth, more research work is required in this direction.

E. HETEROGENEITY OF USED DEVICES

5G-enabled IoT environment consists of various types of devices from powerful servers, laptops, personal digital

assistants, desktops to resource restricted RFID tags and sensing devices. Besides that, these devices work with various types of communication techniques. Devices are also contrasting as per their communication strength, computation capacity, storage size and deployed system software (e.g., operating system). Hence security protocols should be designed in such fashion that it provides protection to different varieties of devices and associated technologies and mechanisms. Thenceforth, more research work is required in this area [27], [60].

F. BLOCKCHAIN BASED SECURITY PROTOCOLS DESIGNING

The operations of blockchain can also be utilized to secure the 5G-enabled IoT environment. Because blockchain operations are decentralized, efficient and transparent to all entities of the communication environment. To devise security protocols in 5G-enabled IoT environment ''blockchain operations'' are also applicable. To perform the required task a block consists of the data about the required functionality e.g., authentication message, data message can be created and added it to the blockchain. In view of that blockchain is provided to legal network entities, then these entities can access the data using the blocks of the blockchain. That work can be accomplished in an effective way using the operation of blockchain. Accordingly, designing of ''blockchain based security protocols'' seems to be a good problem for the future researchers [152], [153].

VII. LESSONS LEARNED

5G-enabled IoT environment provides delay efficient services. It has wide variety of applications, such as healthcare, home automation, remote surgery, autonomous vehicle (AV), virtual reality (VR), flying IoT drones, and security and surveillance. This communication environment facilities day-to-day activities of the people. However, it also agonizes from various ''security and privacy'' issues. To cope this, researchers working in this area proposed various types of security protocols under different categories, such as ''key management protocols'', ''authentication/ user authentication protocols'', ''access control/user access control protocols'' and ''intrusion detection''. The intrusion detection protocols are of three types like ''misuse based detection'', ''anomaly based detection'' and ''specification based detection''. ''Specification based detection'' scheme needs certain constraints and specifications for its deployment. It uses the advantages of the other two schemes. Its false positive rate is also less as compared to the other detection schemes. Inspite of that, it is bit inconvenient as it is time consuming, we need some time in the defining and construction of the required set. It detects ''zero-day attacks'' effectively. In this detection scheme the intrusion detection happens efficiently and effectively with less number of ''false negatives'' and ''false positives'' rates.

The key management protocols of Li *et al.* [120], Li *et al.* [121], Hu *et al.* [122], Mishra *et al.* [123], Sharif *et al.* [124] and Wazid *et al.* [56] were compared and analysed. The protocols of Li *et al.* [120], Li *et al.* [121], Hu *et al.* [122] did not support most of the desired funtionalties and security lineaments, whereas the schemes of Mishra *et al.* [123], Sharif *et al.* [124] did not provide the support for environment of multiple servers. Inspite of that the scheme of Wazid *et al.* [56] supported most of the functionalities and security lineaments.

The user authentication protocols of Challa *et al.* [11] and Wazid *et al.* [138] provided most of functionalities and security lineaments. But, the scheme of Challa *et al.* [11] produced little more computational and communication overheads. Hence, from the functionalities, secuirty lineaments and computation & communication costs point of view, the scheme of Wazid *et al.* [138] seems finer than Challa *et al.*'s method [11].

The access control mechanisms of Luo *et al.* [141], Li *et al.* [139], and Braeken *et al.* [140] did not provide the required functionalities and security lineaments, whereas the method of Das *et al.* [145] provided most of the desired functionalities and security lineaments along with less computation and communications costs.

The intrusion detection mechanisms of Wazid *et al.* [62], Selvakumar *et al.* [146] and Mudgerikar *et al.* [150] performed better with regard to false positive rate and true positive (detection) rate.

There are some future research directions of ''security in 5G-enabled IoT environment'' such as ''security of the existing protocols'', ''efficient design of security protocols'', ''scalability of security protocols'', ''privacy of stored data'', ''heterogeneous nature of devices'' and ''use of blockchain in the designing of security protocols''. These topics should be addressed in near future.

VIII. CONCLUSION

5G-enabled IoT environment suffers from various types of ''security and privacy'' issues as it is susceptible to various types of attacks. It becomes essential to protect the infrastructure of 5G-enabled IoT environment against these attacks. Therefore, different types of security protocols under different categories (for example, ''key management'', ''user authentication/device authentication'', ''access control/user access control'' and ''intrusion detection'') came into picture. In this survey article, the details of various system models (for example, network model and threat model) are provided for 5G-enabled IoT environment. Various security requirements and attacks possible in this communication environment are also outlined. The different types of categories of security protocols are then prepared. The different types of analysis of the existing security protocols in 5G-enabled IoT environment are also organized. Lastly, some challenging problem of future in the security of 5G-enabled IoT environment are displayed to help the researchers working in the same domain.

ACKNOWLEDGMENT

The authors thank the anonymous reviewers and the associate editor for their valuable feedback on the paper which helped them to improve its quality and presentation.

REFERENCES

[1] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020, doi: 10.1109/COMST.2019.2933899.

[2] A. Ahad, M. Tahir, and K.-L.-A. Yau, "5G-based smart healthcare network: Architecture, taxonomy, challenges and future research directions," *IEEE Access*, vol. 7, pp. 100747–100762, 2019.

[3] A. Braeken, M. Liyanage, P. Kumar, and J. Murphy, "Novel 5G authentication protocol to improve the resistance against active attacks and malicious serving networks," *IEEE Access*, vol. 7, pp. 64040–64052, 2019.

[4] Ericsson. (2019). *What is 5G?* Accessed: Oct. 2019. [Online]. Available: https://www.ericsson.com/en/5g

[5] Qualcomm. (2019). *Everything You Need to Know About 5G*. Accessed: Oct. 2019. [Online]. Available: https://www.qualcomm.com/invention/5g

[6] Northeast Now. *China: Shanghai's Hongkou District Becomes First With 5G Network in World*. Accessed: Dec. 2019. [Online]. Available: https://nenow.in/neighbour/china-shanghais-hongkou-district-becomes-first-with-5g-network-in-world.html

[7] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Commun. Standards Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018.

[8] P. Gandotra and R. K. Jha, "A survey on green communication and security challenges in 5G wireless communication networks," *J. Netw. Comput. Appl.*, vol. 96, pp. 39–61, Oct. 2017.

[9] Z. Tian, Y. Sun, S. Su, M. Li, X. Du, and M. Guizani, "Automated attack and defense framework for 5G security on physical and logical layers," 2019, *arXiv:1902.04009*. [Online]. Available: http://arxiv.org/abs/1902.04009

[10] H. Lee. (2015). *Concept and Characteristics of 5G Mobile Communication Systems*. Accessed: Oct. 2019. [Online]. Available: https://www.netmanias.com/en/post/blog/7109/5g-iot/concept-and-characteristics-of-5g-mobile- communication-systems-1

[11] 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.

[12] 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.

[13] 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 Informat.*, vol. 22, no. 4, pp. 1299–1309, Jul. 2018.

[14] 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. Dependable Secure Comput.*, vol. 17, no. 2, pp. 391–406, Mar. 2020.

[15] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[16] S. Bera, S. Misra, and A. V. Vasilakos, "Software-defined networking for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1994–2008, Dec. 2017.

[17] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.

[18] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, Jun. 2015.

[19] RedAlkemi. (2018). *Pros & Cons of Internet of Things*. Accessed: Oct. 2019. [Online]. Available: https://www.redalkemi.com/blog/post/pros-cons-of-internet-of-things

[20] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for Internet of Things: A comprehensive survey," *Secur. Commun. Netw.*, vol. 2017, pp. 1–42, Nov. 2017, doi: 10.1155/2017/6562953.

[21] 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.

[22] 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.

[23] M. Wazid, A. K. Das, and A. V. Vasilakos, "Authenticated key management protocol for cloud-assisted body area sensor networks," *J. Netw. Comput. Appl.*, vol. 123, pp. 112–126, Dec. 2018.

[24] 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.

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

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

[27] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: Survey and outlook," *J. Syst. Archit.*, vol. 97, pp. 185–196, Aug. 2019.

[28] P. D. Baruah, S. Dhir, and M. Hooda, "Impact of IoT in current era," in *Proc. Int. Conf. Mach. Learn., Big Data, Cloud Parallel Comput. (COMITCon)*, Feb. 2019, pp. 334–339.

[29] G. Kobayashi, "The ethical impact of the Internet of Things in social relationships: Technological mediation and mutual trust," *IEEE Consum. Electron. Mag.*, vol. 5, no. 3, pp. 85–89, Jul. 2016.

[30] D. Niyato, X. Lu, P. Wang, D. I. Kim, and Z. Han, "Economics of Internet of Things: An information market approach," *IEEE Wireless Commun.*, vol. 23, no. 4, pp. 136–145, Aug. 2016.

[31] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[32] 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.

[33] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1606–1616, Apr. 2019.

[34] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2019.

[35] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102481.

[36] Devices & Systems, IoT Tech Expo. (2019). *Unlocking IoT Data With 5G and AI*. Accessed: Oct. 2019. [Online]. Available: https://innovate.ieee.org/innovation-spotlight/5g-iot-ai/

[37] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. 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.

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

[39] King's Healthcare. (2019). *A Healing Hand-Giving the World Better Access to Medical Experts Through the Tactile Internet*. Accessed: Oct. 2019. [Online]. Available: https://www.ericsson.com/en/cases/2017/kings-college/kings-healthcare

[40] 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," *Pervas. Mobile Comput.*, vol. 54, pp. 71–85, Mar. 2019.

[41] R. Hussain and S. Zeadally, "Autonomous cars: Research results, issues, and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1275–1313, 2nd Quart., 2019.

[42] M. A. Imran, Y. A. Sambo, and Q. H. Abbasi, "Evolution of vehicular communications within the context of 5G systems," in *Enabling 5G Communication Systems to Support Vertical Industries*. Piscataway, NJ, USA: IEEE, 2019, pp. 103–126, doi: 10.1002/9781119515579.ch5.

[43] K. Jo and M. Sunwoo, "Generation of a precise roadway map for autonomous cars," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 3, pp. 925–937, Jun. 2014.

[44] MWC. *Limitless Intelligent Connectivity*. Accessed: Oct. 2019. [Online]. Available: https://www.mwcbarcelona.com/

[45] M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. De Silva, F. Tufvesson, A. Benjebbour, and G. Wunder, "5G: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1201–1221, Jun. 2017.

[46] F. Alvarez, D. Breitgand, D. Griffin, P. Andriani, S. Rizou, N. Zioulis, F. Moscatelli, J. Serrano, M. Keltsch, P. Trakadas, T. K. Phan, A. Weit, U. Acar, O. Prieto, F. Iadanza, G. Carrozzo, H. Koumaras, D. Zarpalas, and D. Jimenez, "An edge-to-cloud virtualized multimedia service platform for 5G networks," *IEEE Trans. Broadcast.*, vol. 65, no. 2, pp. 369–380, Jun. 2019.

[47] M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of drones," *IEEE Access*, vol. 4, pp. 1148–1162, 2016.

[48] 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.

[49] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV-based IoT platform: A crowd surveillance use case," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 128–134, Feb. 2017.

[50] M. Alam, J. Ferreira, S. Mumtaz, M. A. Jan, R. Rebelo, and J. A. Fonseca, "Smart cameras are making our beaches safer: A 5G-envisioned distributed architecture for safe, connected coastal areas," *IEEE Veh. Technol. Mag.*, vol. 12, no. 4, pp. 50–59, Dec. 2017.

[51] S. A. R. Naqvi, S. A. Hassan, H. Pervaiz, and Q. Ni, "Drone-aided communication as a key enabler for 5G and resilient public safety networks," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 36–42, Jan. 2018.

[52] M. Condoluci and T. Mahmoodi, "Softwarization and virtualization in 5G mobile networks: Benefits, trends and challenges," *Comput. Netw.*, vol. 146, pp. 65–84, Dec. 2018.

[53] M. A. Imran, Y. A. Sambo, and Q. H. Abbasi, "5G communication systems and connected healthcare," in *Enabling 5G Communication Systems to Support Vertical Industries*. Piscataway, NJ, USA: IEEE, 2019, pp. 149–177, doi: 10.1002/9781119515579.ch7.

[54] 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.

[55] 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.

[56] 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.

[57] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[58] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Advances in Cryptology*, L. R. Knudsen, Ed. Amsterdam, The Netherlands: Springer, 2002, pp. 337–351.

[59] 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.

[60] 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.

[61] 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, Nov. 2016.

[62] 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.

[63] S. Sahmim and H. Gharsellaoui, "Privacy and security in Internet-based computing: Cloud computing, Internet of Things, cloud of things: A review," *Procedia Comput. Sci.*, vol. 112, pp. 1516–1522, Jan. 2017.

[64] A. Assiri and H. Almagwashi, "IoT security and privacy issues," in *Proc. 1st Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, Riyadh, Saudi Arabia, Apr. 2018, pp. 1–5.

[65] J. Hou, L. Qu, and W. Shi, "A survey on Internet of Things security from data perspectives," *Comput. Netw.*, vol. 148, pp. 295–306, Jan. 2019.

[66] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[67] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1646–1685, 3rd Quart., 2020.

[68] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2010.

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

[70] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, "Toward a lightweight intrusion detection system for the Internet of Things," *IEEE Access*, vol. 7, pp. 42450–42471, 2019.

[71] H. Chen, C. Meng, Z. Shan, Z. Fu, and B. K. Bhargava, "A novel low-rate denial of service attack detection approach in ZigBee wireless sensor network by combining Hilbert–Huang transformation and trust evaluation," *IEEE Access*, vol. 7, pp. 32853–32866, 2019.

[72] Kamaldeep, M. Malik, and M. Dutta, "Contiki-based mitigation of UDP flooding attacks in the Internet of Things," in *Proc. Int. Conf. Comput., Commun. Automat. (ICCCA)*, Greater Noida, India, May 2017, pp. 1296–1300, doi: 10.1109/CCAA.2017.8229997.

[73] 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.

[74] *How to Avoid the Dreaded Computer Virus*. Accessed: Oct. 2019. [Online]. Available: http://www.magellansolutions.co.uk/malware.html

[75] M. Korolov. (2019). *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

[76] 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.

[77] 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, doi: 10.1109/MILCOM.2017.8170867.

[78] H. Sinanovic and S. Mrdovic, "Analysis of mirai malicious software," in *Proc. 25th Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM)*, Split, Croatia, Sep. 2017, pp. 1–5, doi: 10.23919/SOFTCOM.2017.8115504.

[79] 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, Nov. 2017, pp. 1–4, doi: 10.1109/TELFOR.2017.8249458.

[80] A. Kumar and T. J. Lim, "EDIMA: Early detection of IoT malware network activity using machine learning techniques," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, Limerick, Ireland, Apr. 2019, pp. 289–294, doi: 10.1109/WF-IoT.2019.8767194.

[81] 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, Jun. 2018, pp. 1–6, doi: 10.1109/ISSC.2018.8585344.

[82] 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.

[83] H.-T. Nguyen, Q.-D. Ngo, and V.-H. 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, doi: 10.1109/ICICSP.2018.8549713.

[84] 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, Automat. Test Eur. Conf. Exhib. (DATE)*, Florence, Italy, Mar. 2019, pp. 776–781, doi: 10.23919/DATE.2019.8715057.

[85] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "IoMT malware detection approaches: Analysis and research challenges," *IEEE Access*, vol. 7, pp. 182459–182476, 2019.

[86] 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.

[87] 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.

[88] 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, 2013.

[89] 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.

[90] 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.

[91] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. 19th Int. Conf. Data Eng.*, Berkeley, CA, USA, 2003, pp. 197–213.

[92] 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)*, Hong Kong, vol. 1, Mar. 2004, pp. 586–597.

[93] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in *Proc. 10th ACM Conf. Comput. Commun. Secur. (CCS)*, Washington, DC, USA, Oct. 2003, pp. 42–51.

[94] 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* (Lecture Notes in Computer Science), vol. 740. Berlin, Germany: Springer, Aug. 1993, pp. 471–486.

[95] 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. 7.

[96] 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, pp. 1–14.

[97] 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.

[98] 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.

[99] 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.

[100] 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, Feb. 2005.

[101] 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.

[102] 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.

[103] 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.

[104] 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.

[105] 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.

[106] L. Wu, J. Wang, K.-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.

[107] 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.

[108] 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.

[109] 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, Nov. 2016.

[110] 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.

[111] 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.

[112] 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.

[113] J. Su, V. D. 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.

[114] 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.

[115] 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.*, vol. 19, no. 1, pp. 71–81, Feb. 2020, doi: 10.1007/s10207-019-00437-y.

[116] 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. 2019.

[117] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges," *IEEE Access*, vol. 8, pp. 3343–3363, 2020.

[118] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," *J. High Speed Netw.*, vol. 15, no. 1, pp. 33–51, 2006.

[119] 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.

[120] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in *Cloud Computing*. Berlin, Germany: Springer, 2009, pp. 157–166.

[121] H. Li, F. Li, C. Song, and Y. Yan, "Towards smart card based mutual authentication schemes in cloud computing," *KSII Trans. Internet Inf. Syst.*, vol. 9, no. 7, pp. 2719–2735, 2015.

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

[123] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S. H. Islam, and P. Gope, "Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks," *Multimedia Tools Appl.*, vol. 77, no. 14, pp. 18295–18325, Jul. 2018.

[124] A. Ostad-Sharif, H. Arshad, M. Nikooghadam, and D. Abbasinezhad-Mood, "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme," *Future Gener. Comput. Syst.*, vol. 100, pp. 882–892, Nov. 2019.

[125] AVISPA. (2019). *Automated Validation of Internet Security Protocols and Applications*. Accessed: Oct. 2019. [Online]. Available: http://www.avispa-project.org/

[126] M. Abdalla, P. A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. 8th Int. Workshop Theory Pract. Public Key Cryptography (PKC)*, in Lecture Notes in Computer Science, Les Diablerets, Switzerland, vol. 3386, 2005, pp. 65–84.

[127] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 3027. Berlin, Germany: Springer, 2004, pp. 523–540.

[128] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Comput. Commun.*, vol. 31, no. 12, pp. 2803–2814, Jul. 2008.
[129] W. Li, Q. Wen, Q. Su, and Z. Jin, "An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network," *Comput. Commun.*, vol. 35, no. 2, pp. 188–195, Jan. 2012.
[130] D. He, N. Kumar, J.-H. Lee, and R. S. Sherratt, "Enhanced three-factor security protocol for consumer USB mass storage devices," *IEEE Trans. Consum. Electron.*, vol. 60, no. 1, pp. 30–37, Feb. 2014.
[131] R. L. Rivest, M. E. Hellman, J. C. Anderson, and J. W. Lyons, "Responses to NIST's proposal," *Commun. ACM*, vol. 35, no. 7, pp. 41–54, Jul. 1992.
[132] *Secure Hash Standard*, Standard FIPS PUB 180-1, National Institute of Standards and Technology, U.S. Department of Commerce, Apr. 1995. Accessed: Jan. 2019. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
[133] *Advanced Encryption Standard (AES)*, Standard FIPS PUB 197, National Institute of Standards and Technology, U.S. Department of Commerce, Nov. 2001. Accessed: Dec. 2019. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[134] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Istanbul, Turkey, Apr. 2014, pp. 2728–2733.
[135] P. Porambage, A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila, and B. Stiller, "Group key establishment for enabling secure multicast communication in wireless sensor networks deployed for IoT applications," *IEEE Access*, vol. 3, pp. 1503–1511, 2015.
[136] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Netw.*, vol. 20, pp. 96–112, Sep. 2014.
[137] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Netw.*, vol. 36, pp. 152–176, Jan. 2016.
[138] M. Wazid, A. K. Das, V. Bhat K, and A. V. Vasilakos, "LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment," *J. Netw. Comput. Appl.*, vol. 150, Jan. 2020, Art. no. 102496, doi: 10.1016/j.jnca.2019.102496.
[139] F. Li, Y. Han, and C. Jin, "Practical access control for sensor networks in the context of the Internet of Things," *Comput. Commun.*, vols. 89–90, pp. 154–164, Sep. 2016.
[140] A. Braeken, P. Porambage, M. Stojmenovic, and L. Lambrinos, "eDAAAS: Efficient distributed anonymous authentication and access in smart homes," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 12, pp. 1–11, Dec. 2016.
[141] M. Luo, Y. Luo, Y. Wan, and Z. Wang, "Secure and efficient access control scheme for wireless sensor networks in the cross-domain context of the IoT," *Secur. Commun. Netw.*, vol. 2018, pp. 1–10, Feb. 2018, doi: 10.1155/2018/6140978.
[142] 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.
[143] 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.
[144] K. Fan, H. Xu, L. Gao, H. Li, and Y. Yang, "Efficient and privacy preserving access control scheme for fog-enabled IoT," *Future Gener. Comput. Syst.*, vol. 99, pp. 134–142, Oct. 2019.
[145] 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.
[146] K. Selvakumar, M. Karuppiah, L. SaiRamesh, S. H. Islam, M. M. Hassan, G. Fortino, and K.-K.-R. Choo, "Intelligent temporal classification and fuzzy rough set-based feature selection algorithm for intrusion detection system in WSNs," *Inf. Sci.*, vol. 497, pp. 77–90, Sep. 2019.
[147] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, "Toward a lightweight intrusion detection system for the Internet of Things," *IEEE Access*, vol. 7, pp. 42450–42471, 2019.
[148] V. Sharma, I. You, K. Yim, I.-R. Chen, and J.-H. Cho, "BRIoT: Behavior rule specification-based misbehavior detection for IoT-embedded cyber-physical systems," *IEEE Access*, vol. 7, pp. 118556–118580, 2019.
[149] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K.-K.-R. Choo, "A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks," *IEEE Trans. Emerg. Topics Comput.*, vol. 7, no. 2, pp. 314–323, Apr. 2019.
[150] A. Mudgerikar, P. Sharma, and E. Bertino, "E-spion: A system-level intrusion detection system for IoT devices," in *Proc. ACM Asia Conf. Comput. Commun. Secur. (Asia CCS)*, Auckland, New Zealand, 2019, pp. 493–500.
[151] A. Saeed, A. Ahmadinia, A. Javed, and H. Larikani, "Intelligent intrusion detection in low-power IoTs," *ACM Trans. Internet Technol.*, vol. 16, no. 4, pp. 27:1–27:25, 2016.
[152] 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.
[153] B. Wu, K. Xu, Q. Li, Z. Liu, Y.-C. Hu, Z. Zhang, X. Du, B. Liu, and S. Ren, "SmartCrowd: Decentralized and automated incentives for distributed IoT system detection," in *Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Dallas, TX, USA, Jul. 2019, pp. 1106–1116.

MOHAMMAD WAZID (Senior Member, IEEE) received the M.Tech. degree in computer network engineering from Graphic Era deemed to be University, Dehradun, India, and the Ph.D. degree in computer science and engineering from the International Institute of Information Technology, Hyderabad, India. He was working as an Assistant Professor with the Department of Computer Science and Engineering, Manipal Institute of Technology, MAHE, Manipal, India. He was a Post-Doctoral Researcher with the Cyber Security and Networks Laboratory, Innopolis University, Innopolis, Russia. He is currently working as an Associate Professor with the Department of Computer Science and Engineering, Graphic Era deemed to be University. He is also the Head of the Cyber Security and IoT Research Group, Graphic Era deemed to be University. His current research interests include information security, remote user authentication, the Internet of Things (IoT), cloud/fog/edge computing, and blockchain. He has published more than 80 papers in international journals and conferences in the above areas. Some of his research findings are published in top cited journals, such as the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON SMART GRID, IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS (formerly IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE), *IEEE Consumer Electronics Magazine*, IEEE ACCESS, *Future Generation Computer Systems* (Elsevier), *Computers & Electrical Engineering* (Elsevier), *Computer Methods and Programs in Biomedicine* (Elsevier), *Security and Communication Networks* (Wiley), and *Journal of Network and Computer Applications* (Elsevier). He has served as a Program Committee Member in many international conferences. 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 received the Dr. A. P. J. Abdul Kalam Award for his innovative research works and the *ICT Express* (Elsevier) Journal "Best Reviewer" Award, in 2019.

Ashok Kumar Das (Senior Member, IEEE) received the M.Tech. degree in computer science and data processing, the M.Sc. degree in mathematics, and the Ph.D. degree in computer science and engineering 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 research interests include cryptography, network security, blockchain, security in Internet of Things (IoT), Internet of Vehicles (IoV), Internet of Drones (IoD), smart grids, smart city, cloud/fog computing and industrial wireless sensor networks, intrusion detection, blockchain, and AI/ML security. He has authored over 245 papers in international journals and conferences in the above areas, including over 210 reputed journal papers. Some of his research findings are published in top cited journals, such as the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON SMART GRID, IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS (formerly IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE), *IEEE Consumer Electronics Magazine*, IEEE ACCESS, *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 *Journal of Network and Computer Applications*. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He serves on the Editorial Board of IEEE SYSTEMS JOURNAL, *Journal of Network and Computer Applications* (Elsevier), *Computer Communications* (Elsevier), *IET Communications*, *KSII Transactions on Internet and Information Systems*, and *International Journal of Internet Technology and Secured Transactions* (Inderscience). He is a Guest Editor of *Computers & Electrical Engineering* (Elsevier) for the Special Issue on Big Data and IoT in e-Healthcare, *ICT Express* (Elsevier) for the Special Issue on Blockchain Technologies and Applications for 5G Enabled IoT, and *Wireless Communications and Mobile Computing* for the Special Issue on Security and Privacy for Smart Mobile Devices: Attacks, Challenges, and New Designs. He has served as a Program Committee Member in many international conferences. He served as one of the Technical Program Committee Chairs of the first International Congress on Blockchain and Applications (BLOCKCHAIN 2019), Ávila, Spain, in June 2019, the International Conference on Applied Soft Computing and Communication Networks (ACN 2020), Chennai, India, in October 2020, and the second International Congress on Blockchain and Applications (BLOCKCHAIN 2020), L'Aquila, Italy, in October 2020.

SACHIN SHETTY (Senior Member, IEEE) 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 ACM CCS, IEEE INFOCOM, IEEE ICDCN, and IEEE ICCCN.

PROSANTA GOPE (Member, IEEE) received the Ph.D. degree in computer science and information engineering from National Cheng Kung University (NCKU), Tainan, Taiwan, in 2015. He was a Research Fellow with the Department of Computer Science, National University of Singapore (NUS). He is currently working as a Lecturer with the Department of Computer Science, University of Sheffield, Sheffield, U.K. His research interests include lightweight authentication, authenticated encryption, access control systems, security in mobile communication and cloud computing, lightweight security solutions for smart grid, and hardware security of the Internet of Things (IoT) devices. He has authored over 50 peer-reviewed articles in several reputable international journals and conferences and has four filed patents. He received the Distinguished Ph.D. Scholar Award from National Cheng Kung University, Tainan, Taiwan, in 2014. He also serves as an Associate Editor for the IEEE SENSORS JOURNAL and *Security and Communication Networks*.

JOEL J. P. C. RODRIGUES (Fellow, IEEE) is currently a Professor with the Federal University of Piauí, Brazil and a Senior Researcher with the Instituto de Telecomunicações, Portugal. He is a collaborator of the Post-Graduation Program on Teleinformatics Engineering at the Federal University of Ceará (UFC), Brazil. He is also the Leader of the Next Generation Networks and Applications (NetGNA) research group (CNPq). He has authored or coauthored over 950 papers in refereed international journals and conferences, three books, two patents, and one ITU-T Recommendation. He is a member of the Internet Society and a Senior Member of ACM. He received several outstanding leadership and outstanding service awards from the IEEE Communications Society and several best papers awards. He is an IEEE Distinguished Lecturer, a Member Representative of the IEEE Communications Society on the IEEE Biometrics Council, and the President of the scientific council at ParkUrbis–Covilhã Science and Technology Park. He was Director of the Conference Development—IEEE ComSoc Board of Governors, the Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, the past Chair of the IEEE ComSoc Technical Committee on eHealth and the IEEE ComSoc Technical Committee on Communications Software, a Steering Committee Member of the IEEE Life Sciences Technical Community, and the Publications Co-Chair. He is also the Editor-in-Chief of the *International Journal of 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 IEEE ICC, IEEE GLOBECOM, IEEE HEALTHCOM, and IEEE LatinCom.