IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 9, 2021, accepted June 4, 2021, date of publication June 10, 2021, date of current version June 29, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3088225

Sensor-Cloud Architecture: A Taxonomy of Security Issues in Cloud-Assisted Sensor Networks

RYAN ALTURKI[1], HASAN JUMAILI ALYAMANI[2], MOHAMMED ABDULAZIZ IKRAM[3], MD ARAFATUR RAHMAN[4], (Senior Member, IEEE), MOHAMMAD DAHMAN ALSHEHRI[5], FAZLULLAH KHAN[6], (Senior Member, IEEE), AND MUHAMMAD HALEEM[7]

[1]Department of Information Science, College of Computer and Information Systems, Umm Al-Qura University, Makkah 24372, Saudi Arabia
[2]Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Rabigh 25732, Saudi Arabia
[3]Department of Computer Science, University College in Al-Jamoum, Umm Al-Qura University, Makkah 24372, Saudi Arabia
[4]School of Mathematics and Computer Science, University of Wolverhampton, Wolverhampton WV1 1LY, U.K.
[5]Department of Computer Science, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia
[6]Department of Computer Science, Abdul Wali Khan University Mardan, Mardan 23200, Pakistan
[7]Department of Computer Science, Faculty of Engineering and Technology, Kardan University, Kabul 1003, Afghanistan

Corresponding authors: Ryan Alturki (rmturki@uqu.edu.sa) and Fazlullah Khan (fazlullah@awkum.edu.pk)

This work was supported by the Taif University, Taif, Saudi Arabia, through the Taif University Researchers Supporting Project under Grant TURSP-2020/126.

ABSTRACT The orchestration of cloud computing with wireless sensor network (WSN), termed as sensor-cloud, has recently gained remarkable attention from both academia and industry. It enhances the processing and storage capabilities of the resources-constrained sensor networks in various applications such as healthcare, habitat monitoring, battlefield surveillance, disaster management, etc. The diverse nature of sensor network applications processing and storage limitations on the sensor networks, which can be overcome through integrating them with the cloud paradigm. Sensor-cloud offers numerous benefits such as flexibility, scalability, collaboration, automation, virtualization with enhanced processing and storage capabilities. However, these networks suffer from limited bandwidth, resource optimization, reliability, load balancing, latency , and security threats. Therefore, it is essential to secure the sensor-cloud architecture from various security attacks to preserve its integrity. The main components of the sensor-cloud architecture which can be attacked are: (i) the sensor nodes; (ii) the communication medium; and (iii) the remote cloud architecture. Although security issues of these components are extensively studied in the existing literature; however, a detailed analysis of various security attacks on the sensor-cloud architecture is still required. The main objective of this research is to present state-of-the-art literature in the context of security issues of the sensor-cloud architecture along with their preventive measures. Moreover, several taxonomies of the security attacks from the sensor-cloud's architectural perspective and their innovative solutions are also provided.

INDEX TERMS Sensor-cloud architecture, security, wireless sensor networks, Internet of Things.

I. INTRODUCTION

A wireless sensor network consists of a large number of miniature sensor nodes that capture a large amount of data from the sensing field. Forwarding such a large amount of raw data across the network exposes them to a plethora of challenges such as low quality of service (QoS), i.e., latency, congestion, throughput, and security in these resource-constrained networks. They have limited memory, processing, communication, and most importantly, limited irreplaceable source of energy supply. To overcome the aforementioned limitations, the wireless network is integrated with cloud computing forming a new computing paradigm known as sensor-cloud. Sensor-cloud can be defined as an infrastructure that allows truly pervasive computation using sensors as an interface between the physical and the cyber world and the Internet as the communication medium [1]–[3]. Sensor-cloud overcomes various limitations of the sensor networks as well as enhancing the lifetime of the network. In the sensor-cloud, most of the resources-intensive tasks

The associate editor coordinating the review of this manuscript and approving it for publication was A. Taufiq Asyhari.

FIGURE 1. Applications of wireless sensor networks.

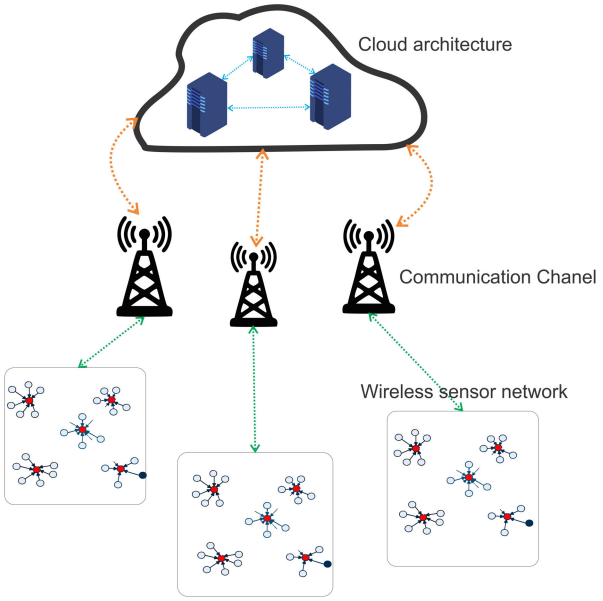

FIGURE 2. Sensor-cloud architecture.

such as processing, storage, and data aggregation are transferred from the resource-constrained sensor networks to the cloud architecture [4].

This improves QoS, enhances network lifetime, and facilitates users to gather, store, access, process, visualize and analyze a large amount of sensory data easily using enriched cloud computing resources. Currently, WSNs are being utilized in several areas like healthcare, defence such as military target tracking and surveillance [5], [6], government and environmental services like natural disaster relief [7], hazardous environment exploration [8], [9], and seismic sensing [10], as depicted in Figure. 1, where data captured by the sensors is forwarded to the cloud infrastructure for further processing.

Although, sensor-cloud offer many advantages such as flexibility, scalability, collaboration, automation virtualization with enhanced processing and storage capabilities, and so forth. However, at the same time suffer from various limitations, such as resource scheduling, Quality of Service, load balancing, and most importantly, security and privacy [11]–[14]. A lot of work has been done to address these issues. However, research on the security, privacy, and trust in the sensor-cloud architecture is limited in the relevant literature. According to [15], 49 % of the businesses are delaying the deployment of the sensor-cloud due to security concerns. Thus, security remains a key concern hindering the widespread adoption of the sensor-cloud.

The main components of the sensor-cloud are sensors, communication medium, and cloud architecture, where each component is responsible for a specific task. For instance, secure pre-processing (deployment of sensors in the sensing field) performing smart sensing and data processing. The communication channel acts as a bridge between the sensors and the cloud architecture, facilitating secure data communication. Finally, the cloud's secure runtime services are provided in the sensor-cloud architecture, as shown in Figure. 2.

Despite the importance of these components, they suffer from various security threats [16]–[19]. This paper aims to present a comprehensive review of various security attacks on these individual components and their countermeasures. It is imperative to protect and secure this architecture vertically from the bottom, i.e., the sensor node to the communication channel. Finally, the cloud of the sensor-cloud architecture. Although a lot of work is available that investigates each component of this architecture's security issues, none of them study security attacks from the perspective of the sensor-cloud architecture with their countermeasures. The main objectives of our research conducted in this paper, are as follows:

1) the importance of security study in the sensor-cloud architecture;
2) sate-of-the-art security and privacy in the sensor-cloud architecture;
3) a taxonomy of security attacks and their countermeasures from the architectural perspective;
4) security attacks on the sensor node, wireless communication channel, and the cloud architecture and their countermeasures; and
5) research challenges ahead.

The rest of this paper is organized as follows. In Section II, we discuss the importance of security in the sensor-cloud platforms; and various reasons for carrying out this research work. In Section III, a detailed overview of the literature is provided, along with highlighting the novelty and contributions of our paper. Next, we discuss various security attacks and their countermeasures from an architectural perspective,

i.e., on the sensors, on the communication channel, and the cloud architecture in Section IV. Similarly, Section V provide a brief discussion on various innovative solutions for tackling security challenges discussed previously. Finally, limitations and future research directions are highlighted in Section VI.

II. MOTIVATION

Recently, the sensor-cloud architecture becomes very popular due to its virtual nature. It facilitates efficient and real-time information sharing among multiple users, dynamic resource management, which, in turn, increases resource utilization. It also enhances the storage and processing capabilities of the traditional sensor network. All these features make this multi-user, multi-applications environment a suitable choice for the real-time decision support system. However, the distributed and virtual nature of the sensor-cloud and a diverse range of stockholders expose this architecture to various challenges. A lot of research work is available in the literature that studies sensor-cloud from various perspectives to address these challenges. However, most of them considered security of the individual component in case of security and are thus limited in their scope. This paper extends the previous work presented in [2]. The proposed work presents a novel sensor-cloud architecture, defining its various components and their relationships. It divides the sensor-cloud architecture vertically into three layers, i.e., sensor-centric, middleware, and client-centric. However, this work lacks security issues facing the overall architecture. This survey enhances previous research work by considering emerging security and privacy issues from the architectural perspective from the lower to the higher layers, i.e., sensors, the communication channel, and the cloud architecture, to fill the gap that exists in the current literature [20], [21].

III. RELATED WORK

The orchestration between the sensors and the cloud architecture with the help of a communication network, also known as sensor-cloud gain momentum in recent years. As stated earlier, the main components of the sensor-cloud are; sensors, the communication medium, and cloud computing. A lot of research work is conducted recently that explores the security issues of each component of this architecture. For instance Wireless sensor networks and security [22]–[29], Secure data communication [30]–[33], and cloud computing and security [34]–[41]. Security in the wireless sensor network is extensively studied. In this regard, the authors in [22], [42] present various security threats and vulnerabilities that occur at various layers of the sensor networks. Moreover, a detailed survey of various security attacks is investigated, and their countermeasures are provided from the latest research. Moreover, the authors also provided a detailed survey of data aggregation techniques and energy-efficient routing protocols. Finally, emerging security issues are also discussed. Similarly, the authors in [23], [43] explore various security issues in the WSN such as IEEE 802.15.4, Berkeley media access control for low-power sensor networks, IPv6 over low-power wireless personal area networks, routing protocols for low-power and lossy networks (RPL), back pressure collection protocol, collection tree protocols, and constrained application protocol for WSN. Moreover, their countermeasures are also provided in this paper. Furthermore, future research directions are also provided at the network layer in order to protect it against various security attacks [44]–[46].

Likewise, the major security aspects of WSNs are outlined in [28]. They classify security attacks as well as their countermeasures. The paper delineates various research challenges and outlines future research directions in this specific domain. Moreover, security attacks such as physical attacks, good and bad-mouthing attacks, and on-off attacks related to the networking layer of the WSN, along with privacy, secrecy, and authentication, are explored in detail in [25], [47], [48]. Another similar work that study routing layer attacks for a better understanding of intrusion detection system in the sensor networks is presented in [26]. Their investigation is based on the analysis of information gathered both from the Sink and victim node. The degree of attack in these networks depends on factors such topology of WSN and the distance from the Sink. Furthermore, the work in [27] investigates the security of the sensor networks in a wide range of applications and scenarios. Moreover, a comprehensive discussion on the current and future security issues in these diverse applications is also provided in this paper.

Similarly, a lot of research work is proposed in the literature that studies security in cloud architecture. In [34], [49], the authors mainly focus on four types of attacks. They are; network-based attacks, VM-based attacks, storage-based attacks, and application-based attacks. Moreover, various countermeasures of these attacks are also provided. Furthermore, novel, innovative, and promising security solutions by modifying the system's configuration are also presented. Similarly, the authors in [35] present a parametric comparison of threats faced by the cloud platform along with possible solutions from the literature. Moreover, various intrusion detection mechanisms are also considered, along with future research directions. Likewise, [36] explore various threats faced by the cloud architecture. It devises a threat identification mechanism that systematically identifies potential threats using the Microsoft STRIDE threat modeling approach in a cloud computing architecture. Another paper studying privacy and security in the cloud architecture is presented in [38]. Moreover, it provides updated and latest practices tackling and avoiding these attacks. It identifies 28 cloud security threats and grouped them into five categories and a detailed discussion by considering up to nine attacks on this architecture. Finally, the paper concludes with limitations and future research directions for further exploration. Similarly, in [40] the authors provide a brief overview on various cloud components, their security issues, risks, along with emerging solutions that may potentially mitigate the vulnerabilities in this architecture. The authors stress that more work to be done to secure the cloud architecture to make it a mature platform for the larger interest of stakeholders.

Another landmark work that identifies security and privacy issues in the cloud architecture along with the latest solutions and their limitations is presented in [41], [50]. Moreover, future research directions are also provided. Finally, a taxonomy of the security attacks that threaten various services and their mitigating solutions on the cloud architecture is provided in [51]. It also provides various open issues and proposes future research directions, particularly from different stakeholders' perspectives, i.e., cloud service providers, data owners, and cloud users.

Apart from the research work that focuses on either edge of the network, the communication channel, or the cloud architecture, some research work is targeting various perspectives of the sensor-cloud architecture. These include concept and architecture [1], and the concept of physical sensors and services virtualization [52]. A detailed discussion on semantically rich service-oriented architecture (SOA) is presented in [53]. Moreover, a theoretical model of the sensor-cloud is presented in [54] and is also validated mathematically. In [2] the authors present an architecture for sensor-cloud which define various components of the protocol stack and their relationship with both the physical sensors and users. Apart from this sensor-cloud is studied from various application perspectives such as, patient data privacy and security in smart health care [55], smart data collection in the sensor-cloud [56]–[59], secure Communication [60], [61], and secure data collection in the sensor-cloud architecture [62]. All these techniques are summarized in the tabular form in the Table. 1.

IV. SECURITY AND PRIVACY ISSUES IN THE SENSOR-CLOUD

The sensor-cloud is a computing paradigm, which facilitates resource sharing and provides a platform to integrate different sensor networks. In these networks, multiple users can build their sensing applications simultaneously without worrying about the traditional limitations of the sensor network. It enables a multi-user on-demand sensory system, where computing, sensing, and network resources are shared among multiple users and applications. Despite the benefits of sensor-clouds, the security issue is open mainly because the masses can access this infrastructure for different purposes. Therefore, it has the inherent challenge of lacking security and privacy issues across the sensor-cloud infrastructure. Although new threats are emerging in this architecture, However, the existing security solutions of stand-alone sensor networks or cloud architecture are infeasible for the sensor-cloud architecture, requiring innovative solutions. Based on the unique security challenges discussed above, in this section, we present a taxonomy of cybersecurity attacks along with their countermeasures on the three components of the sensor-cloud architecture, which are; sensors, the communication channel, and the cloud framework (as shown in Figure 3). These aspects and additional details are further described in the following subsections.

1) **secure the sensor node**
2) **secure communication or wireless channel**
   - **secure data collection at the sensor node**
   - **secure data transmission on the communication or wireless channel**
3) **secure data at the cloud platform**

A. SECURE THE SENSOR NODE

A sensor node can either be physically secured or through the use of authorization and authentication techniques. In the former one, access control mechanisms restrict remote access to the geographical area where sensor nodes are deployed (physical). In the latter one (logical), various authentication techniques are used to authorize and give access only to appropriate and authorized users, or other nodes to these sensors [63]. Moreover, communication between sensors can also be secured using certain security protocols.

B. SECURE THE COMMUNICATION CHANNEL

Security of the communication channel can be divided into two different types: (i) attacks and countermeasures during data collection at the sensor node; and (ii) attacks and countermeasures during secure data transmission on the wireless channel.

1) ATTACKS AND COUNTERMEASURES DURING DATA COLLECTION AT THE SENSOR NODE

1) **device tempering attacks**
2) **eavesdropping**
3) **jamming attacks**
4) **denial of service (DoS) attacks**

a: DEVICE TAMPERING ATTACKS

In the device tampering attacks, the real node is modified into a fake node in such a way that facilitates the attackers to access sensitive and confidential information passing through it or stored within the buffer of the node. Device tampering attacks also result in selective message eavesdropping attacks, which act as a base for launching other serious security attacks such as wormhole and black-hole attacks. The device tempering attacks can be avoided using various tempering proof techniques [66]–[68] proposed in the literature however require additional energy and processing costs.

b: JAMMING ATTACKS

In jamming attacks, the perpetrator tries to interrupt the normal operation of the sensor nodes as well as of the network using a strong jamming source. The jamming source transmits radio signals using the same frequency as the sensor network. It thus adversely affects the communication among various entities of a sensor network. As a result, there is no exchange of messages in the network due to such interference by the attackers [69], [70]. Depends on the jamming source, it may either be strong or weak [63], [71]. In the case of a strong jamming source, it can affect all activities

TABLE 1. Summary of the state-of-the-art related works in the field of secure IoT, cloud computing, fog architecture, and physical sensor devices.

Ref.	Description	Pros	Cons
[22]	Security threats and their countermeasures, data aggregation, energy-efficient routing protocols, and emerging security solutions	Comprehensive analysis of security threats and their countermeasures in WSN	Only consider WSN security
[23]	Detail discussion on IEEE 802.15.4, Berkeley media access control for low-power sensor networks, IPv6 over low-power wireless personal area networks, routing protocols for low-power and lossy networks (RPL), back pressure collection protocol, collection tree protocols, and constrained application protocol for WSN along with their countermeasures.	Security issues and their countermeasures in various WSN protocols.	Exclusively consider WSN security
[28]	Classify security attacks and countermeasures	Delineate various research challenges and outline future research directions	WSN domain only
[25]	Security attacks such as physical attacks, good and bad-mouthing attacks, and on-off attacks at the network layer of the WSN.	WSN attacks along with privacy, secrecy, and authentication.	WSN exclusive
[26]	intrusion detection system in the sensor networks	IDS in WSN	WSN
[27]	Investigate the security of the sensor networks in a wide range of applications and scenarios.	Discuss the current and future security issues in a diverse range of applications	WSN
[34]	Four types of attacks and their countermeasures on the Cloud environment.	Attacks and countermeasures in the cloud environment.	Limited in its scope targeting cloud environment
[35]	Threats faced by the cloud platform, intrusion detection possible solutions, and future research directions	Study various security threats and mitigation techniques	cloud environment, not updated
[36]	Security threat identification using Microsoft STRIDE threat modelling approach	Methods that systematically identify potential threats	Consider only cloud architecture
[38]	Identify 28 cloud security threats and grouped them into five categories as well as a detailed discussion by considering up to nine attacks on this architecture.	Grouping of security threats for the convenience of the readers	Cloud environment
[40]	brief overview on various cloud components, their security issues, risks, along with emerging solutions that may potentially mitigate the vulnerabilities	Attacks and their mitigation strategies	exclusively consider the cloud paradigm
[41]	security and privacy issues in the cloud architecture	detailed and updated work studying security and privacy issues	Cloud environment
[51]	Taxonomy of the security attacks from different stakeholders, open issues and future research directions	Security issues from the perspective of various stockholders, i.e., the data owners, and the cloud users.	Cloud environment
[55]	sensor-cloud architecture such as patient data privacy and security in smart health care	Only consider security issues in health sector	sensor-cloud security in smart health care
[56]	Latest and comprehensive study related to the data collection in the sensor-cloud	WSN and their applications	Discus data collection and only a portion is dedicated to the security of the sensor-cloud in both these papers
[57]	present systematic work on data collection in the sensor-cloud	–	ignore security during data collection
[60]	The latest research related to secure communication in the sensor-cloud	Comprehensive work the focuses on the trustworthy communication	Does not cover all components of the sensor-cloud
[62]	The latest research related to secure data collection in the sensor-cloud architecture	The latest work relate to attacks and their countermeasures during data collection	Does not cover all components of the sensor-cloud computing
[63]	The latest research related to secure sensor-fog-cloud architecture	The latest work relate to attacks and their countermeasures fog layer, in particular	Almost covers all components of the sensor-cloud architecture, including, security of the VMs, etc.
[63]	VM Migration attacks [64], [65]	VM Migration software bugs and is performed without authentication	Server authentication and encrypting migrated memory pages

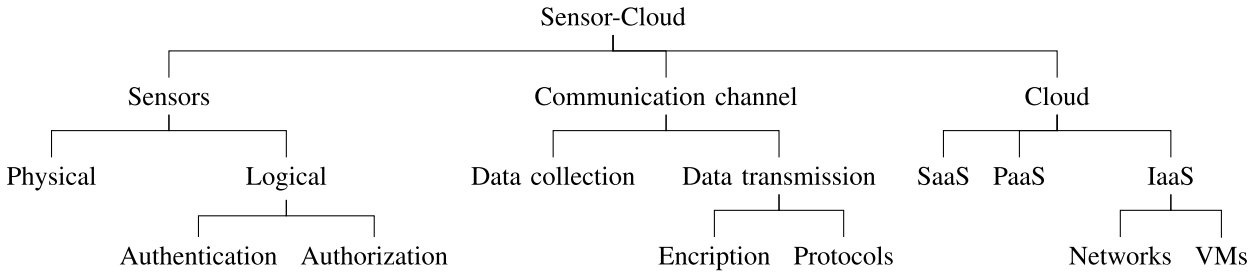

FIGURE 3. Taxonomy of cybersecurity attacks on the three components of the sensor-cloud architecture.

of a network, while a weak source can affect only a portion of the network reachable by the attackers. Jamming attacks can be avoided using Frequency hopping techniques. However, due to high processing and memory requirements, these techniques are unsuitable for the resource-constrained sensor nodes. The Ultra Wide Band (UWB) transmission techniques are considered an alternative solution for protecting these resource-constrained networks from jamming attacks. However, they are not as effective as the frequency hopping technique against the jamming attacks [46]. Frequency hopping can be considered as one of the mechanisms for preventing this kind of attack.

c: DoS ATTACKS

During these attacks, all available resources are exhausted by the attacker node. The attacker monopolized all resources so that the legitimate users are denied access to the resources, applications, and services offered by the network. During these attacks, the attackers act as a normal node and challenge the power and authority of the network, disturbing the smooth operation of the network. Moreover, it weakens the network capacity, and capabilities of offering various services to its sub-entities [72], [73].

2) ATTACKS AND COUNTERMEASURES DURING SECURE DATA TRANSMISSION ON THE WIRELESS CHANNEL

1) **false routing**
2) **packet replication**
3) **man in the middle attacks**
4) **black hole attacks**
5) **sink hole attacks**
6) **worm hole attacks**
7) **selective packet forwarding**
8) **spoofed routing information**
9) **acknowledgement spoofing**
10) **node replication attacks**
11) **passive information gathering**
12) **sybil attacks**

a: FALSE ROUTING

In this type of attack, the perpetrator targets the routing table by injecting incorrect routing information. It is flooded with imprecise information, causing routing table overflow [74], [75]. Moreover, in some instances, the malicious node change and re-routes the packet on a route other than the one for it is expected before transmitting it across the network [76]–[79].

b: PACKET REPLICATION

WSN has limited resources, i.e., energy, bandwidth processing, and communication. In packet replication attacks, the attackers aim to exploit the resource-constrained nature of these sensor nodes. During these attacks, the attackers replicate the received packets and then forward them to other nodes. This causes flooding attacks in the network that causes network congestion and deteriorates the performance of the network. Moreover, the energy of the network is depleted earlier than expected, which shortens the lifetime of the network [16].

c: BLACK HOLE

Another category of attacks that target routing tables are black hole attacks. During these attacks, the malicious node act as a black hole. All or some of the network traffic is re-routed towards the malicious node, which accepts all incoming network traffic and refuses to further forward it towards the other nodes or their final destination. As a result, data communication in the network is adversely disrupted deteriorating the performance of the network [63], [80].

d: SINKHOLE ATTACKS

Likewise, in sinkhole attacks, the attackers redirect all the network traffic towards a specific malicious node due to the false routing information advertised by the compromised node. All nodes in the network follow this incorrect information and thus, nodes in the network are tricked by diverting their traffic towards a malicious route. As a result, data reach a destination other than the desired one. The sinkhole attacks result in selective forwarding attacks because all the network traffic is attracted towards a single point.

e: WORMHOLE ATTACKS

In a wormhole attack, a packet is captured at one location while forwarded from the other allocation using tunnelling technique. The same packet then starts its transmission back into the network from its new location. This type of attack involves two types of competing adversaries. The worm whole attacks may lead to false/forged routing information, change of network topology as well as causing packet loss.

f: SELECTIVE MESSAGE FORWARDING

The attacker nodes keep some selected messages during these attacks while the others are transmitted across the network. Thus, a set of selected messages are dropped and are never forwarded. They are considered lost, which compromises the reliability and integrity of the underlying application. The attacker or the compromised node is usually between the sender and receiver node monitoring the flow of traffic between them. In the black hole attacks, on the other hand, all packets are dropped by the attacker node.

g: SPOOFING ATTACKS

In spoofing attacks, the attacker pretended to be a legitimate user and launch various attacks. They fabricate their identity by using the credentials of the real users. These attacks disrupt network traffic by altering the routing information, creating routing loops, generating false error messages, increasing end-to-end delays, and modifying the routing information that adversely disrupts the flow of traffic in the network. There are many variants of spoofing attacks such as acknowledgment spoofing and IP spoofing. In the former case, an acknowledgment is spoofed by providing false information to the sender about the receiver node, for instance, sending information that a node is alive when in fact, it is dead. In IP spoofing, the attacker uses a forged IP address to hide the identity that facilitates them to exploit the network and launch various attacks in the network. During IP hijacking, the attackers take over the IP addresses of the legitimate users. These may result in congestion, complete disconnection of either the network or users or both from the network that completely paralyzes the network. Moreover, the attackers get unauthorized access to the network and take full control over the sensitive and confidential data stored in these networks. The attackers impersonate to be a trusted e-mail sender resulting in the spread of malware by spoofing the meta-data. Other variants of spoofing attacks are DNS spoofing, ARP spoofing, and so on.

h: NODE REPLICATION ATTACKS

In node replication attacks, the attackers implant a malicious node using the ID of the existing nodes. These attacks disrupt the network's performance by providing wrong routing information that re-routes the packets on the routes other than the one on which it is expected. Moreover, inaccurate information is forwarded from both the victim and attacker nodes towards the decision center that adversely affects the data analysis and decision-making process. Another issue is the copying of the cryptographic keys from the victim network that facilitate attackers to access and comprise the security and privacy of the network and enable them to launch various security attacks on the network. Node replication attacks can be detected by verifying the nodes' identities by some trustworthy nodes/techniques.

i: PASSIVE INFORMATION GATHERING

In passive information gathering, the attackers usually gather information and the data streams from both the node and the network with the help of powerful antennas and receivers. Along with various information, the attackers intercept the sensor node's location, locate the node in the network, and understand the messages transmitting in the network. After locating the node, the attacker can launch various attacks, including damage to the sensor node, implanting malicious nodes, analyse various contents of the packets such as message IDs and timestamps to gain a deeper knowledge of the network.

j: SYBIL ATTACK

A sensor network consist of sensor nodes that work collectively to accomplish a task. In a Sybil attack, a malicious node acts as a group of nodes using the identity of the real nodes simultaneously that affect the overall operation of the network. Few of the issues that arise as a result of Sybil attacks are distributed storage, imprecise location of the node, and incorrect routing information. The WSN can be protected from the Sybil attack by verifying the identity of the nodes. However, the challenging issue is that nodes are resource-constrained, and thus, traditional algorithms are not applicable in these networks. Therefore, light-weight security solutions should be designed to secure the nodes from such security attacks in the future [63].

k: SMURF ATTACK

In these attacks, a large number of the ICMP requests are forwarded towards the victim node. In response to these requests, the victim node sends back unlimited ICMP responses that congest and paralyse the whole network. One of the possible solutions to protect the network from such attacks is to configure devices in the network such as routers and individual computers that ignore constant ICMP requests.

C. SECURING DATA AT THE CLOUD PLATFORM

The three delivery models of the sensor-clouds proposed by the NIST and consequently adopted by the industry are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [81], [82]. In this section, we provide a detailed discussion on a diverse range of security attacks targeting each of these components along with their countermeasures [17], [83]–[85]. A taxonomy of various attacks on three different cloud services, i.e., SaaS, PaaS, and IaaS is given in Figure. 4. Since the cloud is usually virtualized in terms of resource provisioning, VM security is also considered.

1) SOFTWARE AS A SERVICE (SaaS)

In this model, the complete application package is hosted at the cloud server. It is offered to an unlimited number of individual clients as a service on demand. The client does not require to host/save/configure the Software in advance

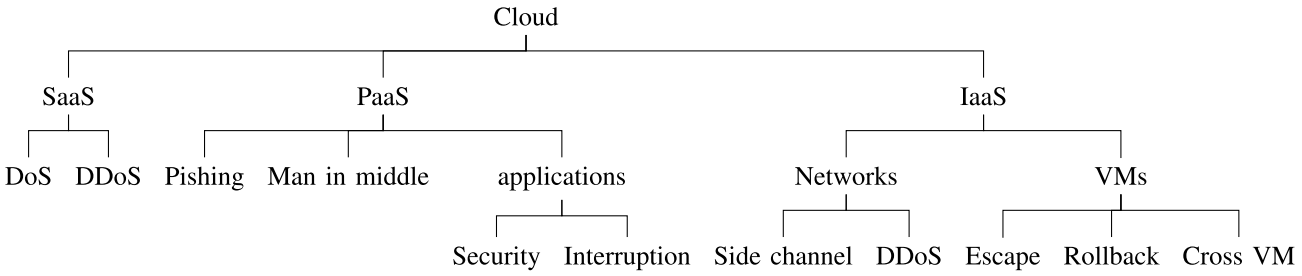

FIGURE 4. Taxonomy of cybersecurity attacks on the three components of the cloud architecture.

FIGURE 5. Software as a service (SaaS) - services like Gmail, Google app engine etc. are common SaaS cloud services.

on their system. This saves the client's money and time [86]. Moreover, the cloud facilitates their clients with issues such as Software licensing, availability of a diverse range of software and an unlimited amount of available memory. This is because the SaaS brings the data and business processes together to utilize the services in a web service or software-oriented architecture, as shown in Figure. 5. A brief account of various security attacks on the SaaS platform is provided below.

1) **denial of service (DoS) attacks**
2) **distributed denial of service (DDoS) attacks**
3) **SQL injection attacks**
4) **cross site scripting**

a: DENIAL OF SERVICE (DoS) ATTACKS

In the DOS attack, the targeted system and resources are flooded with an overwhelming number of requests that adversely affect their normal operation. The attackers sent a large number of unneeded packets that exceed the normal capacity of both the network and, as well as, the server. These attacks force either the network or the targeted system or both so busy that they become unavailable and unable to serve the legitimate users. DoS attacks may cause buffer overflow, packet loss, congestion, and wastage of the useful resources of the network [87], [88].

b: DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS

DDoS attacks pose a serious threat to both consumers and vendors of the cloud. It can significantly damage the customers' data. In DDoS attacks, a large number of Internet bots are deployed that attack a specific application, server, or network with an overwhelming number of requests. As a result, these networks are unable to serve legitimate users. The affected server denies serving all authorized users [89]. To prevent this type of attack, cloud vendors should have a comprehensive protection strategy that secures this infrastructure at all levels [90]. The comprehensive protection strategy includes a denial-of-service response plan, secure network infrastructure, and threat detection strategy. DDoS attacks occur in various forms, and sometimes, it becomes impossible to identify them. One of the possible identification of these attacks is the dramatic decrease in the network's performance or an increase in the number of spam. When such signs appear, the vulnerable device/issue must be addressed at the earliest time [91], [92].

c: SQL INJECTION ATTACK

In SQL injection attacks, the perpetrators inject malicious code that executes and modify SQL commands. These commands even delete the rows, tables, or the entire tables and, in some instances, the whole database.

d: AUTHENTICATION ATTACKS

In these attacks, the attackers try to steal the identity information of the legitimate users they use for authentication. The attackers use such information for accessing their private information and confidential data either flowing through or stored in the network. Authentication attacks can cause other security attacks, such as bypass attacks, brute force attacks, session eavesdropping, replay attacks, and key logger attacks [93].

e: CROSS SITE SCRIPTING ATTACKS

These attacks usually target web-specific applications. The perpetrator usually inserts some client-side scripts of the web applications that aim to know the legitimate users' credential.

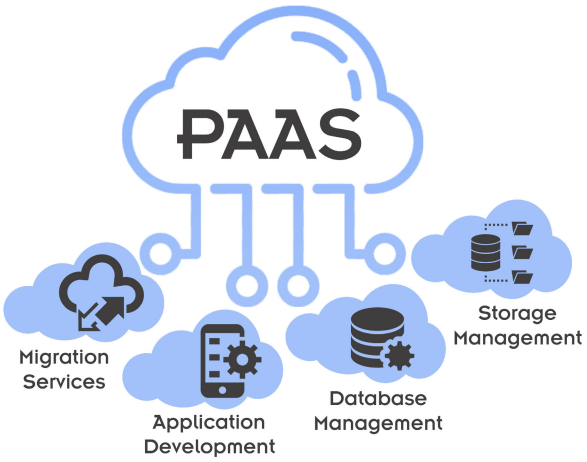

FIGURE 6. Platform as a service (PaaS) - services like online programming, compilers, Google Colab etc. are common PaaS cloud services.

They then use such information for launching various security attacks. The malicious script is automatically executed once legitimate users visit various web applications.

2) PLATFORM AS A SERVICE (PaaS)

In this model, users are provided with some software and development environments by the cloud providers [94]. This offers greater scalability and manageability to the users. These vendors have a greater choice and freedom and have the opportunity to either use the existing or build their customized applications that cater to their specific requirements. Some examples of these applications are operating systems with a stack of applications such as the LAMP platform (Linux, PHP, and MySql), restricted J2EE, Ruby, and so on, as depicted in Figure. 6. The payment mechanism of the PaaS is a pay-per-use model. Few of the common security attacks in the PaaS are presented below.

1) **phishing attacks**
2) **man in the middle attack**
3) **cloud malware**
4) **password reset**
5) **programming flaws**
6) **application security**
7) **software interruption**

a: PHISHING ATTACKS

In fishing attacks, the attackers usually try to access and steal confidential information from legitimate users. It is one of the major sources of identity theft and a favorite choice of the attackers. In these attacks, the attackers usually send an e-mail to the legitimate users asking for personal and confidential information [95]. The users are tricked, and once they respond to that e-mail. Their reply contains sensitive information that is redirected and is forwarded towards the attackers. As a result, the user becomes a victim of the phishing attack. Moreover, opening such an e-mail can install malware, damaging files, the overall system, and accessing confidential information. The attackers can also abuse such information particularly sensitive financial and personal confidential information [96].

b: MAN-IN-THE-MIDDLE ATTACK

In this attack, the attacker tries to intercept the communication between the two parties, which might be VMs [86], to know the information among them. In this way, the confidential information among them has leaked that acts as a base for launching other types of security attacks [63], [97].

c: CLOUD MALWARE-INJECTION ATTACKS

This attack modifies data and various functionalities of the server by deteriorating their performance. Some of the most common malware injection attacks are SQL injection and cross-site scripting (XSS).

d: PASSWORD RESET

In the password reset, the perpetrator tries to urge the victim to sign up for an account for certain services under the attacker's control and is tricked for password resent. Some of these services include free downloads, format conversion, and so on. The attacker then uses this registration information and enables them to access and then reset the password of the victim's multiple accounts on different systems.

e: PROGRAMMING FLAWS

The term flaw is used to describe a problem, weakness, or even an error in a software program. It can pose a severe security threat causing the Software to act abnormally or crash in certain circumstances. These flaws act as the possible entry point for the attackers to launch various security attacks. The perpetrators gain complete control over the system and access to confidential data. As a result, attackers can launch various attacks causing unforeseen damage in terms of time and cost. The organization developing Software must fix the patches while the vendors consequently update them on their computers [63].

f: APPLICATION SECURITY

WSNs are deployed in mission-critical applications. The collected data is periodically transmitted to the sink node for further processing. The sink node acts as a gateway facilitating transferring of collected data towards the cloud. The attackers usually target diverse applications launching various security attacks such as overwhelm, repudiation, data corruption, and malicious code. These attacks adversely affect the network's performance and consume limited energy and bandwidth of the resources-constrained network. Indeed, securing the wireless sensor network is very important to secure confidential data [98].

3) INFRASTRUCTURE AS A SERVICE (IaaS)

IaaS layer is designed to enhance the system's performance by providing clusters, grids, memory, and socialized systems,

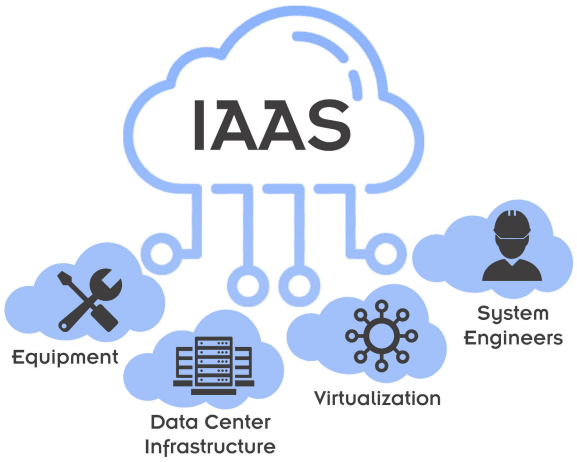

FIGURE 7. Infrastructure as a service (IaaS) - services like AWS EC2, VMs, containers, Google's cloud, etc., are common IaaS cloud services.

and application software to enhance their performance. Various kinds of IaaS services are provided in the capacity of CPU (servers/virtual machines), storage, etc., as given in Figure. 7.

These services are provided to the individual users in a distributed manner instead of a centralized manner [82]. This saves time and costs that otherwise incurs on purchasing expensive and powerful resources. Thus, it not only reduce cost but also improve reliability as opposed to the centralized approach [99], [100]. The user usually pays per use fees for accessing and using these resources to the vendor. Few of the common security attacks on the IaaS are presented below.

1) **stepping stone**
2) **virtual machine escape**
3) **side channel attacks**
4) **malicious insiders**
5) **programming attacks**
6) **VM rollback attacks**
7) **cross VM attacks**
8) **virtual cloud protection**
9) **session hijacking**
10) **traffic flow analysis**
11) **defacement**
12) **connection flooding**
13) **DDoS**
14) **Theft-of-Service attack**

a: STEPPING-STONE ATTACKS

In this type of attack, the attacker usually hides their identity using various techniques. They usually attack using a series of stepping stones. It is very difficult to trace back the identity of the attacker because they hide their actual identity while using a fake identity instead.

b: VIRTUAL MACHINE ESCAPE

This is another common attack that occurs on the IaaS, particularly targeting virtual machines. During this attack, the attacker launches an attack by forcing the victim OS hosted on the VM to communicate directly with the hypervisors. The hypervisors are the virtual machine monitors. As a result, the attackers get full access to all virtual machines and the OS hosting those virtual machines [63], [86], [101].

c: SIDE CHANNEL ATTACKS

In these kinds of attacks, the intruder get information from the implementation of the system, at the design level. They exploit the loophole in the network and access to information such as power consumption, electromagnetic leaks, and sound leak that provide additional knowledge to the attackers for launching other attacks.

d: MALICIOUS INSIDERS

Malicious insider attacks occur when an insider exhausts the system's storage and processing capabilities beyond its limit. The effect of such an attack ranges from moderate to catastrophic, where the system is unable to respond and finally crashes. These types of attacks may significantly degrade the performance of the applications.

e: VIRTUAL MACHINE (VM) ROLLBACK ATTACKS

In a VM roll-back attack, a compromised hypervisor executes a virtual machine from an older snapshot without the knowledge of the user. A user is usually an entity that uses the cloud services and is the owner of one of the VMs [63]. During these attacks, the attacker ignores some security checks or undo few of the security-critical updates. For instance, a perpetrator may launch a brute-force attack to guess the password for login to the VM. Despite restrictions imposed by the OS, such as blocking for a while after three failed attempts or erasing all data after a limited number of times. The attackers can bypass any type of such restrictions infinitely by roll-backing the VM to its initial state. Moreover, the attacker can also roll-back the permission control module to undo the user permission change to expose users' later information to those who should be blocked. The roll-back attacks are different from the reply attacks because, in the reply attacks, an attacker repeatedly sends the previous messages to the VM. However, in roll-back attacks, the VM itself is replied [102]. Apart from these, VM migrations can also be attached as described in [86].

f: CROSS VIRTUAL MACHINE (VM) ATTACKS

The cloud architecture facilitates its customers by providing them with virtual machines (VM) that enable them to scale their resources on-demand. Moreover, it provides logical isolation between the VMs that separate one VM from the other VM. This implies that these are logically individual VMs, but they share the physical server and resources. The attackers usually target such a multi-tenant virtual environment with cross-VM attacks. The attackers use a single VM to target other VMs on the same hypervisor by redirecting their network traffic, controlling them, or accessing them. Moreover, the attackers mainly target the cache memory. They also

target the CPU, memory, I/O devices, as well as the cloud network [19], [20], [63].

g: SESSION HIJACKING

A session refers to all information concerned with an ongoing transaction. The information related to the session is generally stored in a server along with a unique ID. The unique ID is usually a random number with the starting time and date of the session. The session ID is shared with the customers with their first request and is presented back to the server with each subsequent request. This allows the server to access the stored data appropriate to that specific session, making a logical relationship between the current and previous transactions. In cloud computing, session hijacking is a common security issue. During these attacks, the adversary gains unauthorized access to information required for session establishment stored at the cookies. Once the attacker gain access to such information, it empowers them to do everything that a legitimate user can do in the network, compromising its security, privacy, and integrity.

h: DISTRIBUTED DENIAL OF SERVICE ATTACKS (DDoS) ATTACKS

In a DDoS attack, the attackers aim to disrupt the normal operation of the network by denying access to the available resources and the network. Some of these resources include web servers, CPU, bandwidth, and memory. Cloud architecture can adversely affect various cloud services offered by the virtual servers by damaging them. It degrades their quality or sometimes fully breakdown the network connectivity as well as consumes its bandwidth. The attackers usually deploy a large number of agents or bots to launch DDoS attacks. These attackers usually target a bug/flaw or known vulnerabilities in Software to launch such attacks. They usually scan the network to find machines with vulnerabilities that act as agents by the attackers, also known as zombies. The primary purpose of the attacker is to disrupt the normal operation of the network by making it so busy that the legitimate users are denied access to those resources [103].

i: THEFT-OF-SERVICE ATTACKS

In a Theft-of-Service attack, a malicious virtual machine misbehaves in such a manner that the VM hacks the hypervisor, which assigns additional resources than the resource capacity it is supposed to obtain. This additional resource provisioning for the malicious virtual machine comes at the cost of the other VMs co-located on the same server. Therefore, other co-located VMs are assigned fewer resources than what they pay for, which subsequently degrades their performance and increases their monetary costs [63], [82].

V. COUNTERMEASURES AND CONTROLS

Securing the sensor-cloud architecture is a complex task. Because it is the holistic combination of policies, technology, and the people, they must be managed altogether to design a secure system. Few of the possible solutions to secure this architecture against various security threats and attacks are as follows.

A. END-TO-END ENCRYPTION

The prime benefit of the sensor-cloud is that it shifts various resources intensive tasks such as processing and storage from centralized to the distributed architecture. Although this shift of tasks has many advantages on the one hand; but, it also gives rise to many security threats on the other hand. It is highly desirable to apply end-to-end encryption on the data due to the passage of such data from various geographical locations and servers to servers.

B. SCANNING FOR MALICIOUS ACTIVITIES

Despite that, end-to-end encryption is highly effective for securing data against malicious activities. However, it introduces new risks. One such risk is that encrypted data is unreadable by the firewall and intrusion detection system. Thus, novel countermeasure and preventive measures should be devised that differentiate the real encrypted data from that of the malicious data once it reaches these points, i.e., IDS and firewalls.

C. VALIDATION OF CLOUD CONSUMER

Cloud facilitates the users by shifting few of the resources-intensive tasks from the resources-constrained platform to the resources-rich platform (sensor to fog, sensor to remote cloud, fog to cloud). However, one of the challenging issues in these environments is the authentication of genuine and legitimate users from intruders and hackers. In this way, the cloud architecture is protected against various malicious activities by attackers.

D. SECURE INTERFACES AND APIs

APIs and interfaces are important components of cloud architecture. They offer automation, orchestration, and management. It is imperative to detect, control, and mitigate security issues by tracking malicious interfaces and APIs [63]. Management level security threats are further described in [86].

E. INSIDER ATTACKS

Security attacks from the insiders are the most common type of attacks that target the sensor-cloud architecture [63], [73], [86]. These insiders may be either permanent or contractual employees working for an organization. Furthermore, former employees who have left the company also pose a serious security threat due to their in-depth knowledge of the business process and various network components. They can negatively affect the security and privacy aspects of the information system. Few of the possible reasons that an employee becomes a malicious insider are because of their revenge, coercion, ideology, ego, or seeking financial gain through intellectual property theft or espionage. Insiders are difficult to trace due to their double role. These attackers work as an agent for the rival organizations for financial gains. It is a must that the cloud vendors take precautionary

measures by authenticating users and strengthening internal security systems to prevent their organization from such attacks. Few of the possible solutions should be organization policies, frequent role change, educating employees, and the deletion of all accounts related to employees who have left an organization.

F. SECURE LEVERAGED RESOURCES

All resources of the cloud are shared among multiple users due to the multi-tenancy model. In such an environment, it is necessary first to authenticate the users and then secure the shared resources, i.e., hypervisor, orchestration, and monitoring tools [81]. A detailed investigation of such attacks and solutions is presented in [63].

G. BUSINESS CONTINUITY PLANS

It is necessary to keep a record of various security attacks and breaches that happens in the past and respond of that organization to such incidents. This is important because such documents guide the organization if similar security breaches occur shortly. Then, machine learning-based techniques can be applied to the traced and recorded data to predict future security threats/attacks and triggers appropriate avoidance mechanisms.

VI. OPEN RESEARCH CHALLENGES

Cloud computing has revolutionized the way various computing resources are used, controlled, and managed [82]. However, this revolution and development face various issues and challenges. One of such challenging issues is the security of the sensor-cloud. Recently, researchers in the field have taken serious steps to tackle this issue, but there exist several open research issues that need to be addressed and discussed in this section. The attackers targeting the resource-constrained sensor nodes by forcing the node to process a large volume of malicious data exhausting both their energy and resources. One of the possible solutions to stop such attacks from occurring is to add header and control packets. Moreover, strong authentication schemes can negate the effects of such attacks and protect them. However, the design of such schemes is hindered by the following two issues. Firstly, there is no lightweight, universally accepted encryption algorithms supported by the common cryptographic libraries that can be implemented at the hardware level of the embedded devices.

The second issue is related to the additional overhead incurs due to various supplementary information added to the message for additional authentication requirements. In the future, designers should aim for strong authentication schemes with minimum additional information requiring reduced space and processing overhead. Another issue is related to communication protocols in cloud architecture with known vulnerabilities. The interfaces and APIs are important because they facilitate automation, orchestration, and management. However, these protocols, standards, interfaces, and APIs can be manipulated for their known vulnerabilities [63]. The attackers exploit and target these vulnerabilities and launch various attacks. These loopholes act as the first step for the attackers to launch various attacks on the whole architecture. For example, one such example is SOAP messages that can be exploited to target cloud platforms and steal confidential data and information. It is necessary to address those vulnerabilities and improve their security by incorporating strong encryption mechanisms.

In sensor-cloud architecture, the data is distributed across multiple geographical domains. It is necessary to encrypt the data from the source to the destination. In this regard, a lot of work focuses on symmetric solutions. However, such solutions ignore the effect of capture node attacks. It would be interesting to develop optimized and advanced cryptosystems for this architecture in the future. We observed during surveying the literature that IoT security lacks a collaborative solution in which numerous domains (fog, cloud, and sensing devices) communicate with each other to mitigate a certain attack type. Besides, lightweight cryptography, lightweight network security protocols, and digital forensics are more attractive research fields in the sensor-cloud security architectures [63].

VII. CONCLUSION AND FUTURE WORK

In this paper, we focus our discussion on one of the important and challenging issues of security in the sensor-cloud architecture. A state-of-the-art taxonomy of security attacks on the sensors-cloud is also presented. These security attacks are categorized based on the sensor-cloud's architectural perspective targeting various components of this architecture and securing them from security attacks. These components are sensors, cloud architecture, and the channel that facilitate communication between the two entities. Moreover, limitations of the previous surveys as well as the contributions of this survey are also provided. Furthermore, in this paper, limitations and possible future directions are also provided to the readers for future work and possible extensions so as to make sensor-cloud more resilient, reliable, and secure against various attacks in the years ahead.

We expect that security and privacy shall be accounted for at the preliminary design stage of the IoT systems to evade the common drawback of seeing security as an afterthought. Though pursuing the position of intelligent objects is considered a concealment violation; however, it may also have some beneficial cases, i.e., security agencies depend on chasing the smart objects carried by a missing person to identify the location of the missing person. Such kinds of digital forensics in the IoT era will play an important role and is expected to receive further attention in the future [63]. Moreover, the fog domain is supposed to bring the computational capabilities to the network's edge. In the future, we will pay further attention to this domain as it has not received enough attention from academia and the industry.

REFERENCES

[1] A. Alamri, W. S. Ansari, M. M. Hassan, M. S. Hossain, A. Alelaiwi, and M. A. Hossain, "A survey on sensor-cloud: Architecture, applications, and approaches," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 2, Feb. 2013, Art. no. 917923.

[2] S. Madria, V. Kumar, and R. Dalvi, "Sensor cloud: A cloud of virtual sensors," *IEEE Softw.*, vol. 31, no. 2, pp. 70–77, Mar. 2014.

[3] S. K. Dash, J. P. Sahoo, S. Mohapatra, and S. P. Pati, "Sensor-cloud: Assimilation of wireless sensor network and the cloud," in *Proc. Int. Conf. Comput. Sci. Inf. Technol.* Berlin, Germany: Springer, 2012, pp. 455–464.

[4] M. A. Jan, F. Khan, M. Alam, and M. Usman, "A payload-based mutual authentication scheme for Internet of Things," *Future Gener. Comput. Syst.*, vol. 92, pp. 1028–1039, Mar. 2019.

[5] A. Ez-Zaidi and S. Rakrak, "A comparative study of target tracking approaches in wireless sensor networks," *J. Sensors*, vol. 2016, Dec. 2016, Art. no. 3270659.

[6] X. Yu, D. Zhan, L. Liu, H. Lv, L. Xu, and J. Du, "A privacy-preserving cross-domain healthcare wearables recommendation algorithm based on domain-dependent and domain-independent feature fusion," *IEEE J. Biomed. Health Informat.*, early access, Apr. 1, 2021, doi: 10.1109/JBHI.2021.3069629.

[7] M. A. Jan, W. Zhang, M. Usman, Z. Tan, F. Khan, and E. Luo, "SmartEdge: An end-to-end encryption framework for an edge-enabled smart city application," *J. Netw. Comput. Appl.*, vol. 137, pp. 1–10, Jul. 2019.

[8] M. Erdelj, M. Król, and E. Natalizio, "Wireless sensor networks and multi-UAV systems for natural disaster management," *Comput. Netw.*, vol. 124, pp. 72–86, Sep. 2017.

[9] M. D. Alshehri, F. Hussain, M. Elkhodr, and B. S. Alsinglawi, "A distributed trust management model for the Internet of Things (DTM-IoT)," in *Recent Trends and Advances in Wireless and IoT-Enabled Networks*. Cham, Switzerland: Springer, 2019, pp. 1–9.

[10] K. K. Khedo, Y. Bissessur, and D. S. Goolaub, "An inland wireless sensor network system for monitoring seismic activity," *Future Gener. Comput. Syst.*, vol. 105, pp. 520–532, Apr. 2020.

[11] F. Khan, A. U. Rehman, and M. A. Jan, "A secured and reliable communication scheme in cognitive hybrid ARQ-aided smart city," *Comput. Electr. Eng.*, vol. 81, Jan. 2020, Art. no. 106502.

[12] J. Sun, F. Khan, J. Li, M. D. Alshehri, R. Alturki, and M. Wedyan, "Mutual authentication scheme for the device-to-server communication in the Internet of medical things," *IEEE Internet Things J.*, early access, May 10, 2021, doi: 10.1109/JIOT.2021.3078702.

[13] F. Khan, A. U. Rehman, Z. Yanliang, S. Mastorakis, H. Song, M. A. Jan, and K. Dev, "A secured and reliable continuous transmission scheme in cognitive HARQ-aided Internet of Things," *IEEE Internet Things J.*, early access, Apr. 6, 2021, doi: 10.1109/JIOT.2021.3071398.

[14] M. Elkhodr, B. Alsinglawi, and M. Alshehri, "Data provenance in the Internet of Things," in *Proc. 32nd Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, May 2018, pp. 727–731.

[15] S. A. Chaudhry, K. Yahya, F. Al-Turjman, and M.-H. Yang, "A secure and reliable device access control scheme for IoT based sensor cloud systems," *IEEE Access*, vol. 8, pp. 139244–139254, 2020.

[16] A. Cook, M. Robinson, M. A. Ferrag, L. A. Maglaras, Y. He, K. Jones, and H. Janicke, "Internet of cloud: Security and privacy issues," in *Cloud Computing for Optimization: Foundations, Applications, and Challenges*. Cham, Switzerland: Springer, 2018, pp. 271–301.

[17] A. Malik and H. Om, "Cloud computing and Internet of Things integration: Architecture, applications, issues, and challenges," in *Sustainable Cloud and Energy Services*. Cham, Switzerland: Springer, 2018, pp. 1–24.

[18] A. Hussain, S. Nazir, F. Khan, L. Nkenyereye, A. Ullah, S. Khan, S. Verma, and Kavita, "A resource efficient hybrid proxy mobile IPv6 extension for next generation IoT networks," *IEEE Internet Things J.*, early access, Feb. 12, 2021, doi: 10.1109/JIOT.2021.3058982.

[19] W. Zhang, M. Zhu, T. Gong, L. Xiao, L. Ruan, Y. Mei, Y. Sun, and X. Ji, "Performance degradation-aware virtual machine live migration in virtualized servers," in *Proc. 13th Int. Conf. Parallel Distrib. Comput., Appl. Technol.*, Dec. 2012, pp. 429–435.

[20] V. Varadarajan, T. Ristenpart, and M. Swift, "Scheduler-based defenses against cross-VM side-channels," in *Proc. 23rd USENIX Secur. Symp. (USENIX Security)*, 2014, pp. 687–702.

[21] T. Taleb and A. Ksentini, "Follow me cloud: Interworking federated clouds and distributed mobile networks," *IEEE Netw.*, vol. 27, no. 5, pp. 12–19, Sep. 2013.

[22] B. Bhushan and G. Sahoo, "Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks," *Wireless Pers. Commun.*, vol. 98, no. 2, pp. 2037–2077, Jan. 2018.

[23] I. Tomic and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1910–1923, Dec. 2017.

[24] R. Jadhav and V. Vatsala, "Security issues and solutions in wireless sensor networks," *Int. J. Comput. Appl.*, vol. 162, no. 2, pp. 14–19, Mar. 2017.

[25] A. Dhakne and P. Chatur, "Detailed survey on attacks in wireless sensor network," in *Proc. Int. Conf. Data Eng. Commun. Technol.* Singapore: Springer, 2017, pp. 319–331.

[26] C. Ioannou and V. Vassiliou, "The impact of network layer attacks in wireless sensor networks," in *2016 Int. Workshop Secure Internet Things (SIoT)*, Sep. 2016, pp. 20–28.

[27] H. Radhappa, L. Pan, J. X. Zheng, and S. Wen, "Practical overview of security issues in wireless sensor network applications," *Int. J. Comput. Appl.*, vol. 40, no. 4, pp. 202–213, Oct. 2018.

[28] K. Chelli, "Security issues in wireless sensor networks: Attacks and countermeasures," in *Proc. World Congr. Eng.*, vol. 1, no. 20, pp. 876–897, 2015.

[29] M. D. Alshehri and F. K. Hussain, "A centralized trust management mechanism for the Internet of Things (CTM-IoT)," in *Proc. Int. Conf. Broadband Wireless Comput., Commun. Appl.* Cham, Switzerland: Springer, 2017, pp. 533–543.

[30] M. Elhoseny and A. E. Hassanien, "Secure data transmission in WSN: An overview," in *Dynamic Wireless Sensor Networks* (Studies in Systems, Decision and Control), vol. 165. Cham, Switzerland: Springer, 2019, doi: 10.1007/978-3-319-92807-4_6.

[31] R. Tso, A. Alelaiwi, S. M. M. Rahman, M.-E. Wu, and M. S. Hossain, "Privacy-preserving data communication through secure multi-party computation in healthcare sensor cloud," *J. Signal Process. Syst.*, vol. 89, no. 1, pp. 51–59, Oct. 2017.

[32] M. D. Alshehri and F. K. Hussain, "A fuzzy security protocol for trust management in the Internet of Things (Fuzzy-IoT)," *Computing*, vol. 101, no. 7, pp. 791–818, Jul. 2019.

[33] N. Poolsappasit, V. Kumar, S. Madria, and S. Chellappan, "Challenges in secure sensor-cloud computing," in *Proc. Workshop Secure Data Manage.* Berlin, Germany: Springer, 2011, pp. 70–84.

[34] W. Chunming, L. Qianjun, L. Yuwei, C. Qiumei, and Z. Haifeng, "A survey on cloud security," *ZTE Commun.*, vol. 15, no. 2, pp. 42–47, 2019.

[35] M. A. Khan, "A survey of security issues for cloud computing," *J. Netw. Comput. Appl.*, vol. 71, pp. 11–29, Aug. 2016.

[36] J. B. Hong, A. Nhlabatsi, D. S. Kim, A. Hussein, N. Fetais, and K. M. Khan, "Systematic identification of threats in the cloud: A survey," *Comput. Netw.*, vol. 150, pp. 46–69, Feb. 2019.

[37] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "PrivacyProtector: Privacy-protected patient data collection in IoT-based healthcare systems," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 163–168, Feb. 2018.

[38] I. Khalil, A. Khreishah, and M. Azeem, "Cloud computing security: A survey," *Computers*, vol. 3, no. 1, pp. 1–35, Feb. 2014.

[39] M. D. Alshehri, F. K. Hussain, and O. K. Hussain, "Clustering-driven intelligent trust management methodology for the Internet of Things (CITM-IoT)," *Mobile Netw. Appl.*, vol. 23, no. 3, pp. 419–431, Jun. 2018.

[40] G. Ramachandra, M. Iftikhar, and F. A. Khan, "A comprehensive survey on security in cloud computing," *Procedia Comput. Sci.*, vol. 110, no. 1, pp. 465–472, 2017.

[41] Y. Liu, Y. L. Sun, J. Ryoo, S. Rizvi, and A. V. Vasilakos, "A survey of security and privacy challenges in cloud computing: Solutions and future directions," *J. Comput. Sci. Eng.*, vol. 9, no. 3, pp. 119–133, Sep. 2015.

[42] W. Li, Y. Chai, F. Khan, S. R. U. Jan, S. Verma, V. G. Menon, and X. Li, "A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system," *Mobile Netw. Appl.*, vol. 26, pp. 1–19, Jan. 2021.

[43] F. Khan, "Secure communication and routing architecture in wireless sensor networks," in *Proc. IEEE 3rd Global Conf. Consum. Electron. (GCCE)*, Oct. 2014, pp. 647–650.

[44] N. Usman, S. Usman, F. Khan, M. A. Jan, A. Sajid, M. Alazab, and P. Watters, "Intelligent dynamic malware detection using machine learning in IP reputation for forensics data analytics," *Future Gener. Comput. Syst.*, vol. 118, pp. 124–141, May 2021.

[45] M. Dabbagh, B. Hamdaoui, M. Guizani, and A. Rayes, "Software-defined networking security: Pros and cons," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 73–79, Jun. 2015.

[46] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Netw.*, vol. 20, no. 3, pp. 41–47, May 2006.

[47] Y. Zhang, K. Cheng, F. Khan, R. Alturki, R. Khan, and A. U. Rehman, "A mutual authentication scheme for establishing secure device-to-device communication sessions in the edge-enabled smart cities," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102683.

[48] M. A. Jan, F. Khan, R. Khan, S. Mastorakis, V. G. Menon, P. Watters, and M. Alazab, "A lightweight mutual authentication and privacy-preservation scheme for intelligent wearable devices in industrial-CPS," *IEEE Trans. Ind. Informat.*, vol. 17, no. 8, pp. 5829–5839, Aug. 2021.

[49] X. Yu, Y. Chu, F. Jiang, Y. Guo, and D. Gong, "SVMs classification based two-side cross domain collaborative filtering by inferring intrinsic user and item features," *Knowl.-Based Syst.*, vol. 141, pp. 80–91, Feb. 2018.

[50] X. Yu, J. Yang, and Z. Xie, "Training SVMs on a bound vectors set based on Fisher projection," *Frontiers Comput. Sci.*, vol. 8, no. 5, pp. 793–806, Oct. 2014.

[51] H. Tabrizchi and M. K. Rafsanjani, "A survey on security challenges in cloud computing: Issues, threats, and solutions," *J. Supercomput.*, vol. 76, no. 12, pp. 9493–9532, 2020.

[52] P. Evensen and H. Meling, "SenseWrap: A service oriented middleware with sensor virtualization and self-configuration," in *Proc. Int. Conf. Intell. Sensors, Sensor Netw. Inf. Process. (ISSNIP)*, Dec. 2009, pp. 261–266.

[53] S. Chatterjee, R. Ladia, and S. Misra, "Dynamic optimal pricing for heterogeneous service-oriented architecture of sensor-cloud infrastructure," *IEEE Trans. Services Comput.*, vol. 10, no. 2, pp. 203–216, Mar. 2017.

[54] S. Misra, S. Chatterjee, and M. S. Obaidat, "On theoretical modeling of sensor cloud: A paradigm shift from wireless sensor network," *IEEE Syst. J.*, vol. 11, no. 2, pp. 1084–1093, Jun. 2017.

[55] I. Masood, Y. Wang, A. Daud, N. R. Aljohani, and H. Dawood, "Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure," *Wireless Commun. Mobile Comput.*, vol. 2018, Nov. 2018, Art. no. 2143897.

[56] I. Ali, A. Gani, I. Ahmedy, I. Yaqoob, S. Khan, and M. H. Anisi, "Data collection in smart communities using sensor cloud: Recent advances, taxonomy, and future research directions," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 192–197, Jul. 2018.

[57] I. Ali, I. Ahmedy, A. Gani, M. Talha, M. A. Raza, and M. H. Anisi, "Data collection in sensor-cloud: A systematic literature review," *IEEE Access*, vol. 8, pp. 184664–184687, 2020.

[58] W. Aman and F. Khan, "Ontology-based dynamic and context-aware security assessment automation for critical applications," in *Proc. IEEE 8th Global Conf. Consum. Electron. (GCCE)*, Oct. 2019, pp. 644–647.

[59] H. Tao, M. Z. A. Bhuiyan, M. A. Rahman, T. Wang, J. Wu, S. Q. Salih, Y. Li, and T. Hayajneh, "TrustData: Trustworthy and secured data collection for event detection in industrial cyber-physical system," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3311–3321, May 2020.

[60] T. Wang, Y. Li, Y. Chen, H. Tian, Y. Cai, W. Jia, and B. Wang, "Fog-based evaluation approach for trustworthy communication in sensor-cloud system," *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2532–2535, Nov. 2017.

[61] W. Yao, A. Yahya, F. Khan, Z. Tan, A. U. Rehman, J. M. Chuma, M. A. Jan, and M. Babar, "A secured and efficient communication scheme for decentralized cognitive radio-based Internet of vehicles," *IEEE Access*, vol. 7, pp. 160889–160900, 2019.

[62] T. Wang, Y. Li, W. Fang, W. Xu, J. Liang, Y. Chen, and X. Liu, "A comprehensive trustworthy data collection approach in sensor-cloud system," *IEEE Trans. Big Data*, early access, Mar. 1, 2019, doi: 10.1109/TBDATA.2018.2811501.

[63] M. Dabbagh and A. Rayes, "Internet of Things security and privacy," in *Internet of Things From Hype to Reality*. Cham, Switzerland: Springer, 2019, pp. 211–238.

[64] A. A. Khan, M. Zakarya, and R. Khan, "H^2—A hybrid heterogeneity aware resource orchestrator for cloud platforms," *IEEE Syst. J.*, vol. 13, no. 4, pp. 3873–3876, Dec. 2019.

[65] A. A. Khan, M. Zakarya, R. Khan, I. U. Rahman, M. Khan, and A. U. R. Khan, "An energy, performance efficient resource consolidation scheme for heterogeneous cloud datacenters," *J. Netw. Comput. Appl.*, vol. 150, Jan. 2020, Art. no. 102497.

[66] N. Tariq, M. Asim, F. A. Khan, T. Baker, U. Khalid, and A. Derhab, "A blockchain-based multi-mobile code-driven trust mechanism for detecting internal attacks in Internet of Things," *Sensors*, vol. 21, no. 1, p. 23, Dec. 2020.

[67] M. A. Enow, "An effective scheme to detect and prevent tampering on the physical layer of WSN," in *Proc. 5th IEEE Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)/4th IEEE Int. Conf. Edge Comput. Scalable Cloud (EdgeCom)*, Jun. 2018, pp. 172–178.

[68] S. Ali, T. Al Balushi, Z. Nadir, and O. K. Hussain, "WSN security mechanisms for CPS," in *Cyber Security for Cyber Physical System* Cham, Switzerland: Springer, 2018, pp. 65–87.

[69] S. Jaitly, H. Malhotra, and B. Bhushan, "Security vulnerabilities and countermeasures against jamming attacks in wireless sensor networks: A survey," in *Proc. Int. Conf. Comput., Commun. Electron. (Comptelix)*, Jul. 2017, pp. 559–564.

[70] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, "Jamming attacks on wireless networks: A taxonomic survey," *Int. J. Prod. Econ.*, vol. 172, pp. 76–94, Feb. 2016.

[71] F. Khan, A. U. Rehman, J. Zheng, M. A. Jan, and M. Alam, "Mobile crowdsensing: A survey on privacy-preservation, task management, assignment models, and incentives mechanisms," *Future Gener. Comput. Syst.*, vol. 100, pp. 456–472, Nov. 2019.

[72] R. Geetha, A. K. Suntheya, and G. U. Srikanth, "Cloud integrated IoT enabled sensor network security: Research issues and solutions," *Wireless Pers. Commun.*, vol. 113, no. 2, pp. 747–771, Jul. 2020.

[73] E. E. Abel and A. L. S. Muhammad, "Management of WSN-enabled cloud Internet of Things: A review," *Int. J. Comput. Digit. Syst.*, vol. 10, pp. 353–372, Feb. 2021.

[74] J. H. Abawajy and M. M. Hassan, "Federated Internet of Things and cloud computing pervasive patient health monitoring system," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 48–53, Jan. 2017.

[75] F. Khan, A. U. Rehman, M. Usman, Z. Tan, and D. Puthal, "Performance of cognitive radio sensor networks using hybrid automatic repeat ReQuest: Stop-and-wait," *Mobile Netw. Appl.*, vol. 23, no. 3, pp. 479–488, Jun. 2018.

[76] P. P. Ray and N. Kumar, "SDN/NFV architectures for edge-cloud oriented IoT: A systematic review," *Comput. Commun.*, vol. 169, pp. 129–153, Mar. 2021.

[77] X. Yu, F. Jiang, J. Du, and D. Gong, "A cross-domain collaborative filtering algorithm with expanding user and item features via the latent factor space of auxiliary domains," *Pattern Recognit.*, vol. 94, pp. 96–109, Oct. 2019.

[78] J. Li, J. Cai, F. Khan, A. U. Rehman, V. Balasubramaniam, J. Sun, and P. Venu, "A secured framework for SDN-based edge computing in IoT-enabled healthcare system," *IEEE Access*, vol. 8, pp. 135479–135490, 2020.

[79] H. Tao, M. Z. A. Bhuiyan, M. A. Rahman, G. Wang, T. Wang, M. M. Ahmed, and J. Li, "Economic perspective analysis of protecting big data security and privacy," *Future Gener. Comput. Syst.*, vol. 98, pp. 660–671, Sep. 2019.

[80] F. Zhou, M. Goel, P. Desnoyers, and R. Sundaram, "Scheduler vulnerabilities and coordinated attacks in cloud computing," *J. Comput. Secur.*, vol. 21, no. 4, pp. 533–559, Sep. 2013.

[81] A. A. Khan, M. Zakarya, R. Buyya, R. Khan, M. Khan, and O. Rana, "An energy and performance aware consolidation technique for containerized datacenters," *IEEE Trans. Cloud Comput.*, early access, Jun. 5, 2019, doi: 10.1109/TCC.2019.2920914.

[82] M. Zakarya and L. Gillam, "Managing energy, performance and cost in large scale heterogeneous datacenters using migrations," *Future Gener. Comput. Syst.*, vol. 93, pp. 529–547, Apr. 2019.

[83] K. Muhammad, J. Lloret, and S. W. Baik, "Intelligent and energy-efficient data prioritization in green smart cities: Current challenges and future directions," *IEEE Commun. Mag.*, vol. 57, no. 2, pp. 60–65, Feb. 2019.

[84] F. Khan, M. A. Jan, A. U. Rehman, S. Mastorakis, M. Alazab, and P. Watters, "A secured and intelligent communication scheme for IIoT-enabled pervasive edge computing," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 5128–5137, Jul. 2021.

[85] S. Sharma, V. Chang, U. S. Tim, J. Wong, and S. Gadia, "Cloud and IoT-based emerging services systems," *Cluster Comput.*, vol. 22, no. 1, pp. 71–91, Mar. 2019.

[86] P. D. Patel, M. Karamta, M. D. Bhavsar, and M. B. Potdar, "Live virtual machine migration techniques in cloud computing: A survey," *Int. J. Comput. Appl.*, vol. 86, no. 16, pp. 18–21, Jan. 2014.
[87] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Gener. Comput. Syst.*, vol. 78, pp. 659–676, Jan. 2018.
[88] S. Kianoush, M. Raja, S. Savazzi, and S. Sigg, "A cloud-IoT platform for passive radio sensing: Challenges and application case studies," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3624–3636, Oct. 2018.
[89] T. Wang, Y. Mei, X. Liu, J. Wang, H.-N. Dai, and Z. Wang, "Edge-based auditing method for data security in resource-constrained Internet of Things," *J. Syst. Archit.*, vol. 114, Mar. 2021, Art. no. 101971.
[90] S. K. Yr and H. Champa, "An extensive review on sensing as a service paradigm in iot: Architecture, research challenges, lessons learned and future directions," *Int. J. Appl. Eng. Res*, vol. 14, no. 6, pp. 1220–1243, 2019.
[91] M. Zakarya, "Energy, performance and cost efficient datacenters: A survey," *Renew. Sustain. Energy Rev.*, vol. 94, pp. 363–385, Oct. 2018.
[92] W. Itani, C. Ghali, A. Kayssi, and A. Chehab, "Reputation as a service: A system for ranking service providers in cloud systems," in *Security, Privacy and Trust in Cloud Systems*. Berlin, Germany: Springer, 2014, pp. 375–406.
[93] M. N. Aladwan, F. M. Awaysheh, S. Alawadi, M. Alazab, T. F. Pena, and J. C. Cabaleiro, "TrustE-VC: Trustworthy evaluation framework for industrial connected vehicles in the cloud," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6203–6213, Sep. 2020.
[94] M. Zakarya and L. Gillam, "Energy efficient computing, clusters, grids and clouds: A taxonomy and survey," *Sustain. Comput., Informat. Syst.*, vol. 14, pp. 13–33, Jun. 2017.
[95] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19293–19304, 2017.
[96] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in *Proc. Int. Conf. Wireless Algorithms, Syst., Appl.* Cham, Switzerland: Springer, 2015, pp. 685–695.
[97] W. Yao, F. Khan, M. A. Jan, N. Shah, I. U. Rahman, A. Yahya, and A. U. Rehman, "Artificial intelligence-based load optimization in cognitive Internet of Things," *Neural Comput. Appl.*, vol. 32, pp. 16179–16189, Mar. 2020.
[98] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in fog computing: A survey," *Future Gener. Comput. Syst.*, vol. 88, pp. 16–27, Nov. 2018.
[99] P. Hu, S. Dhelim, H. Ning, and T. Qiu, "Survey on fog computing: Architecture, key technologies, applications and open issues," *J. Netw. Comput. Appl.*, vol. 98, pp. 27–42, Nov. 2017.
[100] C. Hennebert and J. D. Santos, "Security protocols and privacy issues into 6LoWPAN stack: A synthesis," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 384–398, Oct. 2014.
[101] M. Yu, T. Quan, Q. Peng, X. Yu, and L. Liu, "A model-based collaborate filtering algorithm based on stacked AutoEncoder," *Neural Comput. Appl.*, early access, pp. 1–9, Mar. 2021.
[102] Y. Xia, Y. Liu, H. Chen, and B. Zang, "Defending against VM rollback attack," in *Proc. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops (DSN)*, Jun. 2012, pp. 1–5.
[103] R. V. Deshmukh and K. K. Devadkar, "Understanding DDoS attack & its effect in cloud environment," *Procedia Comput. Sci.*, vol. 49, no. 1, pp. 202–210, 2015.

RYAN ALTURKI received the Ph.D. degree from the University of Technology, Sydney, Australia. He is currently an Assistant Professor with the Department of Information Science, College of Computers and Information Systems, Umm Al-Qura University, Makkah, Saudi Arabia. He published several publications in high ranked international journals, conferences, and chapter of books. His research interests include eHealth, mobile technologies, the Internet of Things (IoT), artificial intelligence, cloud computing, and cybersecurity.

HASAN JUMAILI ALYAMANI received the B.Sc. degree in computer science from Umm Al-Qura University, Saudi Arabia, in 2006, the M.S. degree in computer science from The University of Waikato, New Zealand, in 2012, and the Ph.D. degree in computer science from Macquarie University, Australia, in 2019. He is currently the Chairman of the Department of Information Systems, King Abdulaziz University, Saudi Arabia.

MOHAMMED ABDULAZIZ IKRAM received the master's degree from the University of Technology Sydney, Australia, in 2015, and the Ph.D. degree from the Department of Computer Science, University of Technology Sydney, in 2020. He is currently working as an Assistant Professor with the School of Computer Science, Al-Jamoum College, Umm Al-Qura University. His research interests include cloud computing, the Internet of Things, networking systems, and data science. He published several publications in these fields.

MD ARAFATUR RAHMAN (Senior Member, IEEE) received the Ph.D. degree in electronic and telecommunications engineering from the University of Naples Federico II, Naples, Italy, in 2013. He worked as a Postdoctoral Research Fellow with the University of Naples Federico II, in 2014, and a Visiting Researcher with the Sapienza University of Rome, in 2016. He is currently a Senior Lecturer with the School of Mathematics and Computer Science, University of Wolverhampton, U.K. Prior to joining the University of Wolverhampton, he was an Associate Professor with the Faculty of Computer Systems and Software Engineering, University Malaysia Pahang. He has coauthored over 60 prestigious IEEE and Elsevier journal and conference publications. His research interests include the Internet of Things (IoT), wireless communication networks, cognitive radio networks, and vehicular communication. He has developed an excellent track record of academic leadership and management and execution of international ICT projects that are supported by agencies in Italy, the EU, and Malaysia. He is also a fellow of the IBM Center of Excellence, Malaysia. He received a number of prestigious international research awards, notably the Best Paper Award from ICNS'15, Italy; the Best Masters Student Award from ITEX'17; awards from International Exhibitions, Malaysia; and iENA'17, Germany. He has served as the publicity chair, the session chair, a program committee member, and a member of the technical program committee (TPC) for numerous leading conferences worldwide.

MOHAMMAD DAHMAN ALSHEHRI received the Ph.D. degree in artificial intelligence of cybersecurity for the Internet of Things (IoT) from the University of Technology Sydney (UTS), Australia. He is currently an Assistant Professor with the Department of Computer Science, Taif University, Saudi Arabia, and a Visiting Professor with the School of Computer Science, UTS. He developed six smart novel algorithms for the IoT to reinforcement cybersecurity with AI that be able to detect the various behaviours of cyber-attacks and provide full secure and protection platform for the IoT from the most harm cyber-attacks. Furthermore, he published several publications in high ranked international journals, top-tier conferences, and chapters of book. His main current research interest lies in the areas of cybersecurity, artificial intelligence, the Internet of Things (IoT), and trust and reputation. He received number of international and national awards and prizes.

FAZLULLAH KHAN (Senior Member, IEEE) received the Ph.D. degree in computer science from Abdul Wali Khan University Mardan, Pakistan. He is currently working as an Assistant Professor with the Department of Computer Science, Abdul Wali Khan University Mardan. He has published his research work in top-notch journals and conferences. His research interests are security and privacy, the Internet of Things, machine learning, software-defined networks, fog computing, and big data analytics. His research has been published in IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGIES, IEEE TRANSACTIONS ON GREEN COMMUNICATION, IEEE ACCESS, *Future Generations Computer Systems* (Elsevier), *Journal of Network and Computer Applications* (Elsevier), *Computers and Electrical Engineering* (Elsevier), and *Mobile Networks and Applications* (Springer). He has served as the Guest Editor for IEEE ACCESS journal, *Multimedia Technologies and Applications* (Springer), and *Mobile Networks and Applications* (Springer).

MUHAMMAD HALEEM is currently an Assistant Professor with the Department of Computer Science, Faculty of Engineering, Kardan University, Kabul, Afghanistan. His research interests are the Internet of Things, machine learning, and data analytics.