IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 13, 2019, accepted December 24, 2019, date of publication December 30, 2019, date of current version January 7, 2020.

Digital Object Identifier 10.1109/ACCESS.2019.2962829

Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges

SUMIT PUNDIR[1], MOHAMMAD WAZID[1], (Member, IEEE), DEVESH PRATAP SINGH[1], ASHOK KUMAR DAS[2], (Senior Member, IEEE), JOEL J. P. C. RODRIGUES[3,4], (Fellow, IEEE), and YOUNGHO PARK[5], (Member, IEEE)

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

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

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning (2017R1A2B1002147). This work was partially supported by National Funding from the FCT-Fundação para a Ciência e a Tecnologia through the UID/EEA/500008/2019 Project; and by Brazilian National Council for Scientific and Technological Development (CNPq) via Grant No. 309335/2017-5. This work was also supported by the Ripple Centre of Excellence Scheme, CoE in Blockchain (Sanction No. IIIT/R&D Office/Internal Projects/001/2019), IIIT Hyderabad, India.

ABSTRACT As we all know that the technology is projected to be next to humans very soon because of its holistic growth. Now-a-days, we see a lot of applications that are making our lives comfortable such as smart cars, smart homes, smart traffic management, smart offices, smart medical consultation, smart cities, etc. All such facilities are in the reach of a common man because of the advancement in Information and Communications Technology (ICT). Because of this advancement, new computing and communication environment such as Internet of Things (IoT) came into picture. Lot of research work is in progress in IoT domain which helps for the overall development of the society and makes the lives easy and comfortable. But in the resource constrained environment of Wireless Sensor Network (WSN) and IoT, it is almost inconceivable to establish a fully secure system. As we are moving forward very fast, technology is becoming more and more vulnerable to the security threats. In future, the number of Internet connected people will be less than the smart objects so we need to prepare a robust system for keeping the above mentioned environments safe and standardized it for the smooth conduction of communication among IoT objects. In this survey paper, we provide the details of threat model applicable for the security of WSN and IoT based communications. We also discuss the security requirements and various attacks possible in WSN and IoT based communication environments. The emerging projects of WSNs integrated to IoT are also briefed. We then provide the details of different architectures of WSN and IoT based communication environments. Next, we discuss the current issues and challenges related to WSN and IoT. We also provide a critical literature survey of recent intrusion detection protocols for IoT and WSN environments along with their comparative analysis. A taxonomy of security and privacy-preservation protocols in WSN and IoT is also highlighted. Finally, we discuss some research challenges which need to be addressed in the coming future.

INDEX TERMS Wireless sensor network (WSN), Internet of Things (IoT), intrusion detection, cloud computing, fog computing, edge computing, security.

I. INTRODUCTION

Wireless Sensor Network (WSN) is the assemblage of homogeneous and heterogeneous resource constrained sensing devices which sense the environment's physical phenomenon and transmit the information to the sink node (base station) via different modes of communication. The information is transferred to the base station for processing as per the requirement of the applications. It is one of the most encouraging technology for the researchers because of its

The associate editor coordinating the review of this manuscript and approving it for publication was Antonio Skarmeta Gómez.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/

effective results from the unattended geographical locations. Some of the critical applications of WSN are in real-time scenarios (for example, boarder surveillance, industrial monitoring, commercial applications, healthcare monitoring, environmental applications, national and international highways monitoring).

Contrarily, Internet of Things (IoT) is composed of different networked objects (i.e., smart devices) which are interconnected to gather, process, refine, and exchange meaningful data over the Internet. These objects are assigned to their respective IP addresses or device identities, and these are able to send and receive data over a network without any human assistance. Since IoT is getting closer to the reach of a common man and is used in our day today lives, it eases all the ways of doing our day today tasks through the smart devices and their applications, but this holistic development is raising the security concerns. All the things are getting smart in IoT paradigm and a common thing among all the devices is the power of getting connected with internet and share the sensed information results with the devices which can be controlled remotely. As IoT is a collection of heterogeneous devices which requires a common platform to communicate with each other (i.e., via a protocol). This requirement gave birth to IoT frameworks such that which architecture or IoT framework should be used for the specific application because security standards for IoT are yet to be finalized. Since the IoT concept came in to existence, many giant bondholders have designed various frameworks according to their vision, which includes "Azure IoT Suite by Microsoft, ARM Bed by ARM and partners, AWS IoT by Amazon, Calvin by Ericsson, HomeKit by Apple, Brillo by Google, and SmartThings by Samsung" [1].

WSN and IoT both are the social reformers of the society, which can transform the whole world in to a smart planet. Both have various applications, but many of the concepts of IoT networks come from the WSNs. Sometimes both terms confuse each other and have many similarities and dissimilarities. They have similarities like in both the networks most of the time the sensing devices are resource constrained having limited processing power, memory and transmission capabilities, and both of them are very powerful for the real time applications like boarder area surveillance where 24x7 hours surveillance is required. In a hazardous situation where human's intervention is not possible, the number of sensors can be deployed randomly where some of them may malfunction or stop working. Therefore, we need strong and energy efficient routing protocols which can quickly do the rearrangement of the network. Because of these complications both WSN and IoT are vulnerable to various attacks like Denial of Service (DoS), sinkhole, blackhole, greyhole, wormhole, selective forwarding, Sybil and hello flood attack, etc. However, WSN and IoT also have some dissimilarities such as in WSNs most of the time the sensing devices simply collect the sensing data and pass as it is to the sink node, whereas in IoT networks sensing devices are smarter than WSNs sensing nodes. Another difference is the use of addressing technique during the routing process, IP addressing technique is used in IoT networks, but WSN uses some different techniques to route their packets such as flat based, hierarchical based and location based routings [2]. All the commercially available IoT frameworks are AWS IoT from Amazon, ARM Bed from ARM and other partners, Azure IoT Suite from Microsoft, Brillo/Weave from Google, Calvin from Ericsson, HomeKit from Apple, Kura from Eclipse and SmartThings from Samsung are available nowadays, for the applications which are used by commercial businesses and end users [1].

WSN and IoT based applications have influenced the life of the people a lot as they can easily facilitate and support the day-to-day activities of the people. As a result, various applications related to WSN and IoT domains came up. In the following, we provide some potential applications related to WSN integrated IoT environment.

Home Automation System: IoT based technology is compatible with almost all machines. In our home appliances, IoT proposes a smart automated system. Users can control home stuff using the IoT based automation system anywhere from the world. Such kind of projects are very helpful in those countries which have more number of elderly people. As the children of these people can help their parents remotely by controlling the smart home appliances using the smartphones [3], [4].

Air Pollution Monitoring System: Air pollution is very common problem these days. Polluted air contains hazardous particles such as led, carbon monoxide, sulfur dioxide and other heavy particles which cause so much air pollution. This further degrades the quality of the air specially in metro cities. Air pollution is a root cause for some of the deadly diseases such as asthma attacks, chronic obstructive pulmonary disease (COPD), reduced lung function, pulmonary cancer, mesothelioma and Pneumonia. Therefore, it becomes important to deploy some mechanism to measure air pollution in an area. Hence, the researchers of WSN and IoT domains came up with some ideas to resolve this problem. Newly manufactured IoT devices can monitor the quality of the air and send data to servers (i.e., cloud server). Such data can be further utilized to predict certain defects related to the quality of the air. These projects are very helpful to detect the air pollution in a city. We can utilize particle matter detector, gas sensor, temperature, and humidity sensor to perform these operations [4], [5].

Smart Health Monitoring System: These days life of the people becoming so stressful and they do not take care of their health properly. Usually, they do not go for regular checkups. IoT projects for example, smart health monitoring systems can resolve this problem. It is possible that "health sensors" in the body of the patient can sense the level (reading) of blood pressure, sugar level, and heartbeat and immediately notify the doctor if it is higher than the normal value. In such scenario smart sensor based devices monitor the health of object (i.e., patient) regularly and send data to the cloud server which can be further accessed by doctor, nurse and the relatives of that patient through their smartphones. The doctor can check the current health status of the patients at any time and anywhere from the world by making the use of such kind of communication environment [4], [6]–[9].

Smart Traffic Management System: Traffic problems are there in almost all metro cities because of increasing number of vehicles in the cities. WSN and IoT based project like "smart traffic management system" can overcome this problem. "Smart traffic management system" consists of smart vehicles (inbuilt with smart sensor) which can communicate among each other. The data of these vehicles can be sent to a cloud server which can be used for further processing and prediction. Therefore a central authority can raise a alarm in case of heavy traffic in some particular streets. This will be very helpful for the drivers who are in some emergency situations (i.e., driver of a ambulance). They can change there root on the basis provided information on time. It can also monitors traffic rules violators [4], [10], [11].

Early Flood Detection and Avoidance: Flood is a very common seasonal problem. Many countries are suffered from this natural disaster. It causes loss of life and also destroys the economy of a country. Therefore, we need early flood detection to reduce the loss of life and property. Hence, researcher working in the domain of WSN and IoT came up with the idea of an early flood detection system. Such a project detects flood situation using the level of humidity, temperature, water level and flow level. Float sensor is used to monitor the level of water. The flow sensor monitors the flow of water. It consists of a water rotor, a hall-effect sensor and a plastic valve body. The flow sensor monitors the flow of water. All such monitored parameters can be accessed through a smartphone to predict the flood kind of situations [4], [12].

Smart Anti-Theft System: Security has become one of the major requirement of current society. Everyone wants to secure their home or company from any kind of physical theft. WSN and IoT based applications can resolve this problem. If a user goes out from his/ her house, they have to turn on the antitheft system which will monitor the floors and any footstep on the floor tiles will send alert to the alarming system. In case if an intruder enters the house, the deployed and activated sensor detects it as the anomaly sends the corresponding data to the the alarm system which has a microcontroller. The microcontroller then makes it a valid signal, activate the camera to take a picture and sends this theft information to the user of that house. Then the user can see that picture on his/ her smartphone [4].

Safety System for Coal Mines: There is always a life risk in caol mines. Coal mines are very dangerous places where a worker can easily lost his/ her life. Therefore, researchers working in the domain of WSN and IoT discovered the idea of "Safety System for coal mines". For the implementation purpose we need a "Arduino" device to interface the associated microcontroller with the gas sensor and temperature sensor. A deployed device is configured in such a way that whenever the gas sensor detects the level of gas beyond the desired level then a alarm message is sent to the respective authorities regarding harmful gas level. In such a way we can save the lives of the people working in the coal mines [4], [18].

Smart Agriculture: The world's population is increasing day by day. Therefore, to feed growing population, the farming industry must use new technological framework such as IoT. Agriculture suffers from certain challenges for example, extreme weather conditions, rising climate change and other environmental factors. The smart farming is based on IoT related frameworks help the farmers to reduce the wastage and enhance productivity. Smart farming process is a hi-tech system with low cost to grow the food cleanly and sustainable for the masses. In a WSN and IoT-based smart farming, a system is built to monitor the crop field by help of sensors (for example, humidity, light, soil moisture, etc.) and to automate the irrigation system. Using such system a farmer can monitor the field conditions using a smartphone from anywhere. That makes it efficient approach as compared to the conventional approach. Smart farming can provide various benefits such as efficient use of water (optimization of inputs and treatments) and fertilizers [4], [19]–[22].

A. MOTIVATION

Sometimes WSN and IoT devices (i.e., sensors) are installed in an "unattended (hostile) environment" (for example, smart security and surveillance applications), where we can not monitor these devices physically whole day and night [23]–[26]. An adversary $\mathcal{A}$ may take the advantage of lack of physical monitoring, and thus he/she can steal some IoT sensor nodes from the deployment area. Using the extracted information from the captured nodes, $\mathcal{A}$ can manufacture attacker nodes and deploy them in the existing network. These attacker nodes may then launch various attacks (i.e., blackhole, sinkhole, wormhole, Sybil and flooding) in the network. These attacks can degrade the performance, efficiency and reliability of the communication. For example, we may experience in decrease of the throughput of the network, increase in the end-to-end delay, and also decrease of the packet delivery ratio [27]. Hence, it becomes extremely essential for intrusion detection protocols to protect such kinds of attacks. In this paper, we provide a survey on the existing intrusion detection protocols for both WSN and IoT enviornments. We believe that the conducted survey work will be helpful for the researchers in this domain of the IDS in WSN and IoT.

B. EXISTING SURVEYS IN INTRUSION DETECTION PROTOCOLS IN WSN AND IoT

In 2012, Farooqi and Khan [13] discussed and analyzed the existing intrusion detection systems for WSNs. They also discussed the security issues and attacks in WSN. The comparative study on the IDS-based security mechanisms were also provided in their survey work.

In 2016, Dhakne and Chatur [14] discussed different detection techniques of IDS, such as anomaly based detection, misuse based detection and specification based detection.

TABLE 1. Existing surveys in intrusion detection protocols in WSN and IoT environments.

Reference	Year	WSN and IoT architectures discussed	Security requirements and attacks	Potential applications of WSN integrated IoT discussed	Taxonomy of security protocols in WSN and IoT	Key areas covered
Farooqi *et al.* [13]	2012	×	✓	×	×	* Different types of intrusion detection systems for WSNs * Security issues and attacks in WSNs * Comparative study of existing IDS-based security mechanisms
Dhakne *et al.* [14]	2016	×	×	×	×	* Different types of intrusion detection methods * Limitations and research challenges of WSNs * Discussion on future directions
Zarpelao *et al.* [15]	2017	×	×	×	×	* Trends, open issues, categories of IDS in IoT * Discussion on future research directions
Elrawy *et al.* [16]	2018	Only IoT architectures	Only security requirements	×	×	* IoT system architectures * Comparative study of IDS protocols in IoT * Future outlook
Khan *et al.* [17]	2019	×	Only attacks	×	×	* Discussion on IoT attacks and IDS implementation * Comparative study on IDS schemes * Discussion on future directions
Our survey	2019	✓	✓	✓	✓	* Various issues and challenges associated with WSN and IoT * Threat model applicable in security of WSN and IoT based communications * Security requirements and various attacks possible in WSN and IoT environment * Various architectures of WSN and IoT * Taxonomy of various security protocols in WSN and IoT * Comparative study of intrusion detection protocols in WSN and IoT * Future research challenges

They further provided the details of intrusion detection systems, which were proposed for WSNs along with their advantages and disadvantages. Some future directions for selection of IDS were also highlighted.

In 2017, Zarpelao *et al.* [15] provided a survey on intrusion detection systems for IoT environment. Their work was conducted to identify trends, open issues and future research directions in IoT communication. They divided the IDS as per the attributes, such as detection method, IDS placement strategy, security threat and validation strategy.

In 2018, Elrawy *et al.* [16] provided the details of IoT architecture and the associated security vulnerabilities. They also demonstrated the studies regarding the design and implementation of intrusion detection systems for IoT. Some key considerations for the development of intrusion detection systems were provided that are needed in the future.

In 2019, Khan and Herrmann [17] provided a survey on intrusion detection systems for IoT environment. They have provided the details of IDS for the Mobile Ad Hoc Networks (MANET), WSN and Cyber-Physical Systems (CPS), which are suitable for IoT. Some future research directions for IoT security were also highlighted.

The summary of existing surveys and our survey presented in this paper in the domain of intrusion detection protocols in WSN and IoT environments is provided in Table 1.

C. CONTRIBUTIONS

In this survey work, the research contributions are summarized below.

- We first highlight various issues and challenges associated with WSN and IoT.
- We then provide the details of threat model applicable in the security of WSN and IoT based communications. Furthermore, we discuss the security requirements and various attacks possible in WSN and IoT based communication environments.

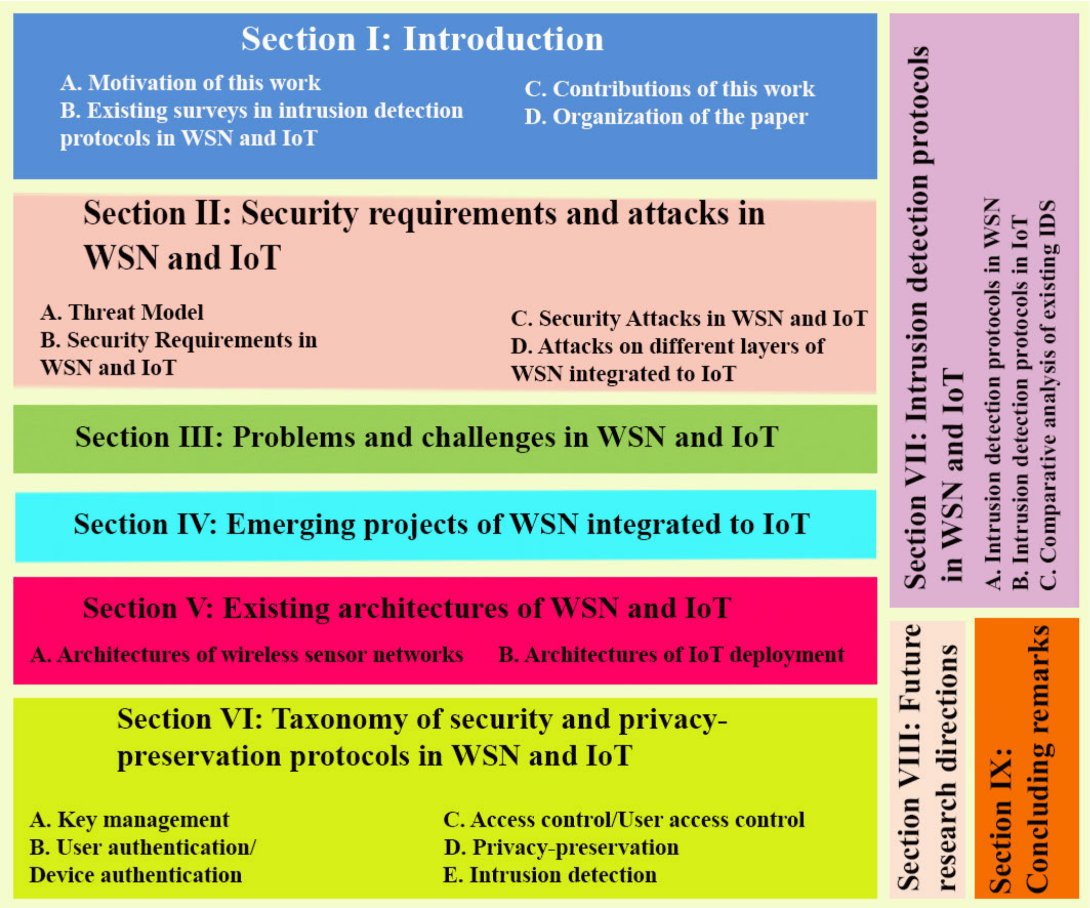
Section I: Introduction
A. Motivation of this work
B. Existing surveys in intrusion detection protocols in WSN and IoT
C. Contributions of this work
D. Organization of the paper
Section II: Security requirements and attacks in WSN and IoT
A. Threat Model
B. Security Requirements in WSN and IoT
C. Security Attacks in WSN and IoT
D. Attacks on different layers of WSN integrated to IoT
Section III: Problems and challenges in WSN and IoT
Section IV: Emerging projects of WSN integrated to IoT
Section V: Existing architectures of WSN and IoT
A. Architectures of wireless sensor networks
B. Architectures of IoT deployment
Section VI: Taxonomy of security and privacy-preservation protocols in WSN and IoT
A. Key management
B. User authentication/ Device authentication
C. Access control/User access control
D. Privacy-preservation
E. Intrusion detection
Section VII: Intrusion detection protocols in WSN and IoT
A. Intrusion detection protocols in WSN
B. Intrusion detection protocols in IoT
C. Comparative analysis of existing IDS
Section VIII: Future research directions
Section IX: Concluding remarks

FIGURE 1. Outline of the paper.

- Next, we discuss various architectures related to WSN and IoT environments.
- A taxonomy of various security protocols in WSN and IoT is also provided.
- We then particularly focus on intrusion detection protocols associated with WSN and IoT.
- We provide a comparative study of intrusion detection protocols associated with WSN and IoT.
- Finally, we highlight some research challenges which need to be addressed in the coming future.

D. ORGANIZATION OF THE PAPER

Rest of the paper is organised as follows. The details of threat model applicable in the security of WSN and IoT based communication along with the security requirements and various attacks possible in WSN and IoT based communication environment is provided in Section II. The problems and challenges of WSN and IoT are discussed in Section III. Various architectures of WSN and IoT are discussed in Section IV. A taxonomy of security and privacy-preservation protocols in WSN and IoT is provided in V. The summary of existing intrusion detection schemes of WSN and IoT is provided in Section VI. We have also provided the comparison of various intrusion detection schemes in this section. Some future research challenges and directions in WSN and IoT are discussed in Section VII. Finally, the paper is concluded in Section VIII. Overall, the organization of the paper is provided in Fig. 1.

II. SECURITY REQUIREMENTS AND ATTACKS IN WSN AND IoT

In this section, we first discuss a threat model associated with the data security in WSN and IoT based communication environment. After that we discuss different security requirements and possible attacks which happen in these environment.

A. THREAT MODEL

The well-known Dolev-Yao (DY) threat model [28] is applicable in WSN and IoT based communication environments as it is applied for other wired/wireless networks [29], [30]. As per the fundamentals of the DY model, any two communicating parties communicate over an insecure public channel. Under this model, end-point communicating parties such as users, IoT sensors, cloud servers and fog servers are not trusted entities. An adversary $\mathcal{A}$ can then modify, delete or insert messages from/in the ongoing communication. Furthermore, $\mathcal{A}$ can physically capture some sensor/IoT sensors and extract important information from its memory [31], [32]. $\mathcal{A}$ can clone new malicious nodes with different attack functionalities (i.e., sinkhole, wormhole and blackhole) program along with the use of extracted information. After the manufacturing of these malicious devices, $\mathcal{A}$ can directly deploy them in WSN and IoT based communication environment [27], [33], [34]. Under the execution of these malicious attacks, the data packets may get lost, dropped, delayed or modified which further degrades the performance of the ongoing communication.

B. SECURITY REQUIREMENTS IN WSN AND IoT

In this section, we discuss the essential security requirements in WSN and IoT based communication environment including the general security requirements as required by other networks [35], [36]:

- *Authentication:* Its a process of validating the identity of a communicating party or device. For example, sender and receiver first verify their identities mutually after that they can start their communication in a secure way. WSN and IoT based communication environment involves various entities such as different devices (for example, WSN or IoT sensors), gateway nodes, different types of users, cloud server(s) and cloud service provider(s), which can authenticate among each other.
- *Integrity:* Integrity mechanism helps to assure the integrity of the exchanged messages. According to this property, the content of the received message should not contain fake insertion, or deletion of information, and not modified during communication.
- *Confidentiality:* Sometimes it is also called as "privacy". It assures that the data transmitted in the channel should be protected against any type of unauthorized disclosure of the information.
- *Non-repudiation:* This mechanism provides the assurance that a communicating party should not refuse the validity of something. It evidences the proof of the data origin and integrity. This makes very hard for a party to refuse who or where a message came from along with the authenticity of that message. Non-repudiation is again divided into the following two categories:
  - Non-repudiation of origin: It confirms that the message was transmitted by the original party (sender) is genuine.
  - Non-repudiation of destination: It confirms that the message was received by the original party (receiver) is genuine.
- *Authorization:* This property assures that only the authentic parties (i.e., sensors) in WSN and IoT based communication environment can provide information to the other parties.
- *Freshness:* This property assures the freshness of the communicated information so that the old messages will not be re-transmitted by the attacker.
- *Availability:* This property assures that the legitimate parties should have access to the associated network services even in case of "Denial-of-Service (DoS)" attacks in WSN and IoT based communication environment.
- *Forward secrecy:* If any device or party leaves WSN and IoT based communication environment, the entity must no longer have access to the future messages.
- *Backward secrecy:* When a new device or party is added to the WSN and IoT based communication environment, it must not have any access to the previously exchanged messages.

C. SECURITY ATTACKS IN WSN AND IoT-BASED COMMUNICATION

The WSN and IoT based communication environment suffers from following types of potential attacks that may be carried out by a passive or an active adversary [37]:

- *Eavesdropping:* This act is also called sniffing or snooping attack. It happens when an adversary eavesdrops the exchanged messages between two (or more) communicating parties. It is also one of the potential threat for WSN and IoT based communication.
- *Traffic analysis:* In this malicious act attacker does the interception of messages and further examines the intercepted messages to know which kind of communication is going there among the communicating parties.
- *Replay attack:* This attack happens if an adversary intercept the exchanged messages and then knowingly delays or re-transmits them to a receiving party.
- *Man-in-the-middle attack (MITM):* In this malicious act an adversary intercepts the exchanged messages and then tries to modify, update or delete the contents of the messages before conveying them to the receiving party.
- *Impersonation attack:* In this malicious act an adversary successfully finds out the identity of one of the genuine communicating party of the network and then update his/her communicated messages and send the updated messages on his/her behalf to a recipient.
- *Denial-of-Service attack:* This attack happens when an malicious actor performs his/her malicious activities to prevent original users from accessing the resources of the system (for example, data from a WSN or IoT sensor). Some of the hazardous DoS attacks of WSN and IoT are blackhole, wormhole, greyhole and sinkhole [27], [33], [34]. The occurrence of such attacks disrupt the whole functionality of WSN and IoT. However, the more powerful version of DoS attack is "Distributed DoS (DDoS)" attack. DDoS is performed by multiple attackers in the network at the same time (for example, through a botnet). Some of examples of DDoS attack are flooding attacks which consume resources (i.e., bandwidth) of the targeted system (i.e., web servers).
- *Malware attack:* This malicious act happens when an adversary executes malicious script (i.e., some malware) in a remote system (i.e., smart IoT device) to perform

TABLE 2. Layerwise attacks on WSN integrated to IoT [47].

Layer	Attacks
Physical	Tampering, sybil attack, jamming, interception
Data link	Sybil attack, exhaustion, collision, unfairness, replay attack, traffic analysis and monitoring, spoofing and altering routing attack
Network	Selective forwarding attack, black hole attack, Homing, sybil attack, hello flood attack, spoofing attack, wormhole attack, neglect and greed, sinkhole attack, grey-hole attack, misdirection attack, Internet smurf attack
Transport	Transport layer flooding attack, desynchronization
Application	False data injection, spoofing and altering routing attack

various unauthorized tasks. Examples are stealing, altering and deletion of sensitive information and hijacking of shell of the system. They may monitor user's system activities without their permission. On the basis of their characteristics malware can be divided into various categories such as keylogger, spyware, trojan horse, ransomware, rootkit, virus and worm [38]–[41].

- *Physical capturing of WSN/IoT devices:* As we discussed in the threat model (see Section II-A), physical capturing of devices (i.e., WSN and IoT sensors) is possible by a physical adversary. After the act of physical capturing of devices, attacker may extract sensitive information from the captured devices to further launch other attacks in WSN and IoT based communication environment [27], [33], [34], [42].
- *Privileged-insider attack:* In this attack a "privileged-insider user" of the trusted authority (server) misuses the stored information to perform other serious attacks (for example, offline guessing of password) [3], [43].
- *Database attack:* In WSN and IoT based communication environment, some attacks are also possible on the database maintained over the cloud. The happening of such attacks cause the discloser of information maintained over the cloud server. The examples are "Cross-Site Scripting (XSS) attack", "Cross-Site Request Forgery (CSRF)" and "Structured Query Language (SQL) attack" [44]–[46].

D. ATTACKS ON DIFFERENT LAYERS OF WSN INTEGRATED TO IoT

The architecture of WSN consists of five different layers, which are physical layer, data link layer, network layer, transport layer and application layer. The attacks corresponding to various layers of WSN stack are provided in Table 2.

Among all these attacks provided in Table 2, the network layer attacks are malignant as they discompose the whole functionality of the network, especially routing mechanism that further causes DoS attacks [34], [47].

III. PROBLEMS AND CHALLENGES IN WSN AND IoT

In this section, we discuss the following problems as well as challenges related to WSNs and IoT environment:

- *Limitations of resources*: In both WSN and IoT environment the sensors are used which are resource constrained in nature as they have limited battery, limited computation and communication capabilities. This is always an issue in terms of device level security as we cannot afford a heavyweight security algorithms which need more resources to protect the network. Hence, we need a low powered security mechanism to minimize the power consumption during the intrusion detection process. This will further prolong the network lifetime. Many techniques have been proposed which consumes low power for intrusion detection process using the lightweight operations [3], [27], [34], [48], [49].
- *Support for scalability without compromising the security*: As the number of IoT devices are increasing every day, so are the security threats. Its quite difficult to scale up the IoT network without protecting the network against the intruders. As we are heading to build smart cities which scale up the IoT network because of the increased number of the heterogeneous devices, which are being added to build a smart city IoT network. Therefore, we need such kind of security protocols in which little modification is allowed when we go for the scale up process of the network. For example, addition of smart sensing device [3] without compromising the security of a large network is much needed [50].
- *Security of mobile sensing devices*: Devices which keep on changing the network topology have to cope with the different security protocols. Hence its quite challenging for the mobile sensing device to maintain the security with different network configurations. There are many wearable devices which monitor the health and location of the human being. But getting connected with different networks because of moving nature of the sensing device and data transmission to cloud servers is quite challenging. Therefore, designing a secure defence mechanism for the mobile sensing devices is much needed [6].
- *Facilitation for heterogeneous network*: IoT environment has variety of sensing devices which have different hardware and software platforms. These devices have different security measures that cause difficulty in their working for a common IoT platform. Therefore, we need to design a secure protocol which can be utilized in different devices [6], [7].
- *Physical security of sensor nodes*: WSN and IoT both networks are prone to the physical capturing of sensor nodes attack. After this physical capturing of sensor nodes adversary $\mathcal{A}$ performs power analysis attack [31] to extract the sensitive information. This results in the further compromising of remaining part of the network which affects the network performing parameters for example, latency, efficiency, accuracy and packet dropping rate. The 24 hours physical monitoring is required to protect against physical capturing of sensor nodes. Therefore, we need such kind of intrusion detection protocols which also work in case of physical capturing of nodes [27], [34]. Further, we may apply tamper-resistant packaging [6] to defend captured nodes from power analysis attack.

- *Localization of nodes*: Gathering the information about the physical or geographical locations of the randomly deployed nodes in WSN is called as the localization process. Due to the harsh weather and unfriendly environmental conditions positions of the sensor nodes may be changed. Because of such conditions the whole network configuration may be changed for this reason we require proper location information of the shifted sensor nodes to reconfigure the network. This may further affect the performance of the deployed intrusion detection protocol. Following techniques are proposed to resolve the problem of localization of nodes. For example, proposed mechanism [51] combined the semi-supervised machine learning technique and support vector regression to find out the target nodes locations. Protocol [52] used semi-supervised hidden Markov model to solve the localization problem for mobile nodes in WSNs.
- *Detection of faulty nodes*: Most of the time WSNs nodes are deployed in the harsh environmental conditions where the reach of human being is very difficult. In that environment some of the nodes may be failed which further disturb the configuration of the network. Therefore, we need some protocols which can overcome the problem of faulty nodes. Reference [53] proposed a model-reduced fault detection technique. Other techniques are heterogeneous fault diagnosis and matrix calculus for detecting the faulty nodes [54], [55]. There are many machine learning techniques which facilitate the fault detection process to improve the results. SVM classifier is used to detect the faults in the network by using the kernel function [56]. Henceforth, we need such kind of intrusion detection protocols which can also overcome the faulty nodes conditions.
- *Nodes synchronization*: Synchronization of clocks of all deployed nodes is mandatory for the designing of various types of protocols in WSN and IoT. Synchronization is required in various tasks such as transmission schedule, intrusion detection, data agglomeration, power management, etc. Synchronization of nodes can be achieved through various proposed techniques for example, time based synchronization for acceleration measurement, counter-based synchronization for duty-cycled in WSNs, use of random bounded communication delays for time synchronization [57]–[59]. There are various machine learning based techniques to synchronize the nodes to perform all the associated WSN tasks mentioned above. Reference [60] used network parameters like end to end delay, clock drift and frequency noise of clock along with regression technique to synchronize the network nodes.

IV. EXISTING ARCHITECTURES OF WSN AND IoT

In this section we have discussed various architectures of wireless sensor networks and Internet of Things.

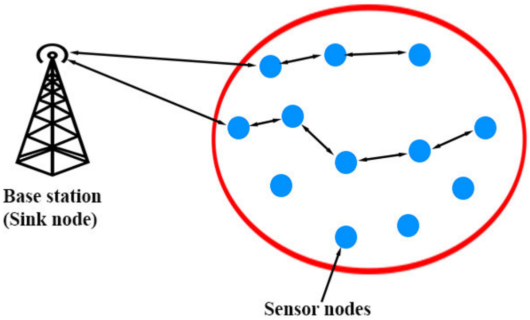

FIGURE 2. Architecture of distributed wireless sensor networks (DWSN) (adapted from [47]).

A. ARCHITECTURES OF WIRELESS SENSOR NETWORKS

The two widely used architectures of WSN are distributed wireless sensor networks (DWSN) architecture and hierarchical wireless sensor networks (HWSN) architecture. We have provided the details of these two architectures in the following part of the section.

1) DISTRIBUTED WIRELESS SENSOR NETWORKS (DWSN) ARCHITECTURE

The architecture of distributed wireless sensor network (DWSN) is provided in Fig. 2. In such architecture there is no fixed infrastructure, and the network topology is not well defined prior to deployment of the sensor nodes in the target field. Most of the time sensor nodes are deployed all over the target field randomly. After the deployment, sensor nodes form an infrastructure-less multi-hop wireless communication between them and data is routed back to the base station (BS). In DWSN either sink node broadcast data query message or the source node floods the query message in the network to find the best route to the sink to send the sensed and collected information. DWSN is also considered as the data-centric approach. There are many protocols used for transfer the sensed information to the sink node like Flooding, Gossiping, Spin, Direct Diffusion, Rumor Routing, Energy-aware routing for low-energy ad-hoc WSN. However, this method is not suitable for wide-reaching and also has network life-time issue for wide-range [47], [61], [62].

2) HIERARCHICAL WIRELESS SENSOR NETWORKS (HWSN) ARCHITECTURE

The architecture of hierarchical wireless sensor network (HWSN) is provided in Fig. 3. In such architecture there is a hierarchy among the nodes based on their capabilities: base stations, cluster heads and sensor nodes [47]. Sensor nodes are generic wireless devices have limited capability. The sensor node has limited battery backup, low storage and limited data processing and communication capability. Clustering is also called as grouping of nodes. Sensor nodes in a cluster communicate among each other in that cluster, and finally communicate with cluster head node. Cluster heads are resource-rich nodes. They are installed with high power batteries, larger memory storage, powerful antenna and

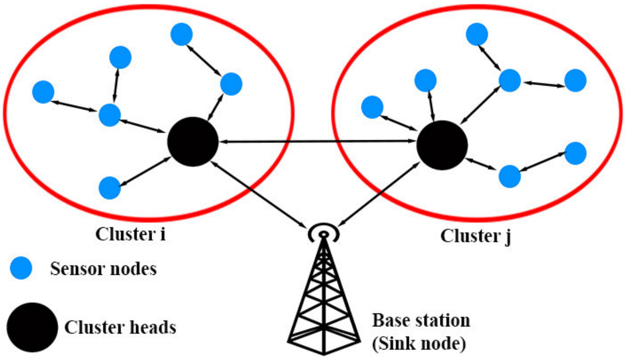

FIGURE 3. Architecture of hierarchical wireless sensor networks (HWSN) (adapted from [47]).

data processing capabilities, and they can execute relatively more complicated numerical operations than sensors, and have much larger radio transmission range. Cluster heads can communicate with each other directly and also relay data between its cluster members and base station. PDA (personal digital assistant) or an IMote2 can be configured as cluster head. Base station (also called the sink node or the gateway node) is a gateway to the other networks, which is considered as the powerful data processing unit (storage center). It is also an access point for human interface. Base station receives sensor readings, performs costly operations on behalf of sensor nodes and also does the task of network management. The base station is assumed to be the trusted entity of the network. Sensor nodes are deployed around one or more hop away from the base station. However, cluster heads are resource-rich as compared to sensor nodes. A cluster head can also directly communicate with base station or indirectly through its neighbor cluster heads. Base station is the most resource-rich node in WSN having high computational and communication power, large storage capacity, and high radio transmission range. Hence it can reach all the nodes in a network. On the basis of required applications, base station can be located either in the center or at a corner of the network [47]. All cluster heads pass the information for further processing to the base station using following two methods: (i) Single hope and (ii) multi hope, this approach can easily extend the network without lifetime issue. Many protocols are used to implement this approach (for example, LEACH, PACT, HEED, PEGASIS, Hierarchical-PEGASIS, TEEN, APTEEN, Energy-Aware Routing for Cluster-based WSN and SecRout [61], [62]).

B. ARCHITECTURES OF IoT DEPLOYMENT

We provide the details of various Internet of Things architectures in the following part of the section.

1) GENERIC INTERNET OF THINGS ARCHITECTURE

The generic architecture of Internet of Things is provided in Fig. 4. In the given architecture there are different scenarios for example, smart home, transport and community. These scenarios are deployed with different smart devices for example, sensors and actuators. These devices facilitate the day to day activities of the people. In all these scenarios, all smart devices are connected to the Internet through a specific device which is called gateway nodes (GWNs) or gateway router. There are different types of users (for example, doctor, industrialist and smart home user) who have interest in accessing the data of relevant IoT devices via the GWN. For their secure communication we need a security protocol which can perform the mutual authentication between a user and a device via the gateway node [43].

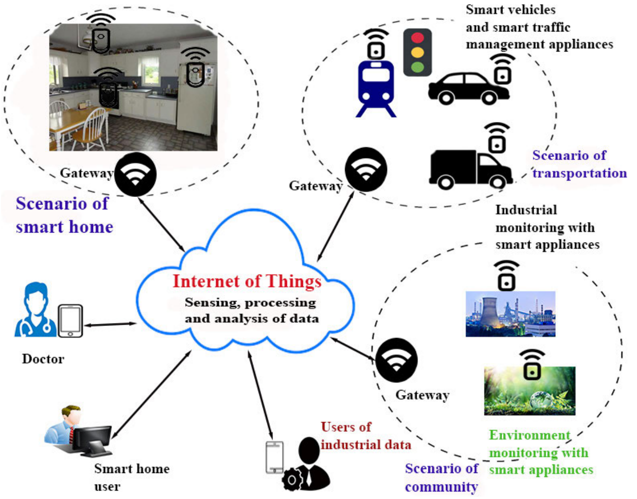

FIGURE 4. Generic Internet of Things architecture (adapted from [43], [63]).

2) CLOUD BASED INTERNET OF THINGS ARCHITECTURE

The architecture of cloud based Internet of Things is provided in Fig. 5. IoT cloud based architecture has three layers which composes of a collection of sensing devices, gateway and cloud servers. Here the collaboration of cloud services with IoT environment makes the whole system worthwhile. The sensing devices communicate through wireless communication technology such as RFID, LAN, IEEE 802.11 and IEEE 802.15.4. This allows the sensing devices to design a rout map from different sources to the destination in a multi hope manner. The gateway node facilitates the communication between sensing devices and the cloud servers. The data which is collected by the sensing devices has to be transferred to the cloud servers for further processing via the gateway node. Finally, data reaches to cloud server which is responsible for organizing the data transfer from the sensing device to user's devices. Cloud server processes the data as per the requirement of the application for different users [42], [64].

3) FOG BASED INTERNET OF THINGS ARCHITECTURE

The architecture of fog based IoT is provided in Fig. 7. In IoT all the objects are getting smart and the data which is produced by these objects is very huge and it is becoming difficult for the internet infrastructure to handle it. Then the combination of IoT and Cloud computing tranquilized the situation but not sufficient to resolve all the IoT issues.

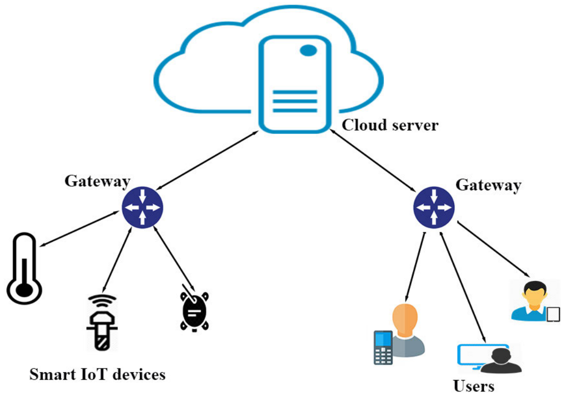

FIGURE 5. Cloud based Internet of Things architecture (adapted from [42], [64]).

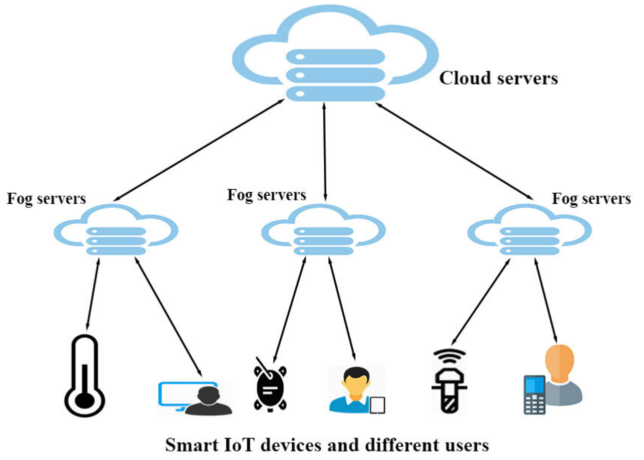

FIGURE 6. Fog based IoT architecture (adapted from [10], [65]).

Therefore, in 2012 CISCO came up with the new concept of computing named as Fog Computing. Fog Computing eases the task of cloud servers and manages data very near to IoT devices like proxy which improves the efficiency, reduces the end to end delay and saves the bandwidth of the infrastructure. There are two frameworks, first one is "fog-device" and the other one is "fog-cloud-device". In first one, the fog servers provide the services and in the second one, the simple tasks are performed by Fog and tedious tasks are performed by Cloud servers. As fog computing performs the data analysis near to the IoT devices, we may consider a real time scenario of data analysis which may be more vulnerable to security breach. Fog nodes consult with the adjacent nodes, and then their combined efforts are used to find out the attacker nodes by analyzing the behavior [10], [65].

4) EDGE BASED INTERNET OF THINGS ARCHITECTURE

The architecture of edge based Internet of Things is provided in Fig. 6. Edge computing is very similar to fog Computing but in place of fog nodes it has an edge node which is the part of the edge devices network and resource rich node which computes and analysis all the data on behalf of its network and transfer the data to cloud servers if required. In edge computing the data produced by the IoT devices remains inside the network and remains safe from the attacker nodes until it is passed to the cloud server. In most of the developed counties it is under the regularity act to keep the data inside the network boundary. There are certain applications of IoT where we can not delay the information by sending it to the cloud servers first and then take the appropriate action because of the safety measures like boarder surveillance, car airbags, safety alarms etc. In edge computing if edge server node resolves most of the queries of users at the network edge level then we can save the bandwidth and decrease the end to end delay. Edge node can also be used for the intrusion detection purpose in an edge based IoT architecture [66].

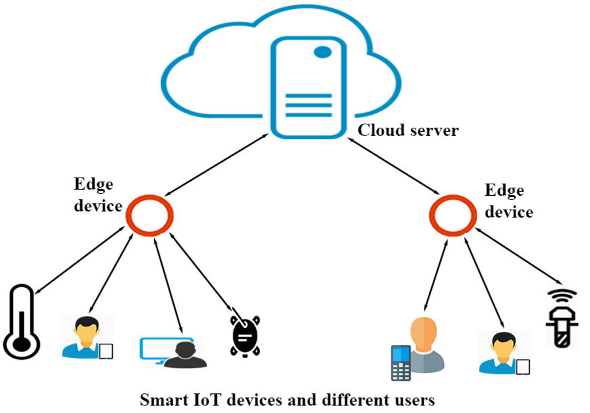

FIGURE 7. Edge based Internet of Things architecture (adapted from [66]).

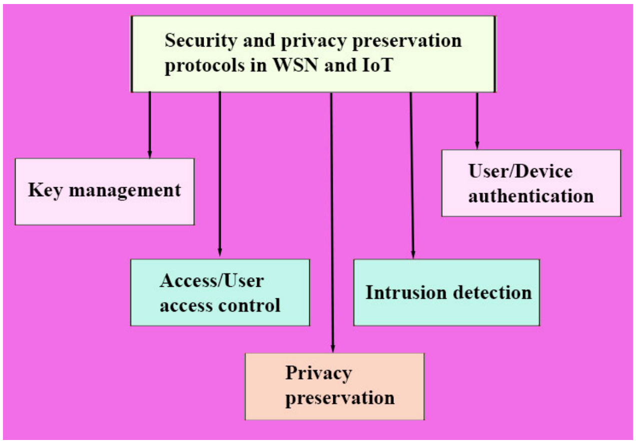
Security and privacy preservation protocols in WSN and IoT
Key management
User/Device authentication
Access/User access control
Intrusion detection
Privacy preservation

FIGURE 8. Taxonomy of security protocols in WSN and IoT.

V. TAXONOMY OF SECURITY PROTOCOLS IN WSN AND IoT

This section briefs the security protocols used in WSN and IoT based communication environment which provide security of the data in transit as well as the stored data. A taxonomy of security protocols in WSN and IoT based communication environment is provided in Fig. 8 similar to that in [67].

A. KEY MANAGEMENT

The process of key management trades in the management of cryptographic keys in WSN and IoT based communication environment among the participating entities. The procedure contains certain steps such as generation, exchange, storing, usage and replacement of keys as per the needs. A key management procedure exhibits a ''cryptographic protocol'' which gives the details of the key servers (for example, trusted authority), users and other involved devices. It is also called as the key distribution and management process among the network communicating entities. The security of the communication system relies on the successful key management [68]–[70], [71]. Typically, a key management protocol contains following phases:

- *Pre-deployment phase:* In this phase, a trusted authority (*TA*) setups the system parameters for various network entities. *TA* also does the registration of different network communicating parties (for example, smart IoT devices, cloud server, different types of users and other involved devices). After the successful registration, the generated information is stored in the devices and then these devices will be deployed/installed in the network.
- *Key generation and distribution:* In this process, the cryptographic keys such as secret keys are generated. A device (for example, trusted authority) who generates the keys is named as the key generator. In the ''symmetric key cryptography'' mechanism, communicating entities should share a secret key which they must exchange in advance before they are going to start their secure communication. To perform the steps of key distribution, typically the neighbor devices utilize their preloaded credentials in order to establish secret pairwise keys among them (for example, the key pre-distribution schemes suggested in [72]–[85]).

  In ''public key cryptography'' mechanism, the key distribution of public keys is performed by a public key server (for example, trusted authority) in which a communicating party creates a pair of keys and further it keeps one key as private and the other key as public. In the next step, public key is uploaded to the server where it can be accessed by any legitimate network entities. Often the trusted authority generates the private and public key pair for a device, and stores private key in the memory of that device, and announces the other corresponding key publicly to the other parties of the network.
- *Key establishment phase:* After the successful deployment of all network entities. All devices and users can start their communication in a secure way under the execution of steps of security protocol. However, before that the network entities have to exchange some messages for the secure computation, communication and establishment of session key. Then after the execution of these steps, the parties can communicate securely.
- *Key revocation and dynamic device addition phase:* Sometimes in an hostile or unattended environment (i.e., battle field communication environment), there are chances that some of network devices (for WSN or IoT sensors) may be physically captured by an enemy (adversary). After that the adversary can extract the secret (private) key stored in this device by using the steps of power analysis attacks [31]. In those circumstances, the *TA* requires to generate a new key pair (private and public) and store them into the memory of new WSN/ IoT sensor (device) before their deployment in the network for the ''public key cryptography'' mechanism.

B. USER AUTHENTICATION/DEVICE AUTHENTICATION

In user or device authentication mechanism, one communicating entity (i.e., device or user) verifies the identity of the other communicating entity (user or device). If mutual verification happens successfully, both communicating parties authenticate each other and establish a session key to secure the communication for future. Device authentication procedure is analogous to the user authentication procedure.

For the sake of simplicity, we explain only the user authentication process here. A user authentication scheme in WSN or IoT based communication environment can have following phases [3], [29]:

- *System setup phase:* A trusted authority *TA* chooses the system parameters in the offline mode.
- *Pre-deployment phase:* Here *TA* does the registration of different communicating entities (i.e., smart IoT devices, users, fog server(s), cloud server(s), gateway(s)). After performing these steps, the *TA* stores the essential information in the memory of the deployed devices.
- *User registration phase:* To access the real-time information from a specific device, a user needs to register him/ herself to the *TA*. For this purpose, user first selects his/her credentials (i.e., his/her identity, password and biometrics information), and then sends these information to the *TA* via a secure channel (for example, in person). After preforming these steps successfully the *TA* issues a smart card or mobile device to the registered user in a secure way by storing the useful information in the memory of smart card or mobile device.
- *Login phase:* In login phase, a user needs to provide his/ her credentials to a specific interface of a device (i.e., his/ her mobile device). Next, mobile device permits the local verification of the entered credentials. After the successful verification of the user credentials, a login request message is formed which is further transmitted to other communicating entity (i.e., gateway, cloud server) via insecure channel.
- *Authentication and key agreement phase:* Upon the arrival of the login request message from the other entity, an entity executes remaining steps as follows. The receiver (i.e., IoT sensor) verifies the authenticity of the message. If it is done successfully, then only the receiver generates an authentication reply message which requires verification of a generated session

key, and then it is sent to the user back via a public channel. When the same entity receives the message, the entity calculates the session key by using the secrets (i.e., temporal and long-term secret credentials) that are known and available in the received message. If the mutual authentication between the user and the receiver (i.e., IoT sensor) is conducted successfully, they establish a session key for their future secure communication.

- *Password and biometric update phase:* To provide better security, it is always recommended to provide the functionality of password and personal biometrics change. By preforming the steps of this facility a genuine user can change his/her password and biometric information using his/ her mobile device or smart card with or without involving the *TA*. However, it is recommended that this phase should be executed locally without involving *TA* in order to reduce the communication and computational overheads.
- *Smart card/ mobile device revocation phase:* If a smart card or mobile device of a genuine user is stolen or lost, the protocol should have a facility of revocation to issue a new smart card or a mobile device to the user along with the new set of stored credentials.
- *Dynamic node addition phase:* In certain situations, the communicating parties (for example, smart IoT devices) are deployed in an hostile environment or unattended environment. In those cases, some devices (i.e., smart IoT devices) may be physically captured by an adversary. Apart from that some devices may fail because of other factors like battery depletion (power failure). To recover from this situation we have to deploy new devices in the network. For that purpose *TA* further generates the new credentials for a new device and stores them in its memory and then that device will be deployed in the network. The *TA* requires to provide the information about the new node addition to the other parties of the network so that the intended users can access the real-time data from the newly deployed devices.

It is important to notice that a user authentication protocol can be classified into several categories based on the number of factors utilized in that protocol. It is called a *single-factor user authentication protocol*, if only the mobile device or smart card or password is used. In a *two-factor user authentication scheme*, both mobile device (smart card) and password are used. In a *multi-factor user authentication scheme (i.e., three factor)*, different factors such as mobile device (smart card), password and biometrics (i.e., fingerprint) can be used for a three-factor user authentication protocol. Moreover, addition of a factor adds more security to a protocol. For example, three-factor user authentication protocol is more secure than a two-factor user authentication protocol [3] although it may incur more computational overhead as compared to single-factor/two-factor user authentication protocol.

C. ACCESS CONTROL/USER ACCESS CONTROL

Access control is a mechanism which restricts the access to the resources in a network. In this process, the users or devices are granted access and privileges to various resources. To improve the lifetime of the WSN and IoT-based communication environment, it is required to deploy new devices (i.e., IoT sensors) in the network. This occurs when IoT devices stop functioning due to battery drainage or because of the physical node capturing attack. Furthermore, an attacker can deploy some malicious devices in the network [27], [34]. Therefore, it is important to distinguish between a genuine device and a malicious device. Hence, we need to design secure access control protocols to prevent malicious nodes entering into the WSN and IoT based communication environment.

The following two tasks are required to be done in an access control protocol:

- *Node authentication:* When a node (i.e., smart IoT device) is newly deployed in WSN and IoT based communication environment, it must authenticate itself to other neighbor nodes. This process assures that it is a genuine node which is authorized to access the information from its neighbor nodes.
- *Key establishment:* When a node (i.e., smart IoT device) is newly deployed, it should be able to establish shared secret keys with its neighbor nodes to do the future communication in a secure way. This can be achieved when this node authenticates with its neighbor nodes successfully.

Access control protocols can be divided into two categories based on their authentication procedure:

- *Certificate-based*: In a "certificate-based access control protocol", each deployed device is loaded with a digital certificate (for example, X.509 certificate [86]) provided by the *TA*. The stored certificate is again used to prove its identity to its neighbor device.
- *certificate-less*: In a "certificate-less access control technique", typically a hash-chain based procedure is followed. Furthermore, to provide access right only to the genuine registered users for different services, the information and resources available in WSN and IoT based communication environment, user access control protocol is much useful.

Therefore, a user access control mechanism is an another influential security perspective.

D. PRIVACY-PRESERVATION

The communication in WSN and IoT based communication environment suffers from serious breaches of consumers' data privacy [87]. For example, a patient's data over the health cloud in a "cloud based health sensor network" may contain the health data of the patient (i.e., patient's diseases history and medicines they take) [88]. To protect customer's personal data privacy from any kind of disclosure, privacy-preserving mechanisms are required [89], [90].

Therefore, our aim should be to design privacy-preservation security protocols. This would further help to protect the secret information of the customers from any kind of leakage [3].

Li *et al.* [91] presented a survey work on various privacy-preserving techniques in WSNs. They mainly reviewed two important categories of privacy-preserving mechanisms for protecting confidential information, context-oriented and data-oriented privacy. Context-oriented privacy protection deals with the protection of contextual information (for example, location and timing information of traffic transmitted in WSN environment. On the other hand, data-oriented privacy protection deals with protection of the privacy of data content. Furthermore, they provided a taxonomy of several privacy-preserving protocols in WSNs.

Sharma and Bhatt [92] designed a privacy-preserving mechanism in which they divided the original message into three parts. These parts are then are communicated along with the hash value with the help of a multipath routing to different servers. By this method, it was shown that their scheme has better performance as compared with the plain-text based transmission, and their scheme is able to protect privacy preservation in an WSN-based healthcare system.

Yamin *et al.* [93] suggested a privacy-preserving scheme, called the to blind approach for protecting a user's identity and also the associated personal data in an IoT environment. Their scheme solves the trust problem, because the users can protect their privacy without having to trust a third party entity in the IoT environment.

E. INTRUSION DETECTION

An "intrusion detection system (IDS)" is deployed to monitor and analyze malicious traffic to protect the devices (i.e., smart IoT devices) from the various attacks. In WSN and IoT based communication environment, an IDS verifies all incoming traffic and searches for any sign of intrusion. If it identifies any threat, the deployed mechanism takes proper actions (i.e., send the notification to the administrators, blocking of malicious source IP address). In WSN and IoT based communication environment, it is also possible that an adversary may physically steal some devices (i.e., IoT sensor). Further, the adversary can deploy his/her malicious devices using the extracted information from the captured devices. These malicious devices may be pre-installed with some malicious script to launch different attacks (for example, routing attack-blackhole, wormhole, sinkhole, etc.) [27], [33], [34], [66]. Under the execution of these attacks, the data packets may be lost, modified, dropped or delayed before forwarding to the destination. This causes a severe degradation in performance of the communication. This may also cause in reduction in "network throughput" and "packet delivery ratio", and increment in high "end-to-end delay" [27], [66]. Therefore, it becomes important to design an effective intrusion detection mechanism to protect the WSN and IoT based communication environment.

The main functions of IDS are as follows [94], [95].

- Identification of the intruder.
- Location information of the intruder.
- Logging of various ongoing activities.
- Tries to stop the malicious activities.
- Reports the malicious activities to the administrator by providing the information about intrusion activity (i.e., active or passive attack).
- Providing information about the intrusion type (i.e., worm hole, sink hole, etc).

The aim of an intrusion prevention systems (IPS) is to monitor and detect anomalies in a network or in a system. The main difference between IPS and IDS is that IPS can prevent against attacks, whereas the IDS can only detects attacks. An IPS can raise alarms, if anomaly is detected, drop packets, perform connection resetting or block malicious traffic from a malicious URL or IP address [94], [95]. On the basis of its deployment, an IDS can be divided into two following categories.

- **Network based intrusion prevention system (NIPS):** NIPS is used in a network for the detection and prevention of different network attacks. It monitors the entire network for malicious traffic by doing the analysis of various ongoing activities in the network.
- **Host based intrusion prevention system (HIPS):** HIPS is an installed software program (package) which is used to monitor a single host for any malicious sign of activities. It does analysis of ongoing activities inside the host.

Since the provided information is very attack specific, therefore it is very useful to prevent such attacks. Hence, IDS becomes an important component for providing security to WSN and IoT based communication environment. However, the security mechanism used in wired and wireless networks are not that useful for WSN as sensor nodes are resource constrained. Hence, designing of efficient intrusion detection protocol in WSN and IoT based communication environment is a challenging task.

1) REQUIREMENTS OF INTRUSION DETECTION SYSTEMS

An IDS should meet the following requirements [94]:

- If we deploy an IDS in system or in a network. It should not introduce new weaknesses to the system/ network.
- The IDS should be designed in such a way that it needs less system/network resources. It should exhibit less computation and communication costs.
- The implemented IDS mechanism should be reliable enough. It should produce less number of false negatives and false positives.

2) CLASSIFICATION OF INTRUSION DETECTION SYSTEMS

Intrusion detection systems (IDSs) can be divided into three groups: (1) anomaly based detection, (2) misuse based detection, and (3) specification based detection [94], [95]. Their details are provided below.

- **Anomaly based detection:** This kind of detection is based on certain statistical behavior methods. Under which two types of flows (for example, network traffic flows) are defined: such as normal flow and abnormal flow (flow under attack). Any deviation from the normal flow is detected as an anomaly. The disadvantage of this mechanism is that we require to update the profile of normal activities according to the changes occur in the network on the regular basis. The advantage of this mechanism is that it can detect an attack accurately and consistently along with less number of false negatives and positives. It is also very useful for the detection of unknown attacks.
- **Misuse based detection:** It is also called rule based or signature based detection. The signatures of an attack are generated when it happens. The signatures of known attacks are utilized to detect future attacks. The advantage of these technique is that it can detect the known attack accurately and efficiently which causes low false positive rate. It is very much like the anti-virus installed in a system.
- **Specification based detection:** In this detection mechanism the specifications and constraints to describe the correctness of the detection process is defined. Then the behavior of the network with respect to the specifications and constraints is monitored. This mechanism also has the capability to detect unknown attacks. It combines the advantages of both anomaly and misuse based detection mechanism by using manually developed specifications and constraints to identify the abnormal behavior. The working of this mechanism is very similar to anomaly based detection mechanism as it also detects attacks on the basis of deviation from the normal flow of the network. It works on the basis of manually developed set of constraints and specifications. That further causes less false positive rate as compared to the anomaly based detection method. Apart from that this method also has certain drawbacks such as it is time consuming because we need to develop the set of specifications and constraints which consumes lot of time.

3) PERFORMANCE PARAMETERS INVOLVED IN AN IDS

The important performance parameters of an "intrusion detection scheme (IDS)" are the "detection rate (*DR*)" (which is also known as "true positive rate (*TPR*) or sensitivity or hit rate"), "false positive rate or fall out (*FPR*)". It is important to consider these parameters in the evaluation of performance of an proposed intrusion detection technique. *DR* can be computed as "the number of attackers detected by an IDS divided by the total number of attackers present in the test sample" which can be estimated as [33], [34],

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

Moreover, *FPR* can be computed as "the number of nodes falsely detected as attacker nodes" which can be estimated as [33], [34],

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

VI. INTRUSION DETECTION PROTOCOLS IN WSN AND IoT

In this section we have provided the details of various intrusion detection protocols in both WSNs and IoT environments.

A. EXISTING INTRUSION DETECTION PROTOCOLS IN WSN

The summary of intrusion detection protocols in WSN is provided as follows. Wang *et al.* [96] proposed two detection models based on the number of sensors used to detect the malicious nodes. These were single and multiple node detection models. Three network parameters i.e., distance travelled by malicious node, probability of detecting the malicious node and the average distance travelled by the malicious node were used. In both heterogeneous and homogeneous WSN environment, the probability to detect the malicious node with respect to distance travelled by the malicious node in the network were computed using the number of nodes deployed in a particular area, node sensing parameters and variety of nodes.

Wang *et al.* [97] proposed a combination of three different types of IDS models used at three different positions at the network: a) first one is at sink level called IHIDS (intelligent hybrid intrusion detection system), b) second one is at the cluster head level and c) third one is at the node level. IHIDS had a self-learning property for the new attacks as it first isolated the abnormal packets from the normal flow and then passed them to the misuse detection module to protect the system. Nodes were resource constrained so they used the rule-based module to detect the predefined attack to reduce the overhead. Their method named as "misuse intrusion detection system".

Salehi *et al.* [98] proposed a IDS in which they detected the sinkhole intruder in two phases. In the first phase they isolated a list of suspicious nodes by checking data inconsistency in all the nodes and in the second phase they identified the sinkhole attacker node from the list of suspicious nodes by analysing and checking the network's traffic information flow.

Wazid *et al.* [27] designed a IDS which detected different types of sinkhole attacks in a hierarchical wireless sensor network. The detection was done in two phases, in the first phase it detected the presence of the sinkhole malicious nodes by using different network performance values for example, identification of different nodes, complete trace of a node from source node to the destination node, battery depletion values and many others. Once a node came under the suspected category then in the second phase technique confirmed the nodes as the sinkhole attacker node with the following types (sinkhole message delay node, sinkhole message modification node and sinkhole message dropping node).

Selvakumar *et al.* [99] proposed an intelligent IDS which was based on temporal reasoning, it used multi-class classification by a self-designed algorithm named "fuzzy and rough set based nearest neighbourhood algorithm (FRNN)''. The proposed framework had eight modules. It was used to reduce the complexity as it removed the redundant attributes and used Allen's intervals algebra operators.

Alaparthy and Morgera [100] designed a multilevel IDS for WSN environment based on the immune system concept of human body. Factors such as battery life, messages or data size, data transfer rate were used to perform the detection. In the proposed work few nodes were placed near the sink node as an immune node with some processing capabilities and then they formed a network among themselves to perform pathogen associated molecular pattern (PAMP) analysis to find the attack.

Sun *et al.* [101] proposed a multilevel IDS using the advantages of negative selection algorithm (NSA) and an improved V-detector algorithm to reduce the complications of resource constrained WSN. Principal component analysis (PCA) was used to reduce the dimensions of detecting features that further reduces the overall complexity of the system. The detection rate can be application specific which varies as per the location. The Gaussian distributed deployed sensor nodes can provide the differentiated detection capabilities at different locations. Therefore, Wang *et al.* [102] provided the analysis of problem of intrusion detection in a Gaussian-distributed WSN. The single sensing detection and multiple-sensing detection scenarios were considered. The performance of Gaussian-distributed WSNs was compared with the performance of uniformly distributed WSNs.

Wazid and Das [33], [34] also proposed a intrusion detection scheme for the detection of blackhole attacker nodes as well as for hybrid anomaly in WSN. The detection was done by resource rich cluster head nodes in an hierarchical wireless sensor network.

B. EXISTING INTRUSION DETECTION PROTOCOLS IN IoT

The summary of intrusion detection protocols in IoT is provided as follows. Jan *et al.* [103] implemented a light weighted IDS to mitigate the most common attack DOS in IoT, by considering a network of resource constrained nodes. They used packet transmission rate for the detection from which two-three features were extracted to reduce the overall time consumed to classify the traffic flow. That again reduces the complexity and time consumed by support vector machine (SVM) to classify and mitigate the DOS attack. However, the implemented work might not gave the desired result in the network which had steady traffic flow.

Sharma *et al.* [104] implemented a light weighted mechanism named as behaviour rule specification-based misbehaviour detection for IoT-embedded cyber-physical systems. It detected the presence of intruder through misbehaviour of an existing node in the network. A smart attacker can easily fail the rule-based system. Therefore, the use of such technique was avoided. In the proposed technique there was profiler which read the module and passed the information to fuzzy analysis module to check whether behaviour rules were valid or not. It then confirmed that behavior-rules were correct by making the use of ``2-layer fuzzy-based hierarchical context-aware aspect-oriented petri net (HCAPN) model''.

Pajouh *et al.* [105] proposed a IDS to detect multiple types of malicious attacks happened in a IoT environment. The designed method used two techniques to reduce the dimensions and minimize the number of features to be used. That made it less complex by using the principle component and linear discriminate analysis. Further they have used two classification techniques i.e., KNN and naive Bayes to detect the malicious activities.

Li *et al.* [106] designed a blockchain driven collaborative signature based intrusion detection system (CBSigIDS) for IoT. In a collaborative signature based IDS rules or signatures were used to detect malicious activity of the intruder. This information was shared with the other nodes of the network to update their data base and improve the intrusion detection rate. But at the same time chances of inside attack might increased because insider nodes provided the fake or malicious signature to degrade the performance of the collaborative IDS. Therefore, to resolve this problem a blockchain based method was used which utilized a very popular distributed database for the detection of the intrusions.

Breitenbacher *et al.* [107] proposed a lightweight host-based anomaly detection System used for IoT environment (HADES-IoT). It was a device-based, impeccable, proactive technique which could be deployed on the Linux based end-devices. The unique feature of this method was that it can be loaded in kernel of the operating system itself. That made it useful to be utilized this in Linux loadable kernel to install HADES-IoT in the Linux based end-devices.

Mudgerikar *et al.* [108] proposed a client system based IDS which used anomalies to detect the intruder called E-Spion. It had three layers of security with increasing level of security. But it had drawbacks as we increased the level of security that also caused the increment in the overhead. In the first module the system compared the name of ongoing running processes and their IDs with the whitelist prepared during the learning phase to separate the malicious process. In the second module they trained ML classifier from the logs generated during the learning phase and then it kept on monitoring the process parameters. The usage of machine learning techniques at the node level made it very expensive technique but it worked effectively.

Saeed *et al.* [109] proposed a IDS which worked in two phases to provide a secure system. In the first phase it used a random neural network model for an anomaly based IDS. In second phase a new tag system was introduced in the design where a tag was associated with the memory locations of the system. The tag-checking method was used to detect the anomalies in the system. Wazid *et al.* [66] also proposed intrusion detection schemes for detection of routing attack for edge-based IoT (EIoT) environment.

TABLE 3. Accuracy comparison of existing IDS techniques in WSN and IoT.

Scheme, Year	Technique used	Detection rate (DR) %	False positive rate (FPR) %	Applicable for WSN	Applicable for IoT
Wang *et al.* [96] (2008)	single-sensing and multiple-sensing detection models	83.00	N/A	✓	×
Wang *et al.* [97] (2011)	Integrated intrusion detection system (IIDS)	90.96	2.06	✓	×
Salehi *et al.* [98] (2013)	Intrusion detection by base station	93.00	10.00	✓	×
Wang *et al.* [102] (2013)	Gaussian versus uniform distribution for intrusion detection	86.00	N/A	✓	×
Wazid *et al.* [27] (2016)	Intrusion detection by cluster head	95.00	1.25	✓	✓
Wazid *et al.* [33] (2016)	Hybrid anomaly detection	98.60	1.20	✓	✓
Saeed *et al.* [109] (2016)	Random neural networks based intrusion detection	97.23	3.48	✓	✓
Wazid *et al.* [34] (2017)	Intrusion detection by cluster head	90.00	3.75	✓	✓
Alaparthy *et al.* [100] (2018)	Immune theory based multi-level intrusion detection	98.00	N/A	✓	×
Sun *et al.* [101] (2018)	Negative selection algorithm (NSA) based intrusion detection	99.50	N/A	✓	×
Wazid *et al.* [66] (2019)	Routing attack detection using edge node	95.00	1.23	✓	✓
Selvakumar *et al.* [99] (2019)	Fuzzy rough set-based feature selection algorithm for intrusion detection	99.87	0.13	✓	✓
Jan *et al.* [103] (2019)	support vector machine based intrusion detection	97.98	44.48	×	✓
Sharma *et al.* [104] (2019)	Behavior rule specification based misbehavior detection	97.80	4.00	×	✓
Pajouh *et al.* [105] (2019)	Two-tier classification model for intrusion detection	84.86	4.86	✓	✓
Mudgerikar *et al.* [108] (2019)	E-Spion a system-level intrusion detection	99.00	N/A	✓	✓

Note: N/A: not available

C. COMPARATIVE ANALYSIS OF EXISTING IDS IN WSN AND IoT

In this section we have compared the performance of various intrusion detection techniques for WSN and IoT. To measure the performance of a IDS we need to compute some performance parameters such as detection rate and false positive rate.

We compare the results of various IDS in WSN and IoT such as Wazid and Das [34], Wazid *et al.* [27], [66], Wang *et al.* [102], [96], [97], Salehi *et al.* [98], Selvakumar *et al.* [99], Alaparthy and Morgera [100], Sun *et al.* [101], Jan *et al.* [103], Sharma *et al.* [104], Pajouh *et al.* [105], Mudgerikar *et al.* [108], and Ahmed *et al.* [109].

The comparative analysis of various IDS schemes proposed in WSN and IoT environments are presented in Table 3. The following observations have been figured out:

- The "detection rate (DR)" for Salehi *et al.*'s scheme [98], Wang *et al.*'s scheme [97], Wang *et al.*'s scheme [102], Wang *et al.*'s scheme [96], Wazid *et al.*'s scheme [27], Wazid *et al.*'s scheme [66], Selvakumar *et al.* [99], Alaparthy and Morgera [100], Sun *et al.* [101] and Wazid and Das [34], Jan *et al.* [103], Sharma *et al.* [104], Pajouh *et al.* [105], Mudgerikar *et al.* [108], Saeed *et al.* [109] and Wazid *et al.*'s scheme [33] are 93.00, 90.96, 86.00, 83.00, 95.00, 95.00, 99.87, 98.00, 99.50, 90.00, 97.98, 97.80, 84.86, 99.00, 97.23 and 98.60 respectively.
- The "false positive rate (FPR)" for Salehi *et al.*'s scheme [98], Wang *et al.*'s scheme [97], Wazid *et al.*'s scheme [27], Wazid *et al.*'s scheme [66], Wazid *et al.* [34], Selvakumar *et al.* [99], Jan *et al.* [103], Sharma *et al.* [104], Pajouh *et al.* [105], Saeed *et al.* [109], and Wazid *et al.*'s scheme [33] are 10.00, 2.06, 1.25, 1.23, 0.13, 3.75, 44.48, 4.0, 4.86, 3.48 and 1.20 respectively.

Further note that the scheme of Wazid *et al.* [27], [34], [66], Selvakumar *et al.* [99], Pajouh *et al.* [105], Mudgerikar *et al.* [108], and Saeed *et al.* [109] are applicable for both WSN and IoT communication. For that purpose we need to do certain changes in their network model and configurations of nodes.

VII. FUTURE RESEARCH CHALLENGES AND DIRECTIONS IN WSN AND IoT

WSN and IoT-based communication environment offers wide variety of applications, such as smart home, smart transportation, smart healthcare and smart cities. Such kind of communication environment needs unique requirements such as real-time data processing and access (for example, real-time monitoring of an patient, environmental condition in an industrial plant, and so on). The data generated by IoT sensors is very huge in nature, and therefore, we can apply to big data analytic procedure on this data to find out certain pattern from this (for example, future health prediction of a patient). Such kind of communication environment is also a part of the Internet. Therefore, it suffers from traditional security, privacy, and other challenges. Among all these problems, intrusion detection in WSN and IoT is one of the critical problem of the domain on which several researchers are presently working. In the following part of the section, we discuss the current challenges for research and then through open discussions, we provide the details of future research directions of intrusion detection in WSN and IoT environment.

A. SECURITY OF INTRUSION DETECTION TECHNIQUES

Most of the intrusion detection techniques proposed for WSN and IoT are not secure as they do not provide full proof security against various types of attacks. Some of the proposed techniques in the literature are attack specific and do not work for multiple attacks at the same time. Therefore, we need to design such kind of intrusion detection techniques which should be robust and secure against multiple attacks at the same time. Designing of such kind of technique can be a challenging problem due to resource limitations of sensors and IoT devices.

B. EFFICIENCY OF INTRUSION DETECTION TECHNIQUES

In WSN and IoT-based communication environment, the WSN sensors and smart IoT sensors are resource constrained as they have less computation power and storage capacity along with short battery life. Hence, such devices can not perform computation, communication and storage intensive operations which need more strength in terms of such parameters. It is also recommended to use small size of messages during the intrusion detection process. The reason behind that is, it may consume other resources of devices which cause fast battery drainage of the sensors in sending and receiving bulky messages. Hence, we need to design intrusion detection techniques in such a way that the proposed technique should exhibit less computation costs, communication costs and storage cost without compromising the security of the technique [27], [34], [42].

C. SCALABILITY OF INTRUSION DETECTION TECHNIQUES

WSN integrated IoT is a kind of large scale heterogeneous network of various communication paradigms and applications which have their own capabilities and requirements. In that way, intrusion detection for such kind of communication environment will be a challenging task. We can have Electronic Health Records (EHRs) of certain users which are stored in an IoT-enabled cloud server for further processing. Various devices inside the Body Area Network (BANs) generate data and send it to the cloud. As a result, this creates a heterogeneous network of various communicating devices. Therefore, we need a specific type of intrusion detection technique which can protect all types of devices of such kind of communication environment. Henceforth, more deep investigation is required in this direction.

D. PRIVACY OF DATA MAINTAINED OVER CLOUD SERVER

The privacy of data explain how we should maintain the information over the various resources. The WSN integrated to IoT based communication is also used for information sensitive applications (for example, smart healthcare). In such privacy-demanding environment, smart health sensors are implanted or wrapped around the body of a patient to sense his/her health data and send the data to the cloud server(s) for storage and processing. As we know such kind of communication environment can be attacked by various types of intrusions [33], [34]. This further causes the disturbance in the transmission of data and also leakage of stored data. It then becomes important to maintain the privacy of data i.e., stored data and data in transit. Therefore, we require new efficient schemes which maintain privacy of the stored data and data in transit. Similarly, privacy-aware intrusion detection schemes should be designed for IoT environment in which device and/or user's privacy should be preserved.

E. HETEROGENEITY OF WSN AND IoT COMMUNICATION ENVIRONMENT

WSN and IoT-based communication environment differs in nature as we have different types of devices ranging from full-edged desktops, laptops, personal digital assistants to low powered sensing devices and low-end RFID tags. Furthermore, these devices work under the principles of different types of communication protocols. Here it also important to maintain that these devices are different in terms of their communication range, storage capacity, computation power and operating system. Therefore, we need to design an effective intrusion detection technique in such a way that it protects all different types of devices and associated technologies [34], [42].

F. CROSS-PLATFORM INTRUSION DETECTION

The heterogeneity of WSN and IoT environment causes problem when we plan to deploy some intrusion detection technique. The heterogeneity allows the interconnection of different application domains, but at the same time it also creates challenges for designing efficient intrusion detection process. For example, when a smart home application requires to access the data from a healthcare sensing device, the intrusion detection must be strong and compatible so that application should retrieve the data from the target network without any problem. However, it is worth to note that most of the time, data is stored over the cloud for which different intrusion mechanisms are required. Therefore, for such kind of applications we need efficient and strong intrusion detection techniques to provide a seamless connectivity across the various IoT platforms [42], [110].

VIII. CONCLUDING REMARKS

In this survey article, we have discussed the security requirements and various attacks possible in WSN and IoT based communication environments. The emerging projects of WSNs integrated to IoT are then summarized. The details of various architectures of WSN and IoT are also provided. We have provided a taxonomy of existing intrusion detection schemes related to WSN and IoT-based communication environments. Furthermore, we have provided the comparisons of intrusion detection schemes of WSN and IoT. Various comparisons such as detection rate, false positive rate and the applicability of the state-of-art schemes are conducted. Finally, we have identified some future research challenges in the design of intrusion detection schemes and other security protocols for WSN and IoT-based communication environments.

ACKNOWLEDGMENT

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

REFERENCES

[1] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018.

[2] A. Raoof, A. Matrawy, and C.-H. Lung, "Routing attacks and mitigation methods for RPL–based Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1582–1606, 2019.

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

[4] R. Chowdhury. (2019). *Top 20 Best Internet of Things Projects (IoT Projects) That You Can Make Right Now*. Accessed: Oct. 2019. [Online]. Available: https://www.ubuntupit.com/best-internet-of-things-projects-iot-projects-that-you-can-make-right-now/

[5] *Air Pollution Diseases*. Accessed: Oct. 2019. [Online]. Available: https://www.environmentalpollutioncenters.org/air/diseases/

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

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

[8] 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.

[9] 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.

[10] 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, doi: 10.1109/jiot.2019.2923611.

[11] M. Wazid, A. K. Das, N. Kumar, V. Odelu, A. G. Reddy, K. Park, and Y. Park, "Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks," *IEEE Access*, vol. 5, pp. 14966–14980, 2017.

[12] H. Larthani, A. Zrelli, and T. Ezzedine, "On the detection of disasters: Optical sensors and IoT technologies," in *Proc. Int. Conf. Internet Things, Embedded Syst. Commun. (IINTEC)*, Hammamet, Tunisia, Dec. 2018, pp. 142–146.

[13] A. H. Farooqi and F. A. Khan, "A survey of intrusion detection systems for wireless sensor networks," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 9, no. 2, pp. 69–83, 2012.

[14] A. R. Dhakne and P. N. Chatur, "A comprehensive survey on intrusion detection systems in wireless sensor network," in *Smart Trends in Information Technology and Computer Communications*, vol. 628. Singapore: Springer, 2016, pp. 541–549.

[15] B. B. Zarpelão, R. S Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, Apr. 2017.

[16] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: A survey," *J. Cloud Comput.*, vol. 7, no. 1, p. 21, Dec. 2018.

[17] Z. A. Khan and P. Herrmann, "Recent advancements in intrusion detection systems for the Internet of Things," *Secur. Commun. Netw.*, vol. 2019, pp. 1–19, Jul. 2019, doi: 10.1155/2019/4301409.

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

[19] G. Writer. (2018). *IoT Applications in Agriculture*. Accessed: Oct. 2019. [Online]. Available: https://www.iotforall.com/iot-applications-in-agriculture/

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

[21] 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.

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

[23] S. Chatterjee and A. K. Das, "An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks," *Secur. Commun. Netw.*, vol. 8, no. 9, pp. 1752–1771, Jun. 2015.

[24] A. K. Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," *Peer-to-Peer Netw. Appl.*, vol. 9, no. 1, pp. 223–244, Jan. 2016.

[25] A. K. Das, "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," *Int. J. Commun. Syst.*, vol. 30, no. 1, Jan. 2017, Art. no. e2933.

[26] A. K. Das, "A secure and efficient user anonymity–preserving three–factor authentication protocol for large–scale distributed wireless sensor networks," *Wireless Pers. Commun.*, vol. 82, no. 3, pp. 1377–1404, Jun. 2015.

[27] 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.

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

[29] 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.

[30] 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.

[31] T. Messerges, E. Dabbish, and R. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.

[32] J. Ryoo, D.-G. Han, S.-K. Kim, and S. Lee, "Performance enhancement of differential power analysis attacks with signal companding methods," *IEEE Signal Process. Lett.*, vol. 15, pp. 625–628, Oct. 2008.

[33] 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.

[34] 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.

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

[36] S. Zeadally, A. K. Das, and N. Sklavos, "Cryptographic technologies and protocol standards for Internet of Things," *Internet Things*, to be published. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2542660519301799

[37] 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. Amsterdam, The Netherlands: Elsevier, 2019, pp. 371–395.

[38] 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.

[39] 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.

[40] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M. A. Latif, F. Al-turjman, and L. Mostarda, "Cyber security threats detection in Internet of Things using deep learning approach," *IEEE Access*, vol. 7, pp. 124379–124389, 2019.

[41] A. Mahboubi, S. Camtepe, and H. Morarji, "A study on formal methods to generalize heterogeneous mobile malware propagation and their impacts," *IEEE Access*, vol. 5, pp. 27740–27756, 2017.

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

[43] 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.

[44] I. Medeiros, M. Beatriz, N. Neves, and M. Correia, "SEPTIC: Detecting injection attacks and vulnerabilities inside the DBMS," *IEEE Trans. Rel.*, vol. 68, no. 3, pp. 1168–1188, Sep. 2019.

[45] J. Fonseca, M. Vieira, and H. Madeira, "Evaluation of Web security mechanisms using vulnerability & attack injection," *IEEE Trans. Depend. Sec. Comput.*, vol. 11, no. 5, pp. 440–453, Sep. 2014.

[46] D. Mitropoulos, P. Louridas, M. Polychronakis, and A. D. Keromytis, "Defending against Web application attacks: Approaches, challenges and implications," *IEEE Trans. Depend. Sec. Comput.*, vol. 16, no. 2, pp. 188–203, Mar. 2019.

[47] M. Wazid, "Design and analysis of intrusion detection protocols for hierarchical wireless sensor networks," Ph.D. dissertation, Center Secur., Theory Algorithmic Res., Int. Inst. Inf. Technol., Hyderabad, India, 2017.

[48] U.S. Department of Commerce. (Apr. 1995). *Secure Hash Standard, FIPS PUB 180-1, National Institute of Standards and Technology (NIST)*. Accessed: Oct. 2019. [Online]. Available: http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

[49] U.S. Department of Commerce. (2001). *National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES)*. Accessed: Oct. 2019. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf

[50] 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.

[51] J. Yoo and H. Kim, "Target localization in wireless sensor networks using online semi–supervised support vector regression," *Sensors*, vol. 15, no. 6, pp. 12539–12559, May 2015.

[52] S. Kumar, S. N. Tiwari, and R. M. Hegde, "Sensor node tracking using semi-supervised hidden Markov models," *Ad Hoc Netw.*, vol. 33, pp. 55–70, Oct. 2015.

[53] H. Geng, Y. Liang, F. Yang, L. Xu, and Q. Pan, "Model-reduced fault detection for multi-rate sensor fusion with unknown inputs," *Inf. Fusion*, vol. 33, pp. 1–14, Jan. 2017.

[54] R. R. Swain, P. M. Khilar, and S. K. Bhoi, "Heterogeneous fault diagnosis for wireless sensor networks," *Ad Hoc Netw.*, vol. 69, pp. 15–37, Feb. 2018.

[55] R. Palanikumar and K. Ramasamy, "Effective failure nodes detection using matrix calculus algorithm in wireless sensor networks," *Cluster Comput.*, vol. 22, no. S5, pp. 12127–12136, Sep. 2019.

[56] S. Zidi, T. Moulahi, and B. Alaya, "Fault detection in wireless sensor networks through SVM classifier," *IEEE Sensors J.*, vol. 18, no. 1, pp. 340–347, Jan. 2018.

[57] W. Wang, S. Jiang, H. Zhou, M. Yang, Y. Ni, and J. Ko, "Time synchronization for acceleration measurement data of jiangyin bridge subjected to a ship collision," *Struct. Control Health Monit.*, vol. 25, no. 1, Jan. 2018, Art. no. e2039.

[58] K.-P. Ng, C. Tsimenidis, and W. L. Woo, "C–Sync: Counter-based synchronization for duty-cycled wireless sensor networks," *Ad Hoc Netw.*, vol. 61, pp. 51–64, Jun. 2017.

[59] Y.-P. Tian, "Time synchronization in WSNs with random bounded communication delays," *IEEE Trans. Automat. Contr.*, vol. 62, no. 10, pp. 5445–5450, Oct. 2017.

[60] D. Capriglione, D. Casinelli, and L. Ferrigno, "Analysis of quantities influencing the performance of time synchronization based on linear regression in low cost WSNs," *Measurement*, vol. 77, pp. 105–116, Jan. 2016.

[61] A. Davis, "A survey of wireless sensor network architectures," *Int. J. Comput. Sci. Eng. Surv.*, vol. 3, no. 6, pp. 1–22, Dec. 2012.

[62] S. Vishwakarma, "An analysis of LEACH protocol in wireless sensor network: A survey," *Int. J. Comput. Sci. Eng. Surv.*, vol. 6, no. 3, pp. 148–154, 2015.

[63] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[64] S. Xu, G. Yang, Y. Mu, and X. Liu, "A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance," *Future Gener. Comput. Syst.*, vol. 97, pp. 284–294, Aug. 2019.

[65] 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.

[66] M. Wazid, P. Reshma Dsouza, A. K. Das, V. Bhat K, 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.

[67] 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.

[68] 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.

[69] J. Li, X. Chen, M. Li, J. Li, P. P. 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.

[70] 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.

[71] 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.

[72] 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.

[73] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Symp. Security Privacy*, Berkeley, CA, USA, May 2003, pp. 197–213.

[74] 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.

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

[76] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 740. Berlin, Germany: Springer, 1993, pp. 471–486.

[77] Y. Cheng and D. P. Agrawal, "Efficient pairwise key establishment and management in static wireless sensor networks," in *Proc. 2nd IEEE Int. Conf. Mobile Ad Hoc Sensor Syst.*, Washington, DC, USA, Nov. 2005, p. 550.

[78] D. Liu, P. Ning, and W. Du, "Group-based key predistribution for wireless sensor networks," in *Proc. ACM Workshop Wireless Secur. (WiSe)*, Sep. 2005, pp. 1–10.

[79] 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.

[80] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Trans. Sen. Netw.*, vol. 2, no. 4, pp. 500–528, Nov. 2006.

[81] 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.

[82] 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.

[83] 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.

[84] 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.

[85] 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.

[86] (2016). *X.509: Information Technology—Open Systems Interconnection—The Directory: Public-Key and Attribute Certificate Frameworks*. [Online]. Available: https://www.itu.int/rec/T-REC-X.509

[87] Y. Hong, W. M. Liu, and L. Wang, "Privacy preserving smart meter streaming against information leakage of appliance status," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 9, pp. 2227–2241, Sep. 2017.

[88] M. Wazid, S. Zeadally, A. K. Das, and V. Odelu, "Analysis of security protocols for mobile healthcare," *J. Med. Syst.*, vol. 40, no. 11, p. 229, Nov. 2016.

[89] M. Badra and S. Zeadally, "Design and performance analysis of a virtual ring architecture for smart grid privacy," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 321–329, Feb. 2014.

[90] S. Zeadally, A.-S.-K. Pathan, C. Alcaraz, and M. Badra, "Towards privacy protection in smart grid," *Wireless Pers. Commun.*, vol. 73, no. 1, pp. 23–50, Nov. 2013.

[91] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, "Privacy preservation in wireless sensor networks: A state-of-the-art survey," *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1501–1514, Nov. 2009.

[92] N. Sharma and R. Bhatt, "Privacy preservation in WSN for healthcare application," *Procedia Comput. Sci.*, vol. 132, pp. 1243–1252, Jan. 2018.

[93] M. Yamin, Y. Alsaawy, A. B. Alkhodre, and A. A. A. Sen, "An innovative method for preserving privacy in Internet of Things," *Sensors*, vol. 19, no. 15, p. 3355, Jul. 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/15/3355

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

[95] E. Darra and S. K. Katsikas, "A survey of intrusion detection systems in wireless sensor networks," *Intrusion Detection Prevention Mobile Ecosyst.*, pp. 393–458, Sep. 2017.

[96] Y. Wang, X. Wang, B. Xie, D. Wang, and D. Agrawal, "Intrusion detection in homogeneous and heterogeneous wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 7, no. 6, pp. 698–711, Jun. 2008.

[97] S.-S. Wang, K.-Q. Yan, S.-C. Wang, and C.-W. Liu, "An integrated intrusion detection system for cluster-based wireless sensor networks," *Expert Syst. Appl.*, vol. 38, no. 12, pp. 15234–15243, Nov. 2011.

[98] S. A. Salehi, M. A. Razzaque, P. Naraei, and A. Farrokhtala, "Detection of sinkhole attack in wireless sensor networks," in *Proc. IEEE Int. Conf. Space Sci. Commun. (IconSpace)*, Malacca, Malaysia, Jul. 2013, pp. 361–365.

[99] 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.

[100] V. T. Alaparthy and S. D. Morgera, "A multi–level intrusion detection system for wireless sensor networks based on immune theory," *IEEE Access*, vol. 6, pp. 47364–47373, 2018.

[101] Z. Sun, Y. Xu, G. Liang, and Z. Zhou, "An intrusion detection model for wireless sensor networks with an improved V–detector algorithm," *IEEE Sensors J.*, vol. 18, no. 5, pp. 1971–1984, Mar. 2018.

[102] Y. Wang, W. Fu, and D. P. Agrawal, "Gaussian versus uniform distribution for intrusion detection in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 2, pp. 342–355, Feb. 2013.

[103] 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.

[104] 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.

[105] 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.

[106] W. Li, S. Tug, W. Meng, and Y. Wang, "Designing collaborative blockchained signature-based intrusion detection in IoT environments," *Future Gener. Comput. Syst.*, vol. 96, pp. 481–489, Jul. 2019.

[107] D. Breitenbacher, I. Homoliak, Y. L. Aung, N. O. Tippenhauer, and Y. Elovici, "HADES-IoT: A practical host-based anomaly detection system for IoT devices," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, Auckland, New Zealand, 2019, pp. 479–484.

[108] 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.*, Auckland, New Zealand, 2019, pp. 493–500.

[109] A. Saeed, A. Ahmadinia, A. Javed, and H. Larijani, "Intelligent Intrusion Detection in Low–Power IoTs," *ACM Trans. Internet Technol.*, vol. 16, no. 4, pp. 1–25, Dec. 2016.

[110] EBU Tech. *Cross-Platform Authentication*. Accessed: Oct. 2019. [Online]. Available: https://tech.ebu.ch/groups/CPA

SUMIT PUNDIR received the M.Tech. degree in computer science engineering from Uttarakhand Technical University, Dehradun, India, in 2009. He is currently pursuing the Ph.D. degree in computer science and engineering with the Graphic Era Deemed to be University, Dehradun. His research interests include information security, the Internet of Things (IoT), and wireless sensor networks. He has published 12 articles in national and international conferences in these research areas.

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

DEVESH PRATAP SINGH received the M.Tech. degree in computer science and engineering and the Ph.D. degree from Uttarakhand Technical University, Dehradun, India, in 2009 and 2015, respectively. He is currently a Professor and the Head of the Computer Science and Engineering Department, Graphic Era Deemed to be University, Dehradun. His research interests include information security, wireless sensor networks, the Internet of Things, and soft computing. He has published more than 50 research articles in his area of expertise. He is also a member of the ACM.

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 current research interests include cryptography, network security, blockchain, security in the Internet of Things (IoT), the Internet of Vehicles (IoV), the Internet of Drones (IoD), smart grids, smart city, cloud/fog computing and industrial wireless sensor networks, and intrusion detection. He has authored over 200 articles in international journals and conferences in these areas, including over 175 reputed journal articles. Some of his research findings are published in top cited journals, such as the IEEE Transactions on Information Forensics and Security, the IEEE Transactions on Dependable and Secure Computing, the IEEE Transactions on Smart Grid, the IEEE Internet of Things Journal, the IEEE Transactions on Industrial Informatics, the IEEE Transactions on Vehicular Technology, the IEEE Transactions on Consumer Electronics, the IEEE Journal of Biomedical and Health Informatics (formerly the IEEE Transactions on Information Technology in Biomedicine), the *IEEE Consumer Electronics Magazine*, the IEEE Access, the *IEEE Communications Magazine*, *Future Generation Computer Systems*, *Computers & Electrical Engineering*, *Computer Methods and Programs in Biomedicine*, *Computer Standards & Interfaces*, *Computer Networks*, *Expert Systems With Applications*, and the *Journal of Network and Computer Applications*. He has served as a Program Committee Member for many international conferences. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He has severed as one of the Technical Program Committee Chairs of the International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, in June 2019. He is on the Editorial Board of the *KSII Transactions on Internet and Information Systems*, the *International Journal of Internet Technology and Secured Transactions* (Inderscience), and the *IET Communications*. He is also a Guest Editor of *Computers & Electrical Engineering* (Elsevier) for the special issue on Big Data and the IoT in e-Healthcare and the *ICT Express* (Elsevier) for the special issue on Blockchain Technologies and Applications for 5G Enabled IoT.

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 also the Leader of the Next Generation Networks and Applications Research Group (CNPq). He has authored or coauthored over 800 articles in refereed international journals and conferences, three books, two patents, and one ITU-T Recommendation. He is also the Director for Conference Development of the IEEE ComSoc Board of Governors, the IEEE Distinguished Lecturer, the Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, the President of the Scientific Council at ParkUrbis—Covilhã Science and Technology Park, the Past-Chair of the IEEE ComSoc Technical Committee on eHealth and the IEEE ComSoc Technical Committee on Communications Software, a Steering Committee Member of the IEEE Life Sciences Technical Community, the Publications Co-Chair, and a Member Representative of the IEEE Communications Society on the IEEE Biometrics Council. He is also a member of the Internet Society and a Senior Member of the ACM. He had been awarded several Outstanding Leadership and Outstanding Service Awards by the IEEE Communications Society and several best papers awards. He has been the General Chair and the TPC Chair of many international conferences, including the IEEE ICC, IEEE GLOBECOM, IEEE HEALTHCOM, and IEEE LatinCom. He 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.

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