IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 18 May 2023, accepted 3 July 2023, date of publication 12 July 2023, date of current version 21 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3294479

TOPICAL REVIEW

A Comprehensive Survey on the Cooperation of Fog Computing Paradigm-Based IoT Applications: Layered Architecture, Real-Time Security Issues, and Solutions

MUHAMMAD BURHAN[1], HINA ALAM[2], AHMAD ARSALAN[3], RANA ASIF REHMAN[4], (Senior Member, IEEE), MUHAMMAD ANWAR[5], MUHAMMAD FAHEEM[6], AND MUHAMMAD WAQAR ASHRAF[7]

[1]Department of Information Technology, University of the Punjab, Lahore 54590, Pakistan
[2]School of Systems and Technology, University of Management and Technology, Lahore 54770, Pakistan
[3]Faculty of Information Technology and Computer Science, University of Central Punjab, Lahore, Pakistan
[4]Department of Computer Science, National University of Computer and Emerging Sciences, Lahore Campus, Lahore, Pakistan
[5]Department of Information Sciences, Division of Science and Technology, University of Education, Lahore, Pakistan
[6]School of Technology and Innovations, University of Vaasa, 65200 Vaasa, Finland
[7]Department of Computer Engineering, Bahauddin Zakariya University, Multan, Pakistan

Corresponding author: Muhammad Faheem (muhammad.faheem@uwasa.fi)

This work was supported in part by the University of Vaasa and in part by the Academy of Finland.

ABSTRACT The Internet of Things (IoT) can enable seamless communication between millions of billions of objects. As IoT applications continue to grow, they face several challenges, including high latency, limited processing and storage capacity, and network failures. To address these stated challenges, the fog computing paradigm has been introduced, purpose is to integrate the cloud computing paradigm with IoT to bring the cloud resources closer to the IoT devices. Thus, it extends the computing, storage, and networking facilities toward the edge of the network. However, data processing and storage occur at the IoT devices themselves in the fog-based IoT network, eliminating the need to transmit the data to the cloud. Further, it also provides a faster response as compared to the cloud. Unfortunately, the characteristics of fog-based IoT networks arise traditional real-time security challenges, which may increase severe concern to the end-users. However, this paper aims to focus on fog-based IoT communication, targeting real-time security challenges. In this paper, we examine the layered architecture of fog-based IoT networks along working of IoT applications operating within the context of the fog computing paradigm. Moreover, we highlight real-time security challenges and explore several existing solutions proposed to tackle these challenges. In the end, we investigate the research challenges that need to be addressed and explore potential future research directions that should be followed by the research community.

INDEX TERMS Internet of Things, fog computing, edge computing, fog-based IoT, real-time security challenges.

I. INTRODUCTION

In the wake of the invention of computers and the Internet, many experts view the development of the Internet of things (IoT) as a key resolution in information and communication technology (ICT). The IoT facilitates the connection of several smart objects and sensors to the Internet, allowing the collection of data from the physical environment. Through this capability, it allows the automatic and dynamic storage and processing of the accumulated data [1], [2], [3], [4], [5]. Moreover, the IoT is not solely dependent on a single technology but incorporates six essential components within

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

the physical environment: identification, sensing, communication, computation, services, and semantics [6], [7], [8]. The identity of smart objects and sensors is assigned in the identification process, while sensing refers to capturing the data from smart objects and sensors. For this purpose, several technologies such as wireless sensor network (WSN) [9], [10], radio frequency identification (RFID) [11], [12], near field communication (NFC) [13], [14], Bluetooth [15], [16], [17], Wi-Fi [18], [19], and long-term evolution (LTE) [20], [21] are used. Then, the processing is performed on the collected data to extract important and useful data and remove unnecessary data. By using the collected data, the appropriate service and decision are chosen to send a response to the IoT devices. However, the interconnection of these elements enables the applications of IoT such as smart homes [22], [23], health care domain [24], [25], intelligent transportation systems [26], [27], [28], animal tracking [29], [30], and smart robotic grippers [31].
Thus, the growth of IoT applications has led to the generation of vast amounts of data, resulting in heavy network and processing loads. In the process, these vast amounts of data require huge and extensive storage capacity, computing resources, and communication bandwidth. Based on the insights from Cisco, it is expected that the number of Internet-connected devices will exceed 50 billion in the coming years, with an estimated average of seven devices per person being under human control [32], [33]. According to John T. Chambers (former CEO and executive of Cisco), there will be an astonishing 500 billion devices associated with the Internet by the year 2025 [34]. However, the research and academic community is facing a significant challenge in managing the immense and massive amounts of data generated by IoT applications [35], [36].

To address this challenge, the integration of IoT with cloud computing led to the emergence of the Cloud of Things (CoT) [37], [38], [39]. In addition, cloud computing provides a centralized computing model that offers wide computing resources and storage capacity. This integration enables the smooth collection of data from IoT devices and simplifies the computation process for the gathered data [40], [41]. Hence, Figure 1 is used to illustrate the CoT model, where devices transmit data to the cloud directly. Then, an appropriate decision is taken according to the result of analysis and computation, both of which take place in the cloud. Furthermore, the CoT model consists of two layers; (i) the storage and control layer and (ii) the device layer. The storage and control layer provides the facility for the centralized storage and computation of vast amounts of data. For this purpose, it utilizes the IoT devices and the data generated from these devices to control and manage the IoT services. The second layer, the device layer, is composed of IoT devices connected to the Internet, each other, and the cloud. Moreover, the device layer is not restricted to only complicated devices but also includes simple and small objects such as appliances, furniture, and works of art [42]. Thus, common communication mediums (routers, gateways, and bridges) and other communication protocols are used to achieve communication within layers and across layers [43]. This approach has several benefits, such as requiring minimal monitoring and management efforts. As a consequence, it has given birth to a multi-billion industry. Simultaneously, this process requires a substantial amount of network bandwidth to transmit the data directly to the cloud [44], [45]. In addition, the centralization of resources within cloud-based IoT solutions frequently leads to a significant physical gap between IoT devices and the cloud infrastructure. Consequently, this can lead to an increase in average network latency and jitter [46], [47], [48]. As a consequence of the inherent communication delay in cloud computing, end-users face challenges to access time-sensitive applications that require rapid response times and mobility support, such as intelligent transportation systems and augmented reality experiences. Furthermore, the cloud-based IoT communication model faces security and privacy threats for applications that are delay-sensitive, location-aware, and mobility-supported [49], [50].

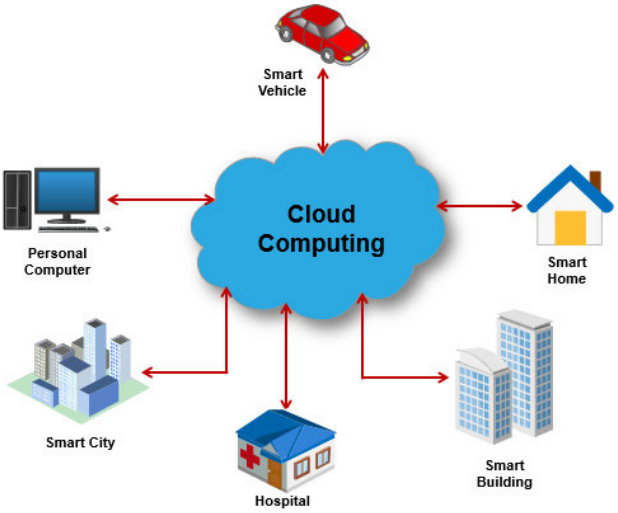

FIGURE 1. The communication model of the Cloud of Things.

The fog computing paradigm is conceptualized as an expansion of the cloud computing paradigm, acting bridge to provide services between end-user devices and cloud servers [51], [52], [53], [54]. Furthermore, this term has also been elaborated by various organizations and researchers according to their perspectives [55], [56], [57], [58]. It is characterized by its decentralized nature. Instead of acting as a substitute for cloud computing, it is an extension of the cloud situated at the network edge in closer proximity to the physical objects. Furthermore, it acts as an intermediary between the end-users and the cloud. It brings computation resources and storage to the network edge and closer to the end-users [59], [60], [61], [62]. In other words, it creates a hierarchical infrastructure, fog platform is used to store the temporary data as well as perform local data analysis. While a cloud platform is used to store the data permanently as well as perform global data analysis [63], [64]. According to the studies of Atlam et al. [65], Zhang et al. [66], Bonomi et al. [67], and Dastjerdi et al. [68], the fog computing paradigm consists of several characteristics, which are summarized as follows:

- Low Latency: IoT devices have a very low physical distance from the fog nodes. Thus, the fog performs data analysis locally separate from the cloud, and, by so doing, provides low latency.
- Location-Awareness: Fog computing supports the awareness of device location, enabling the active or passive tracking of fog nodes to deliver services to devices at the network edge.
- Geographic Distribution: The fog computing paradigm provides services in a distributed form. However, the location of an end user's devices can easily be tracked to support the mobility feature.
- Scalability: The fog computing paradigm provides distributed resources and storage with data analysis to support large-scale IoT devices. In contrast, the centralized cloud requires heavy management to support large-scale IoT devices and IoT applications.
- Physical Distance: The fog nodes can receive the data from IoT devices within a single hop. Thus, data transmission occurs directly and efficiently. In contrast, the cloud computing paradigm receives aggregated data summaries from several devices and within multiple hops.
- Mobility Support: The fog computing paradigm can support high mobility as well as connect to mobile devices. It provides the capability to communicate with mobile devices by using mobility-based communication protocols such as the location ID separation protocol (LISP).
- Bandwidth Saving: The fog computing paradigm reduces the amount of network transmission and saves bandwidth. Because, it expands the functionalities of storage, analysis, and computation at the network's edge.
- Security and Privacy: The fog computing paradigm provides resources (storage, analysis, and computation) at the network edge, bringing them closer to end-users and ensuring that data remains in proximity. Additionally, it provides high security and privacy measurements to the data. In contrast, data stay in the cloud for storage and to perform data analysis and computation in the cloud computing paradigm. Therefore, the cloud provides less security and fewer privacy measures as compared to fog computing.

Table 1 provides a comparison of the fog computing paradigm with other computing models, such as the cloud computing paradigm. The fog computing communication model offers distinct characteristics, such as low latency, location-awareness, decentralized distribution, scalability, less physical distance, support for mobile devices, and bandwidth savings. However, due to these characteristics, it faces some unavoidable security and privacy threats [69], [70], [71], [72], [73], [74]. Furthermore, it is deployed by fog service providers, which may not be as secure and trusted as the more-established cloud providers. Also, IoT devices have limited resources in terms of storage and computing, which can have the effect of making them vulnerable to being compromised and easily hacked, stolen, or broken. Unfortunately, no research and systematic studies to identify the security and privacy challenges, along with security resources in fog computing paradigm-based IoT applications, have yet been conducted. However, the research on security and privacy issues of fog computing paradigm-based IoT applications is still in its early stages. Accordingly, it is essential to conduct a thorough study of the security and privacy requirements to design and implement IoT-based applications.

This survey paper delves into a closer look at real-time security and privacy challenges, such as identity identification, authorization (access control), end-user privacy preservation, intrusion detection and prevention, and trust management in fog computing-based IoT applications. All of these challenges make clear the necessity to provide a promising method for building IoT applications that provide secure and reliable real-time services for the end-users. The contributions made by this article are summarized as follows:

- This article makes specific contributions to the proposed layered architecture of fog-based IoT applications.
- It also constructs a picture for understanding the working of IoT applications under the fog computing paradigm.
- This article demonstrates real-time security and privacy challenges, such as authentication, authorization, end-user privacy preservation, intrusion detection and prevention, and trust management, which may affect the fog-based IoT network as well as end-users.
- It also reviews the possible existing and promising solutions to ensure reliable and secure real-time services for fog-based IoT applications.
- Further, this article also highlights the research challenges and suggests future research directions for the research community.

Furthermore, the organization of this article is as follows:

- Section I is used to describe the introduction of IoT. In addition, this section also presents the introduction of cloud computing and fog computing along with their characteristics.
- Section II presents the architecture of fog computing-based IoT applications.
- Section III is used to highlight real-time security issues, such as authentication, authorization, end-user privacy preservation, intrusion detection and prevention, and trust management. Further, this section also presents the existing possible solutions.
- Section IV is used to describe the research challenges and future research directions.
- Section V is used to elaborate the conclusion of this article as final remarks.

TABLE 1. The comparison of the fog computing paradigm over the cloud computing paradigm.

Sr.	Characteristics	Fog Computing Paradigm	Cloud Computing Paradigm
1	Latency	It provides low latency to IoT applications.	It provides high latency to IoT applications.
2	Location-Awareness	It supports the characteristic of location awareness.	It does not support the characteristic of location awareness.
3	Distribution	It provides geographical distribution.	It provides centralized distribution.
4	Scalability	It can support a large scale of IoT applications.	It faces management overhead to support large-scale IoT applications.
5	Physical Distance	It transmits data from IoT devices within one hop.	It receives data in aggregated and summarized form. Generated by multiple devices.
6	Mobility Support	It provides high support to IoT mobile devices.	It does not provide high support to IoT mobile devices.
7	Bandwidth	The computation resources are offered at the network edge, resulting in bandwidth savings.	The computation resources exist in the cloud. However, IoT devices require high bandwidth.
8	Security and Privacy	It provides high-security measurements of data.	It offers fewer security measures.
9	Real-Time Interaction	To facilitate immediate communication, it enables real-time transmission of data between IoT applications and services.	To facilitate immediate communication, it enables real-time transmission of data between IoT applications and services.
10	Communication Delay	The proximity of resources to end-users significantly reduces transmission delays between IoT devices and fog nodes.	The availability of resources on the cloud may lead to transmission delays.

II. LAYERED ARCHITECTURE OF FOG COMPUTING-BASED IOT NETWORK

The fog computing paradigm relocates the operations closer proximity to the end-users of IoT applications. Its key objective is to provide low latency and save bandwidth to ensure the reliable and secure real-time and time-sensitive services of IoT applications [75], [76]. According to Ni et al. [77], the architecture of a fog-based IoT network consists of a cloud–fog–device framework, where three layers exist, named the cloud, the fog, and the IoT device layer. In contrast, according to [78], [79], [80], and [81], there are six layers, named, the physical, the monitor, the pre-processing, the transit, the security, and the transport layer. This section provides an overview of the proposed layered architecture for an IoT network based on fog computing.

A. THREE-LAYERED ARCHITECTURE OF FOG-BASED IOT NETWORK

Figure 2 demonstrates the basic architecture, consisting of the three-layers.

1) DEVICE LAYER

This layer is composed of IoT devices. Further, two types of IoT devices exist in this layer; mobile devices and static devices. Thus, mobile devices can transmit data through wireless and ad hoc manners [82]. In addition, static devices cannot respond to emergency events. According to Gazis [83], these devices have limited resources (storage, analysis, and computation) along with limited bandwidth for the transmission of data. Therefore, these devices have pre-defined functionalities to perform monitoring tasks on a product or building. In addition, fog computing includes the characteristic of location awareness. These devices, mobile and static, may have GPS enabled in them and sense the physical environment and collect data. Then, the collected data are sent to the fog layer for transit storage as well as analysis and computation. Similarly, these devices also can respond to the physical environment according to the instruction and information directed by the middle layer, the fog layer.

2) FOG LAYER

This layer consists of a variety of network equipment that can perform computation, for example, router, switches, bridges, etc. These devices are known as fog nodes. Further, this layer extends the cloud computing paradigm to the network edge as well as nearer to the end devices. The fog nodes can perform real-time data storage, data analysis, and computation. By so doing, the computation load on resource-constrained IoT devices is reduced. The fog nodes are at a shorter physical distance from the IoT devices, as they exist one hop away from the IoT devices. Therefore, they maintain provisional knowledge regarding the end-users and their devices such as location information. In addition, this layer receives the data from IoT devices to perform data analysis and computation and provide temporary data storage capacity. Then, data is sent to the cloud through other nodes or directly.

3) CLOUD LAYER

Cloud data centers exist in this later. It has significant amounts of data storage space and computation resources. It also can access Internet-connected end-users at any time and from anywhere. Further, the cloud receives the data in a summarized form from fog nodes, where the analysis process is performed on the collected data to improve the quality of applications and services provided by the IoT [84], [85], [86], [87].

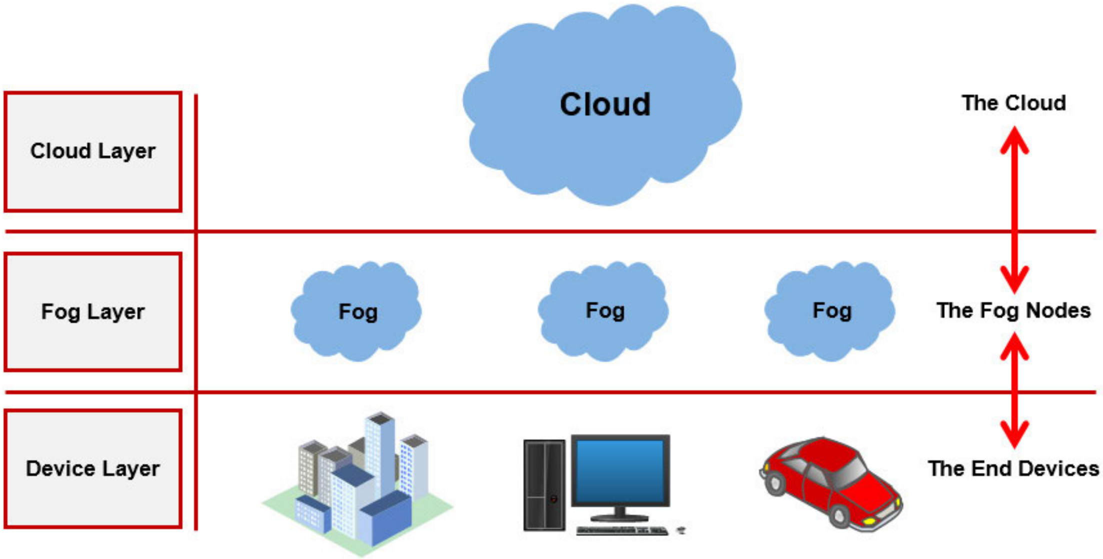

FIGURE 2. The basic, three-layered architecture of a fog computing-based IoT application.

B. SIX-LAYERED ARCHITECTURE OF FOG-BASED IOT NETWORK

Figure 3 demonstrates the complex and secure layered architecture of a fog-based IoT network, consisting of a six-layered hierarchy.

1) PHYSICAL LAYER

This layer consists of IoT devices, which are enabled with GPS to fulfill the requirements of fog computing and are distributed geographically. Further, these devices can sense the physical environment.

2) MONITOR LAYER

This layer is used to monitor the whole network, including IoT devices and fog nodes in terms of resource utilization, availability, and accessibility of all networks. It also monitors the functionality provided by a device, for example, which device is performing what task and at what time.

3) PRE-PROCESSING LAYER

This layer performs the task of the management level. It analysis the vast amount of data coming from IoT devices by using several filtering and pruning algorithms to extract useful information. Moreover, fog nodes have limited data storage space as compared to the cloud. However, this layer is considered to be necessary for fog computing-based IoT applications.

4) TEMPORARY STORAGE LAYER

There are two types of data generated by IoT applications; sensitive and less-sensitive data. The data that requires a real-time response on an immediate basis, whenever an emergency event occurs, is known as sensitive data. However, the temporary storage layer is used to provide transit data storage as well as perform real-time analysis and computation. Besides this, temporary storage is not provided for the data generated by the less-sensitive applications of IoT. These applications sent data directly to the cloud.

5) SECURITY LAYER

This layer provides cryptography where the encryption and decryption of data come into play. It collects data from the bottom layer (temporary storage layer) and performs encryption by converting all collected data into an unreadable form. To perform encryption, the key used is known by the owner of the data. Furthermore, the security layer conducts integrity measures to detect any attempts to tamper with the data by an attacker.

6) TRANSPORT LAYER

This layer gathers the encrypted data from the security layer, which it sends to the cloud where analysis is performed. Furthermore, data may be stored for a long time.

To understand the working of IoT applications under the fog computing paradigm, let us consider Figure 4, where the high-level architecture of fog computing-based IoT applications is represented. The fog nodes are deployed at the edge of the network and closer to the IoT devices, where they collect data from IoT devices. They can be in the form of simple network equipment such as routers and gateways, or complex devices such as embedded servers and video surveillance cameras. These devices have been built with intelligent. However, the data generated by the sensitive applications is stored, analyzed, and computed on intelligent devices. Thus, any sign of problems can be detected comparatively closer to the IoT devices, enabling the fog nodes to respond to the IoT devices

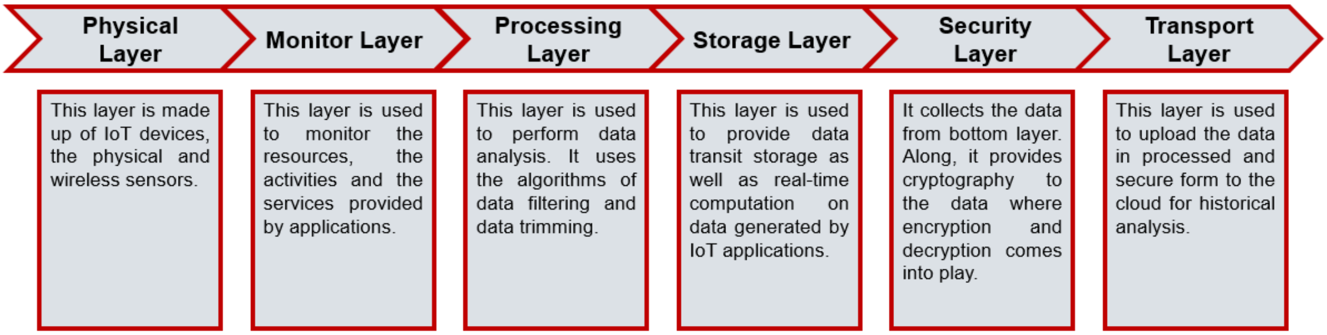
Physical Layer
Monitor Layer
Processing Layer
Storage Layer
Security Layer
Transport Layer
This layer is made up of IoT devices, the physical and wireless sensors.
This layer is used to monitor the resources, the activities and the services provided by applications.
This layer is used to perform data analysis. It uses the algorithms of data filtering and data trimming.
This layer is used to provide data transit storage as well as real-time computation on data generated by IoT applications.
It collects the data from bottom layer. Along, it provides cryptography to the data where encryption and decryption comes into play.
This layer is used to upload the data in processed and secure form to the cloud for historical analysis.

FIGURE 3. The secure and six-layered architecture of fog computing-based IoT applications.

immediately whenever needed. In contrast, the data generated by less-sensitive applications are sent to the cloud by using fog nodes or directly. The cloud provides data storage capacity, analysis, and computation, as the data cloud center has a significant amount of data storage capacity. The data can be stored here for months and years. The cloud can be used to perform various functionalities, such as big data analytics, parallel processing, and machine learning. In addition, several technologies are used to achieve communication within each layer and across layers, including wired communication and wireless communication; wired communication includes Ethernet and fiber optic technology, while wireless communication includes routers, gateways, switches, bridges, satellite links, and IEEE 802.11 a/b/c/g/n/p [88].

III. REAL-TIME SECURITY ISSUES AND SOLUTIONS FOR FOG COMPUTING-BASED IOT APPLICATIONS

The fog computing communication environment includes numerous characteristics for IoT applications, such as location awareness, device mobility, low latency, geographic distribution, wireless access, and heterogeneity [89]. Meanwhile, there is a variety of security and privacy threats exist in computing. Therefore, there is a need for a protection mechanism to provide security to fog-based IoT applications, otherwise, the end users cannot trust the network and use and enjoy the real-time services of IoT applications. Thus, this study chooses to focus on secure and reliable real-time services for IoT applications.

In the following section, we review several security challenges concerning real-time services. We divide the literature into five categories based on the real-time services of IoT applications, namely, authentication, access control, end-user privacy, intrusion detection and prevention, and trust management, as shown in Figure 5. We also introduce some existing promising solutions that can be used to address and overcome these challenges. Moreover, we identify existing and possible solutions to make sure the authentication and access control rights in the network and prevent the network from being accessed by an attacker while preserving and mitigating the private information of end-users from being accessed by an attacker. Furthermore, we present the techniques used in the proposed solutions and demonstrate their advantages and limitations.

A. AUTHENTICATION

The IoT concatenates the real-time services provided by smart objects and sensors to enable communication with the physical environment. Therefore, this characteristic of the IoT leads to various security challenges, where attackers can gain network access, utilize the resources of the network, and affect the infrastructure without having correct credentials or suffering any liabilities. However, it is a difficult task to secure authenticity and creditability before accessing the services, while providing guarantees that all entities involved in the communication process are trusted. For example, an attacker may pretend to be an intended user to gain access and utilize the services of the network without leaving a mark of evidence of the intruder's misbehavior and malicious activities.

1) EXISTING SOLUTIONS FOR AUTHENTICATION

Several methods have been proposed to mitigate the problems of authenticity and provide security and reliability for communication in the network. Thus, the following sub-section presents the existing promising solutions to ensure authenticity in the network, in the forms of identity authentication, cooperation-based authentication, and anomaly authentication.

a: IDENTITY-BASED AUTHENTICATION

Loffi et al. [90] used the existing multi-factor mutual authentication protocol and proposed a new flexible method that made use of a challenge-response function, a nonce, and an adjustable variable response time to improve the accuracy of their model. Furthermore, elliptic curve cryptography serves as the encryption cipher in the proposed model.

Chandrasekhar and Singhal [91] proposed an authentication strategy. It aims to provide integrity and authenticity for cloud storage when data comes from multiple sources and is accessible by multiple users. While such dangers exist, cloud computing does provide the benefits of flexibility, scalability, low cost, accessibility, and availability. The proposed

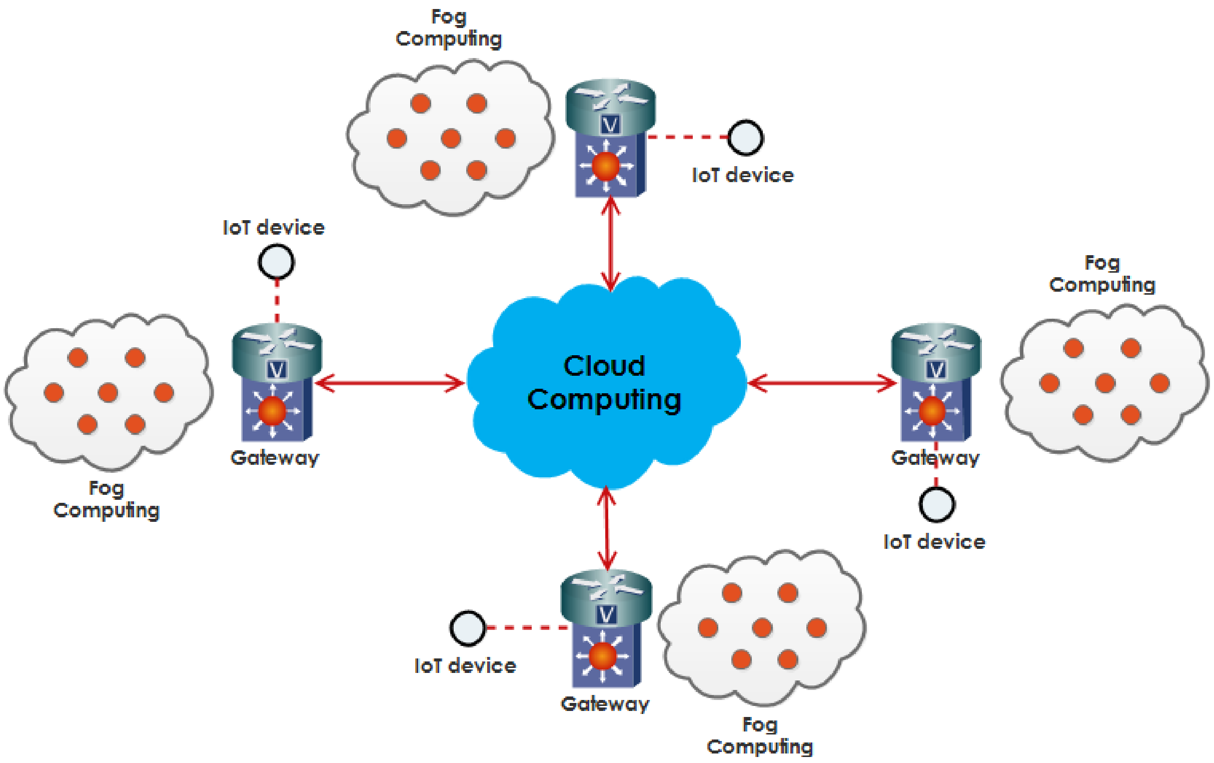

FIGURE 4. The high-level architecture of IoT applications clarifies the working of its devices under the fog computing paradigm.

query-based authentication strategy is constructed by using a multi-trapdoor hash function and a special enhanced form of encryption [92], [93]. It permits clients to validate the accuracy and authenticity of query results while achieving minimal communication and computation overhead.

An alternative authentication scheme involves the development of a secure and authenticated key agreement strategy specifically designed for smart grid applications [94]. Moreover, this scheme is based on the Canetti-Krawczyk (CK) adversary model [95], [96]. According to it, an authentication model should provide the property to make secure all the past sessions and future sessions as well. However, the authors reported the Tsai and Lo scheme [97], which is considered to be the first anonymous scheme. At the same time, it provides weak security measurements and may permit leaks to numerous security attacks such as a session exposure attack. However, Odelu et al. proposed a protocol to overcome the security weaknesses that exist in the Tsai and Lo scheme. The authors asserted that their proposed protocol requires low computation costs to provide a variety of security functionalities. It also establishes security for the session keys in the CK adversary model.

Jiang et al. [98] proposed an authentication scheme to ensure authentication between two entities in a wireless sensor network (WSN) environment. Further, the authors enhance the work of He et al. [99] to increase efficiency as well as enable resistance against various known attacks such as user impersonation and eavesdropping attacks. However, the proposed scheme has two phases; registration and authentication phase. The registration of users is performed in the first phase, which employs the elliptic curve cryptography (ECC) model instead of modular exponentiation. In the second phase, the login and the authentication are performed to establish a session key whenever users want to use the sensed data. In addition, the proposed scheme can fulfill the requirement of mutual authentication that exists in Burrows–Abadi–Needham (BAN) logic [100]. Therefore, it is considered to be untraceable and enables resistance against known attacks.

Hu et al. [101] proposed a scheme in combination with data encryption and data accuracy to overcome the issues of confidentiality, integrity, and availability for the communication process of face identification and face resolution applications in fog computing-based IoT. For these purposes, it provides three key countermeasures, consisting of authentication and session key agreement, advanced encryption standard (AES) based encryption mechanisms, and a hash data integer algorithm. The session key is generated by using the algorithm of Diffie–Hellman key agreement [102], [103]. In addition, the AES symmetric key encryption algorithm is used to ensure the confidentiality of the data. A hash data integer algorithm, for example, SHA-I, is used to confirm the integrity or accuracy of the data. The experimental results demonstrate that the proposed scheme introduces a slight

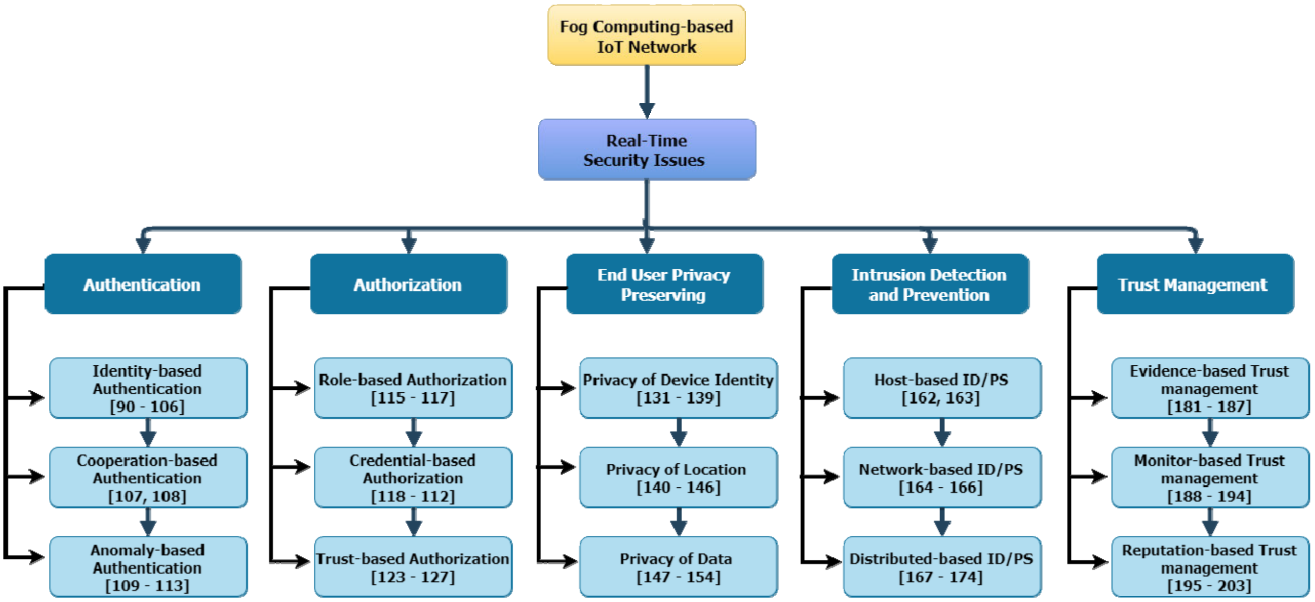
Fog Computing-based IoT Network
Real-Time Security Issues
Authentication
Authorization
End User Privacy Preserving
Intrusion Detection and Prevention
Trust Management
Identity-based Authentication [90 - 106]
Cooperation-based Authentication [107, 108]
Anomaly-based Authentication [109 - 113]
Role-based Authorization [115 - 117]
Credential-based Authorization [118 - 112]
Trust-based Authorization [123 - 127]
Privacy of Device Identity [131 - 139]
Privacy of Location [140 - 146]
Privacy of Data [147 - 154]
Host-based ID/PS [162, 163]
Network-based ID/PS [164 - 166]
Distributed-based ID/PS [167 - 174]
Evidence-based Trust management [181 - 187]
Monitor-based Trust management [188 - 194]
Reputation-based Trust management [195 - 203]

FIGURE 5. **The real-time security challenges in fog computing-based IoT applications.**

increase in communication and computation overhead while ensuring system confidentiality, integrity, and availability. Additionally, the fog computing paradigm highlights the need for secure and reliable information rather than outdated information. Hence, it can be thought of as a limitation of the proposed scheme because it deals with the retroceded information. Furthermore, this article does not consider the mobility feature of IoT devices.

Software-defined networking (SDN), where switches act as fog nodes simultaneously, can be a good choice for a fog computing-based IoT network to manage network flow automatically and dynamically [104]. In SDN, the controller is used to control and manage all switches through the OpenFlow channel to transmit commands and requests as well as states against commands and requests from the switches. Therefore, it is imperative to ensure the security of the OpenFlow channel in SDN [105]. However, Li et al. [106] detect a MiTM attack and packet modification utilizing a bloom filter. The bloom filter acts as an efficient data structure to test the existence of any fabricated and fake element in a given set. Hence, the controller can detect packet fabrication and modification by collecting all bloom filters. If there are differences between filters, the controller detects it as a MiTM attack and confirms that the packets are fabricated and modified during their transmission. Furthermore, the authors highlight that if an attacker intercepts an OpenFlow channel that consists of a one-flow path between the controller and switches, the proposed scheme does not work. In other words, if the OpenFlow channel consists of one flow path, the proposed scheme cannot detect the MiTM attack between the controller and the switches. At the same time, the proposed scheme does not provide a solution for mobile devices.

b: COOPERATION-BASED AUTHENTICATION

Lin and Li [107] and Zhou et al. [108] have made some efforts to propose cooperation-based authentication schemes for users. These proposed schemes are used to reduce communication and computation overhead. These schemes do not require a trusted authority to perform the process of authentication. Thus, they shorten the delay to authenticate the individuals. Moreover, these schemes accept the cooperation of neighbor nodes to eliminate the unnecessary authentication process on the same message through different users. However, these schemes can resist numerous attacks, such as a free-riding attack where fake and unnecessary efforts are not consumed in the network. Furthermore, these schemes encourage user cooperation and accept the help of adjacent neighbor nodes to avoid entangling the system's resources in unnecessary and time-consuming authentication processes.

c: ANOMALY-BASED AUTHENTICATION

When using the real-time services of IoT applications, end users expect to avoid disclosing private information regarding their identity during the authentication process. If an attacker intercepts information, he/she would be able to identify the trajectory and intersection information of the user [109], [110]. However, Lu et al. [111] proposed an approach to enable the nodes to verify the credentials of end users without extracting the identity information of the user such as a user's location. However, nodes cannot distinguish the target users. Furthermore, extensive experiments are not performed by the authors to confirm the effectiveness of the proposed approach, nor did they identify what they present as a strong threat model.

Kumar et al. [112] designed an ensemble learning-based IDS for the IoMT network to identify cyber-attacks using fog-cloud architecture. The proposed scheme consists of two engines; traffic processing and intrusion detection engine. The first engine includes feature mapping, feature selection, and feature normalization. The authors make use of the XGBoost-based ensemble method with various machine-learning techniques to train their system for detecting cyber-attacks. In the intrusion detection engine, the authors made use of the ToN_IoT dataset to test the proposed detection system and claimed that this approach is capable of achieving an accurateness of 96.35%, and a detection rate of 99.98%. Moreover, it can minimize the false alarm rate by up to 5.59%. According to the authors, they have proposed the first ensemble learning-based IDS for the IoMT environment using fog-cloud architecture.

In addition, Manimurugan [113] developed the IoT-Fog-Cloud computing model with the help of the machine learning approach. This proposed approach aims to recognize the cyber-attacks in the IoT smart city. The model was trained using the Improved Naïve Bayes algorithm on the UNSW-NB15 dataset to detect attacks. The authors claimed that the proposed approach outperforms in terms of detection rates and accuracy.

Thus, Table 2 summarizes all the proposed existing and promising solutions to ensure authentication in the network. It also provides techniques for overcoming the problem and presents the advantages and limitations of the proposed solutions.

B. AUTHORIZATION

An authorization mechanism plays a critical role in the IoT ecosystem by allowing control and management of access to information and resources within the network. It ensures that only authorized entities can utilize the network's resources. In addition, it also prevents unauthorized access to sensitive information and resources. The IoT implements two types of authorization mechanisms; physical and logical authorization [114]. Thus, both forms of authorization mechanisms have become much-criticized as well as a challenging task in IoT applications. Once implemented, an authorization mechanism asks the following questions:

- What mechanism should be allowed to access the specific and required service?
- Which users have the authority to access specific information?
- Which types of operations are allowed to be the user after accessing the service of the network?

1) EXISTING SOLUTIONS FOR AUTHORIZATION

Several mechanisms have been proposed to ensure authorization (access control) and make it impossible for malicious attackers to utilize the system's resources and information. In the following subsection, we investigate the various proposed solutions for authorization mechanisms, including role-based authorization, credential-based authorization, and trust-based authorization.

a: ROLE-BASED AUTHORIZATION

Role-based authorization mechanisms are used in traditional systems to provide access privileges to network resources and information by using the roles of individuals, for example, doctors, professors, managers and assistants, and so on [115]. For better understanding, let us consider an example. In case of a road accident, the doctor must have access to the user's location to ensure timely and effective medical support. Ordinarily, of course, information regarding the user's location should be kept confidential. Hence, Hu et al. [116] presented a system based on user identity to effectively control and manage location information and other private credentials in emergencies. Nevertheless, it ensures that only an authorized user can use the user's private information. In the case of regular situations, the system does not show information to any individual. Moreover, the IoT consists of nodes that have dynamic characteristics and possess constrained computing power and storage capacity. Therefore, the proposed scheme is thought to be limited applicability due to these limitations.

Dang and Hoang [117] presented a model for managing mobility and securing data in the fog environment. The proposed model features three modules that serve distinct purposes. Firstly, the Fog-based Privacy-aware Role-Based Access Control (FPRBAC) module enables authorization between fog nodes within the network. Secondly, the Region-Based Trust-Aware (RBTA) module assists trust translation among fog nodes belonging to different regions. Lastly, the mobility management service module handles location requests within a region model.

The model implemented the mobility service with location registration that addresses the location issues by storing various information about fog devices. It is based on values of trust between regions where fog nodes can join and leave within relevant assigned roles. The FPRBAC module serves the purpose of authenticating requests for users to access computing resources from fog nodes. This authentication process is based on granting permissions that have been assigned to the respective roles. Furthermore, the experimental results demonstrated that the proposed model exhibits superior performance compared to other approaches.

b: CREDENTIAL-BASED AUTHORIZATION

In a credential-based authorization mechanism, a special type of certificate is required from the user to access resources and information related to the network. However, an attacker must be unable to bypass the authorization mechanism without a required certificate of information. Therefore, this mechanism is considered to be secure and authenticated in the IoT environment. The credential-based access control mechanism encompasses two types: attribute-based access control and capability-based access control [118]. In attribute-based authorization, each user has a special type of attribute, which is used to access a particular resource or piece of information. However, Lewko and Waters [119] proposed a model that

TABLE 2. The proposed solutions and their classification on real-time authentication in fog computing-based IoT applications.

Scheme	Type	Technique(s)	Advantages	Drawbacks
Leandro Loffi et al. (2021) [90]	Identity-based Authentication	- Mutual and multi-factor authentication method	It improves performance cost, energy consumption, and runtime performance as well. Furthermore, the communication cost is the same as compared to other studies.	It uses a complex algorithm.
Chandrasekhar and Singhal (2017) [91]	Identity-based Authentication	- Multi-trapdoor hash function - Enhance form of encryption	It ensures the problem of correctness and authenticity of query results. It achieves constant communication and computation overhead.	It only ensures the correctness of query results.
Odelu et al. (2018) [94]	Identity-based Authentication	- Identity-based Signature	It is considered a secure and authenticated key agreement protocol for communication.	It may face the effect of tracking attacks and impersonating attacks.
Jiang et al. (2016) [98]	Identity-based Authentication	- Elliptic curve cryptography - Burrows-Abadi-Needham (BAN) Logic	It ensures the authentication between the user-sensor and the user gateway. It resists various known attacks, such as eavesdropping and user impersonation.	This model does not consider the wormhole and black hole attack.
Hu et al. (2017) [101]	Identity-based Authentication	- Session key agreement and authentication - AES symmetric key encryption - Hash data integer (SHA-I)	It ensures confidentiality, integrity, and authentication during communication between entities. It can detect MiTM and identity forgery attacks.	It increases little bit communication and computation overhead. Further, it deals with retroceded information. Further, mobility parameters are also not considered.
Li et al. (2017) [106]	Identity-based Authentication	- Bloom filters	It includes the cooperation of SDN to detect packet fabrication and modification using a bloom filter.	It cannot detect the MiTM attack if OpenFlow consists of one flow path.
Lin and Li (2013) [107]	Cooperation based Authentication		It provides high support to IoT mobile devices.	It does not provide high support to IoT mobile devices
Zhou et al. (2015) [108]	Cooperation based Authentication	- Cooperation of adjacent nodes	It does not involve the trusted party performing the authentication process. It takes help from neighbor nodes. It can resist attacks, such as free-riding attacks.	It does not hide the location of the devices. However, this model is not suitable for location-based applications.
Lu et al. (2012) [111]	Anomaly-based Authentication	- Anomaly method	It enables authentication without extracting personal information.	The authors did not perform enough experiments. Further, they did not use a strong threat model.
Prabhat Kumar et al. (2021) [112]	Anomaly-based Authentication	- XGBoost-based ensemble method that combines DT, NB, and RF to	It detects malicious activities in the IoMT network. Furthermore, the ToN_IoT dataset shows high accuracy	It is not capable of detecting malicious activities, such as DDoS and ransomware. It only detects normal and abnormal

TABLE 2. ***(Continued.)*** **The proposed solutions and their classification on real-time authentication in fog computing-based IoT applications.**

			design the detection model	and detection rate.	instances.
S. Manimurugan (2021) [113]	Anomaly-based Authentication	-	Improved Naïve Bayes classifier based on the principal component analysis technique	It improves the efficiency of anomaly detection. Further, shows high accuracy and detection rate.	There is still a requirement to further improve and update the system to cover the physical attacks.

establishes a policy system in which each user is given certain attributes according to his/her requirements. To use a particular resource or piece of information, the user's attributes are matched with the pre-defined rule system. Once the user's attributes meet the criteria defined in the rule system, they become able to access the required resource or information.

In contrast, the second type of credential-based access control, capability-based authorization, recognizes the communicable and unforgettable markup as being unique and uses it to access the privileges of resources or an item of information. The key concept of capability is introduced in [120]. However, Hernández-Ramos et al. [121] presented a distributed model that depends on the existing abilities of smart objects in respect of communication and computation power. In the proposed model, the owner of the resource or service provides authorization certificates to the individuals who want to use it. However, the user has to possess such an authorization certificate er to perform the corresponding resource or service request operation. Furthermore, the authors acknowledge the principle of least privilege to manage and control access to a resource or item of information. It provides security to the system as a centralized mode in terms of end-to-end level validation, although it requires each user to have the ability to publish a key certificate. Therefore, this process is one drawback of the proposed model, which needs, in addition, further enhancements to overcome security obstacles.

Yao et al. [122] presented a study on the privacy and security limitations present in existing symmetric and public key cryptosystems within the fog environment. The authors proposed an innovative approach called attribute credential-based public key cryptography (AC-PKC) that provides authentication, access control with privacy preservation, and flexible key management. In the proposed approach, they introduced registered but anonymous attribute credentials for fog nodes. It uses a combination of elliptic curve cryptography (ECC) and certificate-less public key cryptography (CL-PKC) to establish a robust public-key scheme. It effectively addresses security concerns such as authentication, encryption, and access control with privacy preservation. Furthermore, the performance of the proposed approach was evaluated based on various aspects including security, computation overhead, privacy preservation, communication overhead, and flexibility. Through performance analysis and comparison, it was demonstrated that the proposed approach offers a dynamic security mechanism suitable for fog computing.

c: TRUST-BASED AUTHORIZATION

Traditional authorization mechanisms are not compatible with the unique challenges offered by distributed IoT, applications where roles and credentials are used to authorize the users. However, a trust-based authorization mechanism is considered to be an advanced extension of traditional authorization mechanisms for IoT devices. However, Bernabe et al. [123] presented a network strategy to ensure reliable and effective communication between smart IoT devices that the authors call the TAC-IoT. It is based on values of trust such as reputation, quality of service, and security considerations along with social equipment. Furthermore, constrained and unconstrained devices have been used to implement and evaluated the proposed network.

In addition, Mahalle et al. [124] proposed an authorization model based on fuzzy trust values such as experience, knowledge, and recommendations, which they named FTBAC. The trust values are assigned by the appropriate authority. Moreover, the authorization model presented in this study comprises three distinct layers: the device layer, the requesting layer, and the authorization layer. The device layer consists of the IoT devices involved in the communication process, illustrating their interconnectedness and functionality. Hence, the requesting layer is used to collect the factors of knowledge, experience, and recommendation values to evaluate the fuzzy trust values. The third layer, authorization, is used to make decisions about collecting fuzzy trust values.

Another study carried out by Daoud et al. [125], focuses on developing an efficient distributed access control model for Fog-IoT networks following a secure resource allocation management framework to guarantee a high-security level between different resources and operational parts by adding real-time constraints. They introduced a comprehensive scheduling process and efficient mechanism for resource allocation to guarantee improved performance and the lowest latency level.

In another study [126], the authors proposed a security framework for Fog-IoT systems comprising two key components: the Trust Management Component (TMC) and the Security Component (SC). The SC guarantees the authentication, authorization, integrity, and confidentiality of data, while the TMC assesses the performance of Fog-IoT nodes using a trust model based on network communication and Quality of Service (QoS) parameters. The access control policies within the SC incorporate trust values to certify that only trusted nodes can access fog resources. The model was tested using Raspberry Pi 3 Model B+ and subjected to various networks to evaluate its memory and time complexity.

One more research study conducted by Zhang et al. [127] proposed a secure multi-cloud collaboration model based on trust values to address security concerns arising from untrusted service providers or malicious users in the Cloud-Fog environment. The researchers propose a role-based trust evaluation scheme to enhance user security in the context of Multi-Cloud Service Composition (MCSC). In addition, the study puts forth secure collaboration and an efficient user authentication scheme to safeguard service security. The proposed framework employs a single sign-on technique, ensuring that only authenticated users can access component services using a single set of credentials. The authors performed extensive testing and analysis to confirm the suitability of the proposed, particularly in terms of user and service security protection.

Table 3 summarizes all the proposed existing and possible solutions to ensure authentication and prevent the access of an attacker in the network, along with techniques that can overcome the problems. In addition, it presents the advantages and limitations of the proposed solutions.

C. END-USER PRIVACY PRESERVING

The fog computing-based IoT communication paradigm requires two-way communication. Firstly, the data is gathered from the physical environment and subsequently transmitted to the fog nodes. Then, the nodes possess the capability to store the gathered data and can also transmit it to the cloud as per the requirements of the application. During this process, end-user privacy is critical to prevent data leakage from being detected by malicious attackers. Three types of privacy issues exist in fog-based IoT applications [128]. The first is the privacy of IoT devices. The resource constraints of IoT devices make them vulnerable to a decreased capacity for performing encryption and decryption processes on data, thereby interpreting them as vulnerable to malicious attacks. Thus, an attacker becomes able to steal the private information exchanged between two entities. There are several types of mobile computing applications of the IoT, which provide location-based services. However, location privacy is considered to be a second privacy issue because the place of equipment can provide information regarding the owner. Therefore, a malicious attacker may infer the IoT mobile devices [129], [130]. The last privacy issue is the protection of the user's data generated by IoT devices. Therefore, privacy leakage of users in IoT applications has attracted the attention of the research community as well as academia and industry.

1) EXISTING SOLUTIONS FOR END-USER PRIVACY PRESERVING

The following sub-section describes the existing solutions regarding how IoT devices handle identity privacy, location privacy, and data privacy.

a: PRIVACY OF DEVICE IDENTITY

Guan et al. [131] designed a new scheme for fog- IoT systems that offer multi-authority for locally managing the devices. It uses the Paillier algorithm during data aggregation for data privacy. The authors proposed the integration of a local certification authority with specialized fogs at the network edge to handle pseudonym management, permitting real-time service for device registration and updates. The experimental results comparing the scheme to existing ones shows the suitability of the proposed scheme for fog-enhanced IoT systems.

Zhang et al. [132] highlight the limitations of the conventional PPDA solutions that have been previously used for protecting IoT devices and proposed a scheme to overcome the performance and privacy issues that occurred by the resource constraint of IoT devices. It integrates a paillier homomorphic encryption method and an online/offline signature technique to guarantee integrity verification and privacy-preserving during the data aggregation process. The comprehensive security analysis conducted by the authors shows that the proposed technique gives promising results.

According to Khan et al. [133], many privacy-preservation strategies have been proposed for fog-enabled aggregation, but there is no proper scheme in fog-enabled smart grids for fault tolerance that allows the system to produce accurate results even in the presence of faulty meter, Therefore, the proposed approach introduces a robust and distributed data aggregation technique in the fog-based environment. This technique ensures fault-tolerance and offers important security. Furthermore, the scheme utilizes the Boneh-Goh-Nissam (BGN) cryptosystem for metering data privacy, while the elliptic curve digital signature algorithm (ECDSA) is selected for source authentication due to its smaller key sizes and efficiency on resource-constrained devices. The scheme also addresses replay and false data injection attacks, ensuring the authenticity and confidentiality of user data.

Lu et al. [134] proposed a lightweight privacy preservation and data aggregation scheme for fog computing-based IoT applications. This scheme permits the aggregation of data from various types of IoT devices. To ensure data security, the proposed scheme employs three techniques: homomorphic Paillier encryption [135], the Chinese remainder theorem [136], and a one-way hash function. These techniques are specifically designed to solve the limitations of IoT devices with limited bandwidth. Furthermore, false data injection attacks can also be resisted by enhancing the security of the proposed model. As a result, as compared to the basic strategy of privacy preservation based on Paillier encryption [137], this model is likely to be effective in respect of fault tolerance, communication overhead, and computation

TABLE 3. The proposed solutions and their classification on real-time authorization in fog computing-based IoT applications.

Scheme	Type	Technique(s)	Advantages	Drawbacks
Hu et al. (2011) [116]	Role-based Authorization	- Roles of individual	It reveals private information in an only emergency to an authorized individual.	Due to its dynamic nature, mobility, limited computation resources, and storage, the applicability is considered limited.
Thanh Dat and Doan Hoang (2017) [117]	Role-based Authorization	- Region-Based Trust Aware (RBTA) Model	It offers the capability to protect the data.	The assessment of the model does not encompass the aspects of feasibility and efficiency.
Lewko and Waters (2011) [119]	Credential based Authorization	- Attributes-based Access Control	The utilization of resources is depending upon the satisfaction of pre-defined policy criteria related to the user's attributes.	It may face the issue of role explosion. The management of roles is considered complex. Along, It is complex to analyze as attributes need maintenance and provisioning.
Harnandez-Ramos et al. (2013) [121]	Credential based Authorization	- Capability-based Access Control	It uses the principle of least privilege. It requires an authority certificate from the end user to access resources or information.	It may face management overhead as it requires a key certificate each time. Further, it needs to overcome security obstacles.
Xuanxia Yao et al. (2019) [122]	Credential based Authorization	- Public Key Cryptography - Elliptic Curve Cryptography (ECC)	It is suitable for distributed and dynamic fog computing environments. Further, it provides flexibility, privacy-preserving, and relatively low computation and communication cost.	It is a complex system, especially for fog-based applications.
Bernabe et al. (2016) [123]	Trust based Authorization	- Trust values e.g., reputation, QoS, security, and social equipment	It ensures communication between two entities by using trust values.	The utilization of trust is not defined. Further, there is no strategy to deal with malicious attackers.
Mahalle et al. (2013) [124]	Trust based Authorization	- Fuzzy-based trust value - The experience, knowledge, and endorsement	It ensures authorization during communication within the network by assigning trust values to devices. The values are assigned by an appropriate authority.	It increases time and energy consumption as it takes access to the controls by increasing the trust values.
Wided Ben Daoud et et al. (2019) [125]	Trust based Authorization	- A distributed access control based on a security resource management framework	It offers low latency, thus reducing the complexity involved in administering and managing security and resource allocation.	The model does not consider the mobility model for the devices.
Junejo et al. (2020) [126]	Trust based Authorization	- Attribute-based access control - Trust-based behavioral monitoring	It is a lightweight mechanism for resource-constrained devices.	The model is evaluated using a few numbers of attacks.
Jiawei Zhang et al. (2022) [127]	Trust based Authorization	- Trust values-based model	It provides security to the devices using two components; a trust management component and a security component.	It is a complex model to deal with mobile devices.

cost. However, it does not include the feature of traceability, which is one drawback of the proposed model.

Wang et al. [138] proposed a scheme to address the challenges of secure aggregation and identity privacy in fog computing. It involves four key entities: a system manager, a terminal device, a fog node, and a cloud server. The system manager provides help to other entities to generate public and private keys. The terminal device acts as the connection between users in the IoT. The fog node acts as a bridge between the terminal device and the cloud server and stores data for communication as well as controls and manages all terminal devices. However, the terminal devices depend on the fog node rather than the network gateway. The last entity, the cloud server, has large and strong computing power. Therefore, it can process all data coming from the fog nodes as well as the terminal devices. Furthermore, the authors did not consider the complete scenario of an adversary model, nor did they consider the issue of privacy of the location.

b: PRIVACY OF LOCATION

Huo et al. [140] proposed a location difference-based proximity detection model intended to achieve proximity detection while preserving the privacy of fog node locations. It utilizes the Paillier encryption algorithm [141], [142], [143], [144]. Additionally, it employs a decision tree approach for proximity detection, which proves to be highly effective and reliable in terms of communication and computation costs when compared to alternative proximity detection strategies [145]. However, it is worth noting that the authors did not consider the feature and impact of traceability in the proposed model.

Yang et al. [146] proposed a scheme to address the privacy concerns associated with the sensitive location information of prover systems, particularly in location-based applications. Furthermore, the scheme tackles this problem by utilizing the bounded retrieval model. Moreover, the proposed scheme is designed for both one-dimensional and three-dimensional scenario models. Experimental results indicate that the one-dimensional scenario model offers superior effectiveness and protection of location privacy against verifiers compared to the three-dimensional scenario model.

c: PRIVACY OF DATA

Wang et al. [147] proposed a fog server to store partial and incomplete information instead of a cloud server, which can be controlled by users. In addition, the authors designed a dummy rotation algorithm to hide the real trajectory information against the dummy trajectory information by incorporating the principles of similarity, intersection, practicability, and association. Dummy trajectory information provides a better way to mislead the behavior of a malicious attacker. The performance of the proposed privacy preservation scheme is measured by the following four metrics: trajectory disclosure property, average Euclidean distance, local data volume, and position disclosure probability. In addition, integrity is not considered among the performance evaluation metrics.

Koo and Hur [148] proposed a data privacy preservation protocol to delete duplicate data and manage the resources of the network effectively and efficiently in the fog computing communication paradigm. The protocol aims to achieve fine-grained access control by using a user-level key management mechanism that uses an update mechanism, pairing-based cryptography, and a Merkle (hash) tree [149]. It incorporates three entities: the end-user, the fog, and the cloud. Moreover, it also provides a capability for managing and controlling ownership. It is efficient concerning communication overhead, computation cost, and storage capabilities as compared to traditional data duplication protocols [150] and provides secure and reliable user-level key management. At the same time, it has some drawbacks that are viewed as limitations of the proposed protocol. Specifically, the authors used a limited adversary model and so the proposed protocol cannot resist differential attacks.

Mobile devices contain large amounts of private information related to the end-user, which cannot be sent directly to perform processing without being protected by any privacy preservation mechanism. Accordingly, the protection of private and important information of the user is very necessary before using any method of processing. To tackle this problem, some researchers have put their efforts into proposing promising optimal solutions [151], [152]. Du et al. [153], proposed a query model based on differential privacy for privacy protection. It sizes information regarding the structure along the edge weights of data centers supported by the fog computing communication paradigm. Furthermore, it uses a Laplace operator (differential operator) to achieve the best results of the privacy-preserving model [154]. The proposed model also can resist various malicious attacks in their early stages, such as a fog node recognition attack, and achieves high data reliability, efficiency, and low energy consumption. In addition, the experimental results show that the model is effective. On the other hand, the authors consider the limited adversary model.

Table 4 summarizes all the proposed existing and possible solutions for preserving the user's privacy and mitigating the user's private information regarding the identity, location, and data generated by applications from being learned by an attacker. It also gives all the techniques used to overcome the problem and presents the advantages and limitations of the proposed solutions.

D. INTRUSION DETECTION AND PREVENTION

In fog computing-based IoT applications, a malicious attacker can muddle the entities, including IoT devices and fog nodes. Therefore, the implementation of intrusion detection and prevention systems is necessary, aiming to detect malicious attackers as well as protect the architecture of fog-based IoT applications. Furthermore, it is not enough to implement this system in only one layer but must be implemented across the entire architecture. There are numerous systems proposed to detect and mitigate malicious attacks [155]. These proposed schemes are used in various applications to identify and mitigate the abnormal behavior exhibited by malicious attackers, including the smart grid application [156], [157], the cloud-based application [155], and the SCADA system [158]. However, to implement an intrusion detection and prevention system on each layer of fog-based IoT applications, several challenges arise as regards controlling and managing real-time notifications, false alarms, and response time [159].

1) EXISTING SOLUTIONS FOR INTRUSION DETECTION AND PREVENTION

Several solutions have been proposed to detect and protect the architecture of fog-based IoT applications against malicious activities by attackers. The following subsection details the current solutions based on host-based, network-based, and distributed intrusion detection and prevention mechanisms.

TABLE 4. The proposed solutions and their classification on real-time end-users privacy preservation in fog computing-based IoT applications.

Scheme	Contribution	Technique(s)	Advantages	Drawbacks
Zhitao Guan et al. (2019) [131]	Provides a secure data aggregation and privacy-preserving environment for fog-based-devices	- Device-oriented anonymous privacy-preserving scheme with authentication using multi-authority	It is a lightweight authentication protocol for resource-constrained devices, ensuring security and privacy within the IoT environment.	It is considered a complex environment for the fog-based-devices.
Jiale Zhang et al. (2020) [132]	Proposed a verifiable lightweight privacy-preserving data aggregation scheme for the edge computing environment	- Paillier Homomorphic Encryption - An online/offline signature technique	It is a lightweight and accurate solution that encounters minimal computational complexity and communication overhead.	It is evaluated using a few number of attacks.
Hayat Mohammad Khan et al. (2021) [133]	The system provides a robust, distributed, and privacy-preserving fog-based data aggregation technique with fault-tolerant various security properties	- Boneh-Goh-Nissam cryptosystem - Elliptic Curve Digital Signature Algorithm	It avoids false data injection attacks. Further, it is efficient in terms of encryption, aggregation decryption, and communication costs.	It did not consider severe attacks that may affect the performance of the fog-based device's communication environment.
Lu et al. (2017) [134]	Provides privacy to individual IoT device	- Homomorphic paillier encryption - Chinese remainder theory - One-way hash function	It is considered effective for fault tolerance, computation efficiency, and minimal communication overhead.	It does not consider the effect of traceability.
Wang et al. (2018) [138]	To tackle the problems of identity privacy and anonymity preserving	- Elliptic curve public key cryptography - Castagnos-Laguillaumie cryptosystem	It ensures the privacy of the identity of the devices. Along, it reduces communication overhead as well as computation costs.	It only focuses on identity privacy rather than location privacy. Further, the adversary model is considered limited.
Huo et al. (2017) [140]	Ensures location privacy along with proximity detection	- Paillier encryption - Decision tree	It achieves the updated form of location privacy-preserving. Along, it is considered effective and reliable for enhancing computation efficiency and reducing communication overhead. Along, it provides storage capabilities as well.	It does not consider the effect of traceability.
Yang et al. (2018) [146]	Provides privacy to the location information of the devices	- Position based cryptography - Position-based key agreement and distribution - Position based computation	It does not involve extra and unnecessary communication overhead and computation costs to achieve privacy.	Integrity measurements are not considered by authors. The model cannot deal with resist colliding and collision attacks.
Wang et al. (2017) [147]	Provide a privacy-preserving way for trajectory information	- Dummy rotation algorithm instead of real-trajectory information	It is considered a reliable scheme to provide privacy to trajectory information. Along, it is effective in terms of quality, energy consumption, and data utilization.	The integrity parameter is not considered for the performance evaluation metric.
Koo and Hur (2018) [148]	Provides privacy to data generated by devices	- User-level key management and update method - Pairing based cryptography - Merkle hash tree	It provides secure and reliable user-level key management. Further, it provides an effective strategy in terms of communication overhead, cost computation, and storage capabilities.	It cannot resist differential attacks. Further, the adversary model is considered limited.
Du et al. (2017) [153]	Optimal solution to provide data privacy and differential privacy	- Laplace operator (differential operator) - Query function	It resists various malicious attacks in the early stages, such as fog node recognition attacks. It achieves high data reliability, efficiency, and low energy consumption. It is considered suitable for large-scale data sets.	The adversary model is not considered as mature.

a: HOST-BASED INTRUSION DETECTION AND PREVENTION

Vieira et al. [160] indicate that grid and cloud computing communication environments have a distributed nature. This, unfortunately, in many cases makes finding the vulnerabilities to exploit easy for a malicious attacker. In addition, the behavior of an attacker is silent, because an attacker in the cloud and grid communication environment leaves no trace paths in a node operating system. Therefore, it becomes imperative to deploy an intrusion detection and prevention system to efficiently identify the malicious behaviors of attackers and proactively prevent their intrusion. The system monitors the behavior of each node and sends a notification as an alert to other nodes in the network whenever an attack occurs. To operate efficiently, the system requires compatibility among nodes, different protocols, and maintenance and update mechanisms. To fulfill these requirements, the authors proposed a middleware layer as cloud middleware, named the grid and cloud computing intrusion detection system. It consists of four components; node, service, audit system, and storage service. The node accesses the resources provided by the network through a middle layer, middleware. The second component facilitates communication between nodes. The audit system serves as a crucial component within the proposed architecture, acting as a supervisor. It functions to gather information from various sources, including the log system, trace files, services, system events, system calls, file systems, and messages transmitted between nodes. The storage service stores the captured data to perform the process of analysis. Based on the observation and results of the analysis, the proposed system calculates the probability of an attack. If the calculated probability is high, the occurrence of a malicious attack is indicated, and the proposed system sends a notification in the form of an alert message to all the other nodes in the network. However, the proposed scheme needs some further steps to ensure its actions are accurate and effective.

Arshad et al. [161] presented an abstract model aimed at reducing the time interval related to the integration of intrusion detection and prevention mechanisms. According to the authors, the process of intrusion detection requires a response on an immediate basis to prevent the behavior of an attacker. Therefore, the time interval between intrusion detection and prevention must be minimal. Furthermore, the model uses two types of techniques to detect the behavior of an attacker, namely, signature-based detection and anomaly-based detection. In signature-based detection, the model analyzes the behavior of each node against a pre-defined database and identifies the malicious node as an attacker. In anomaly-based detection, the model provides the profile and description for normal as well as an attacker's behavior. At present, the description of the proposed model has made petitions, but no experiments have been conducted to produce results that could be discussed and evaluated. In addition, achieving the delicate balance of minimizing intrusion response while maintaining the overall security and privacy of the cloud infrastructure presents a considerable challenge.

b: NETWORK-BASED INTRUSION DETECTION AND PREVENTION

Hamad and Al-Hoby [162] have addressed the problem of intrusion detection and prevention for communication between nodes as securely and reliably in the cloud computing communication environment. The researchers proposed a cloud intrusion detection service framework that can be implemented by cloud providers. This framework enables clients to subscribe to security-as-a-service, offering a range of capabilities. The proposed framework consists of three layers: the user layer, the system layer, and the database layer. The user layer provides an interface for cloud subscribers to define rules and requirements for protection. Moreover, it enables both client and administrator to access different services, that is configuration detail, subscription detail, and security monitoring services. The second layer, named the system layer, operates as a bridge between the user and the database, offering the necessary application programming interface (API) for accessing the database. The database layer provides a fast-tracking system tracing all settings of the subscription and updating the setting details accordingly. The service-based detection and prevention system within the proposed framework introduces extra computation and communication overhead compared to the traditional detection and prevention systems.

According to Houmansadr et al. [163], a smartphone is a fast type of communication and provides powerful and advanced computing and connectivity functionalities. Simultaneously, it uses a software architecture similar to personal computers. However, it is also vulnerable to security threats such as viruses, worms, and Trojan horse programs [164]. Hence, the researchers have proposed a system called the cloud-based intrusion detection and response time for smartphones. This proposed framework provides a user-friendly interface that is designed to be accessible and intuitive, catering to users with varying levels of technical expertise. The proposed solution provides light resource equipment and the capability for the detection and prevention of an attacker in real time. Furthermore, it analyzes the behavior of all the system calls of smartphones and detects any abnormal system calls. Then, it takes appropriate action to prevent the abnormal system call through scalability, low cost, and resistance, whenever an abnormal system call is detected. The authors deployed the proposed framework in an Android-based, HTC Droid Incredible smartphone. However, the generated attack graph of the proposed framework cannot automatically decide to take preventive response action in the smartphone environment.

c: DISTRIBUTED-BASED INTRUSION DETECTION AND PREVENTION

The traditional intrusion detection and prevention system uses two component-based architectures; collection and analysis. This architecture is considered to be effective only to make small collections of hosts to monitor them. However, Dastjerdi et al. [165] presented a scalable, flexible, and cost-effective system that is based on mobile agents, regardless of their geographical location, to address the limitations observed in traditional systems. This customized system is specifically designed to enhance the security of users in cloud computing environments. Its goals are to attain scalability, low latency, cost reduction, and decreased network load. The system design is derived from two models: a peer-to-peer intrusion detection system utilizing mobile agents [166] and a distributed intrusion detection system employing mobile agents [167]. The proposed system consists of four key components: a controller, an agent, an agency, and a mobile agent. The agent's primary part is to detect malicious activities and generate alert messages that are then forwarded to the controller. The controller collects all relevant information in a log file. Subsequently, a mobile agent is dispatched by the controller to collect evidence for further analysis and auditing. The proposed system represents an improvement over existing solutions in terms of trust management. However, it is important to consider that an increase in the number of devices connected to the mobile agent may also elevate network load.

In a different research study focusing on intrusion detection in IoT systems, the researchers [168] proposed a distributed ensemble design that integrates the utilization of fog computing. The architecture of the proposed system consists of three phases; preprocessing, anomaly detection, and traffic testing. In the first phase, data is processed, and optimized features are selected. In the second phase, a random forest-based ensemble method using XGBoost, Gaussian naïve Bayes, and K-NN algorithms are used for classification. This model is carried out on UNSW-NB15 and DS2OS datasets. Furthermore, the authors also highlight the shortcomings of the centralized computing-based IDS techniques that have been previously used for securing resource-constraint devices.

The authors [169] have proposed a hybrid binary classification method (DNN-kNN) for intrusion detection using the Deep Neural Networks (DNN) and k-Nearest Neighbor (kNN) algorithm that is capable to operate in the fog computing layer. In the detection process, the gain ratio attribute evaluation technique has been used for selecting the best attributes for detecting the attacks. Furthermore, the proposed DNN-kNN method is not capable of detecting routing attacks and has minimal processing and memory overhead at the fog node.

Ram [170] integrates trust computing into cloud computing to build a secure and reliable network for cloud-based applications. The proposed method deploys an individual sensor at each cloud-computing region, which is used to detect the malicious activity of an attacker. Furthermore, it drops all packets whenever the attacker is detected and generates an alert message to inform other sensors deployed at other cloud-computing regions regarding the attacker and its malicious behavior. The proposed method consists of four modules: a detection module, an alert-clustering module, threshold calculation, and a response and blocking system. Furthermore, the detection module has three components: a block, communications, and mutual modules. The block checks the integrity and correctness of the packets sent from the source node and drops all bad packets related to the attacker. The communication submodule is used to send an alert message to all other regions whenever the malicious activity of an attacker is detected. The third submodule, the mutual module, is used to collect the alert message. However, each region has an alert clustering module, with the ability to evaluate the accuracy by calculating its severity, as well as the capability to decide whether the received alert is true or false. Thus, the proposed method provides the capability to detect and prevent malicious security attacks such as DoS attacks and distributed denial of service (DDoS) attacks. Furthermore, this method sends an alert message to all other regions. Hence, if there are n number of sensors, then n (n − 1) alert messages will be exchanged between all regions. This results in the issue of scalability as well as communication overhead, with any increase in the number of sensors.

Liu et al. [171] reported the existence of various challenges in traditional traffic control systems, such as heavy roadside sensors and the attraction of malicious vehicles. Also, traditional traffic control systems face the problem of a single point of failure. Therefore, Liu et al. proposed two intelligent light control systems using the fog computing communication paradigm where traffic lights act as fog nodes. The first scheme is very simple and can be considered to be an extension of traditional work [172]. It is used to detect and mitigate a DoS attack. The hardness of the proposed scheme depends on the computation of the cryptographic puzzle, namely, the Diffie-Hellman puzzle. It is likely to be secure and reliable, but the fog nodes do not have storage and computation capabilities. However, if the number of nodes is large, storage and computation overhead occur. Considering this effect, the authors proposed an improved scheme to mitigate the above-stated issue. The improved scheme depends on the hash collision puzzle. According to the experimental results, the second proposed scheme reduces communication overhead, computation cost, and unnecessary storage utilization. Accordingly, it is considered to be a fog-friendly scheme.

Table 5 summarizes all the proposed existing and promising solutions for discovering the malicious activities of an attacker as well as protecting the services provided by the applications. It also provides the techniques used to overcome the problem as well as the advantages and limitations of the proposed solutions.

E. TRUST MANAGEMENT

In a fog computing-based IoT network, the fog node may have the ability to communicate and establish trusting relationships with other fog nodes. However, the fog node cannot know how the other nodes are going to behave in a real-time IoT environment. Thus, the authentication and authorization (access control) mechanisms play an important role to mitigate the presence of malicious IoT devices and fog

TABLE 5. The proposed solutions and their classification on real-time intrusion detection and prevention in fog computing-based IoT applications.

Scheme	Type	Technique(s)	Advantages	Drawbacks
Vieira et al. (2010) [160]	Host-based ID/PS	- Hybrid signature-based detection - Detection of the anomaly using an artificial neural network (ANN)	It does not provide a false rate to detect an unknown attack as it uses an artificial neural network. Along, it provides low computation cost.	The proposed strategy requires further investigation to make it accurate and effective.
Arshad et al. (2011) [161]	Host-based ID/PS	- Hybrid signature-based detection - Anomaly-based detection	The duration between detection and prevention is a minimum time.	There are no experimental results evaluated and discussed.
Hamad and Al-Hoby (2012) [162]	Network-based ID/PS	- Service based detection	It uses a security-as-a-service way to facilitate the users. Furthermore, it can detect known attacks in their early stages.	It increases communication overhead. Along, it cannot detect unknown attacks.
Houmansadr et al. (2011) [163]	Network-based ID/PS	- Anomaly-based detection	It enables smartphone devices to detect an attacker and his malicious behavior and activities.	The external attacks cannot be detected by it. Further, it cannot take an appropriate decision against malicious activity.
Dastjerdi et al. (2009) [165]	Distributed ID/PS	- Anomaly detection	It is considered scalable, effective, and robust to detect and prevent malicious attackers and their activities regardless of their locations.	As the number of devices associated with the Mobile Agent increases, it leads to a higher network load.
Kumar et al. (2021) [168]	Distributed ID/PS	- Distributed ensemble design-based IDS	The system can detect rare attacks and has attained a low false alarm rate.	It may face high computational costs due to the machine learning algorithms.
Souza et al. (2020) [169]	Distributed ID/PS	- Deep Neural Networks - k-Nearest Neighbor (kNN)	It provides high accuracy and recall rate. Further, it faces low overhead in terms of memory and processing costs.	It is not capable to detect routing attacks.
Sanjay Ram (2012) [170]	Distributed ID/PS	- Distributed	It can detect and prevent malicious security attacks, including DoS and DDoS.	It may face a scalability issue.
Liu et al. (2018) [171]	Distributed ID/PS	- Cryptographic puzzle (Diffie-Hellman) - Hash collision puzzle	It is considered a fog-friendly scheme. Along, it reduces communication, computation, and storage utilization to mitigate false data injection attacks.	An attacker may manipulate the power state valuation.

nodes. Furthermore, this mechanism also facilities the establishment of a secure relationship between the IoT devices and fog nodes in the network. However, it remains difficult to provide a guarantee that all the entities in the network are trusted as well as can resist attackers and their malicious behavior. Regardless, the end-users require reliable and secure services and a robust trust model from the IoT applications. Hence, establishing and maintaining a certain level of trust is essential to facilitate effective communication with each other. There are no unique words or definitions to explain trust. Generally, it is defined as a combination of attributes such as confidence, security, and reliability. An entity must have these attributes for other entities to communicate and transmit messages in the network [173], [174], [175], [176]. As a result, several researchers have dedicated their efforts to tackling the challenge of trust management within the communication environment of cloud computing [177], [178]. Nevertheless, in the fog computing communication environment, there is a need to consider the matter of trust management to guarantee the reliability and security of communication between IoT devices and enable seamless connectivity within the fog nodes network. Furthermore, the trust management protocol requires the following questions to be answered to make a trustworthy protocol in the network:

- What are the key attributes that define the trustworthiness of individual IoT devices and fog nodes within a fog-based IoT network?
- Which entity has the right or permission to validate as well as monitor the assigned attributes of the IoT device and fog node?

1) EXISTING SOLUTIONS FOR TRUST MANAGEMENT

The following sub-section presents the proposed robust trust model for evidence-based, monitor-based, and reputation-based trust management.

a: EVIDENCE-BASED TRUST MANAGEMENT

Li and Singhal [179] and Yu et al. [180] examine trust management using two models: an evidence-based model and a monitor-based model. The evidence-based model establishes the authenticity of relationships between entities by leveraging specific attributes, such as response-based evidence. These attributes may encompass elements like public keys, identity addresses, or other values that substantiate the trustworthiness of the entity. These attributes are produced by an entity itself or other entities. Furthermore, these attributes can be accessed either online or offline. Several mechanisms exist to evaluate trustworthiness through different types of attributes such as a trust chain [181], mutual friend [182], packet forwarding ratio [183], and recommended trust level [184], [185].

b: MONITOR-BASED TRUST MANAGEMENT

This model sustains the trust level of each entity through both direct and indirect observation. Direct observation specifically scrutinizes the malicious and self-centered conduct of neighboring nodes, encompassing activities like DoS attacks and packet-dropping attacks. The indirect observation, on the other hand, focuses on feedback and recommendations submitted and forwarded by other neighbors or adjacent nodes. Hence, Buchegger and Boudec [186] have proposed the CONFIDANT protocol in an ad hoc network, which effectively detects the behavior of individual nodes and protects the network against potential malicious activities from attacker nodes. It consists of four components, namely, the monitor system, the reputation system, the trust manager, and the path manager. The monitor system sends a notification to the reputation system whenever it detects the malicious behavior of an attacker node in the network. The reputation system maintains a table containing the name of a node among its ratings. If the rating of a node exceeds that of a pre-defined threshold, the rating of a node is updated to identify it as a malicious attacker node. Furthermore, the reputation system maintains a list, named the blacklist, which is intended to contain the name of all malicious attacker nodes, which it sends to the trust manager periodically. The trust manager generates an alert message and sends it to the whole network in its transmission range. The last component, path manage, is used to assign ratings to paths according to the rating of the nodes that exist on the path and to delete those paths that contain attacker nodes. The authors did not discuss the mechanism for computing the reputation and feedback values, nor does the proposed scheme provide any mechanism to prevent the malicious attacker node from broadcasting false information regarding the other neighbor nodes in the network.

Marti et al. [187] proposed two mechanisms, named the watchdog locator and path rater method. The watchdog location is deployed on each node to mitigate the malicious activities of an attacker node, while simultaneously maintaining the buffer of recently forwarded packets by each node. At the same time, it monitors the buffer and performs a comparison with the packets that exist in the buffer to identify any similarities. If a monitored packet bears similarity to a packet stored in the buffer, it is transmitted to neighboring nodes within the network's transmission range. Conversely, if a packet remains in the buffer for an extended period, the watchdog locator increments the failure count by one. If the failure count reaches a pre-defined threshold, however, the watchdog locator assumes the node to be an attacker node. The second proposed mechanism is the path rater. It is used to ensure a reliable route between nodes to ensure communication is secure. It accomplishes this by computing the path metrics and selecting the one with the highest path metric value. Subsequently, it removes the nodes that have low path metric ratings and identifies them as attacker nodes. In addition, the proposed mechanisms are likely to be unable to detect the malicious nodes in the case of packet collision as well as the collision of malicious nodes.

Wei et al. [188] proposed a scheme to enhance security in an ad hoc network. It uses uncertain reasoning to calculate the trust value. The concept of uncertain reasoning comes from the field of artificial intelligence, aiming to address problem-solving and offer flexibility across various fields, including expert systems, data fusion systems, and multi-agent systems [189], [190], [191], [192]. However, the proposed scheme provides the ability to detect malicious node behavior and mitigate issues like unreliable wireless connections and buffer overflow. These factors contribute to dropped and tampered transmitted packets within the system. However, it improves the performance concerning throughput and the packet forwarding ratio. In addition, it increases end-to-end delay along with communication overhead.

c: REPUTATION-BASED TRUST MANAGEMENT

In reputation-based trust management, the trust level is computed by reputation, which is a perception that an agent or peer makes about a node by using past actions [193]. It is an important metric for evaluating the trustworthiness of a node. In addition, reputation-based trust management does not require central coordination, a central database, and a global view of the network. Hence, some researchers put efforts into applying reputation-based trust management mechanisms in various applications, such as mobile ad hoc networks, mobile crowdsensing applications, vehicular ad hoc networks, and many other delay-tolerant kinds of networks [194], [195], [196], [197]. Furthermore, Adams et al. [198] proposed three types of reputation-based trust management schemes, namely, positive, negative, and hybrid reputation. Thus, positive reputation-based trust management focuses on the feedback and observation of the nodes, which exhibit positive behavior in the network. Negative reputation-based trust management focuses on the recorded complaint, feedback, and observation of the nodes that exhibit negative behavior in the network. In the hybrid reputation, nodes are considered to be trustworthy and

TABLE 6. The proposed solutions and their classification on real-time trust management in fog computing-based IoT applications.

Scheme	Type	Components	Description/Advantages	Drawbacks
Li and Singhal (2007) [179] Yu et al. (2013) [180]	Evidence-based Trust Management	- Public key - Identity address	It establishes a true relationship as response-based evidence. For this purpose, the public key and identity address are used.	The devices have limited specifications. However, the applicability of this strategy is considered limited.
Buchegger and Boudec (2002) [186]	Monitor-based Trust Management	- Monitor system - Reputation system - Trust manager - Path manager	It percepts the behavior of each node to detect and prevent the network from malicious behavior of an attacker.	It does not detect and prevent malicious attacks, such as false message flooding.
Marti et al. (2000) [187]	Monitor-based Trust Management	- Watchdog locator - Path rater	It ensures a reliable path between nodes for secure communication.	The proposed scheme is considered unable to detect the malicious activities of nodes in case of packet collision as well as node collision.
Wei et al. (2014) [188]	Monitor-based Trust Management	- Uncertain reasoning - Bayesian interface - Demester-Shafer theory	It uses certain reasoning to compute the trust value. To be specific, it uses the Bayesian interface and Demester-Shafer for direct and indirect observation respectively.	It leads to an increase in both end-to-end delay and communication overhead encountered during network communication.
Adams et al. (2005) [198]	Reputation-based Trust Management	- Positive reputation - Negative reputation - Combination of both, positive and negative	The trust values are computed by using reputation. It operates without the need for central coordination, or global network view.	It does not ensure security and reliability between entities during communication. However, [199], [200], and [201] indicate the security problems in it.

feedback is used to reflect the node's reputation negatively. In addition, Yunfang [199], Ruohomaa and Kutvonen [200], and Ruohomaa et al. [201] have identified the problem in the trust scheme of Adam et al., which proposes a hybrid solution as a robust trust model to ensure security and reliability in the network.

Table 6 summarizes a comprehensive overview of the current and promising solutions that goal to ensure the reliability and security of services offered by IoT applications to end-users. It outlines the techniques or components employed to address specific challenges and presents the advantages and disadvantages related to each proposed solution.

IV. RESEARCH CHALLENGES AND FUTURE RESEARCH DIRECTIONS

This section highlights the various research directions. Furthermore, this section aims to assist the academia and research community in further investigation of these issues.

A. IDENTIFICATION AND PROTECTION OF SENSITIVE DATA

In IoT applications, smart sensors and objects are used to collect data from the physical environment such as health status, traffic information, pollution levels, and information regarding personal activities. Thus, some data may be sensitive, for example, information regarding personal activities and health status. While some data may not be considered sensitive, for example, traffic information and pollution levels. Nonetheless, distinguishing sensitive data from a vast amount of data is considered a challenging task. Because it is determined by the end-users according to their priority and choice. In addition, several applications of IoT produce data that have different security levels for different users. Therefore, the identification of sensitive data is considered an initial step to protecting data in fog-based IoT networks. Although, there are several works proposed to encrypt the data [202], [203], [204]. Regrettably, these mechanisms cause unnecessary communication and computation overhead. Hence, the researcher must consider the identification process to identify the sensitive data before using the protection mechanism.

B. SECURE DATA SHARING

In fog based IoT network, IoT collects the data from the physical environment whereas the fog computing paradigm offers the capability of temporary storage for the collected data. However, data must be encrypted from being forwarded to fog nodes to prevent sensitive data leakage. There are several encryption mechanisms to attain fine-grained data sharing in the cloud computing paradigm [205], [206], [207], [208]. But efficiency is still considered a bottleneck to implementing these encryption mechanisms on fog-based IoT networks. Therefore, fog based IoT communication environment requires an efficient fine-grained data-sharing approach to manage decryption key distribution in a better way as well as minimize resource utilization.

C. BRING YOUR OWN DEVICE (BYOD) BASED AUTHORIZATION

Due to advancements in technology, each person has multiple devices to connect to the Internet such as a PC, laptop, smartphone, tablet, and wearable devices. However, it is considered a challenging task to manage and control the multiple Internet-connected devices owned by one user. In addition, the fog computing paradigm has the feature of decentralized communication. Therefore, it does not focus on the devices, it only focuses on the user who accesses them. Hence, it is considered necessary to propose a new mechanism to control and manage all devices owned by one user as well as a key management mechanism for fog nodes. There are some key management and device management mechanisms to provide authorization to multiple devices belonging to one owner. These mechanisms use identity or password-based authentication to verify the authenticity of the user. Along, provide session key by using bring-your-own-device management to reduce the overhead of mobile device management for secure and reliable communication to other devices [209], [210], [211]. But it does not focus on the mobility feature of devices. Hence, authorization mechanisms need further investigation where multiple devices should be able to access the real-time services along a union of old devices that should be consistent and compatible.

D. SYBIL ATTACK

It is a vague attack where an attacker node may act like it has multiple identities. Furthermore, it was familiarized by Douceur in 2002 [212]. However, the fog computing paradigm is considered susceptible to a Sybil attack which poses a significant security concern, where attackers can fabricate fake identities. In the presence of a Sybil attack in the fog-based IoT network, the intended user may receive false data from a fake node and the IoT application may generate false results. Furthermore, attackers behave similarly to the intended and legitimate users, therefore it is considered extremely difficult to detect the misbehavior of an attacker in the network. There are several works proposed to detect the Sybil attacker in the network, where the behavior of both, the intended user and attacker are compared such as social community, social graph, and friend relationship [213], [214], [215], [216]. Besides, the fog computing paradigm has decentralized nature. Therefore, these proposed schemes become unable to detect the behavior of a Sybil attack effectively and efficiently. However, the fog-based IoT network requires an effective and efficient based Sybil attacker defense scheme while preserving the privacy of real-time services provided by the IoT applications.

E. BIG DATA ANALYSIS

IoT applications generate data in a vast amount. However, the analysis of this data is performed by using different data mining and machine learning algorithms and these algorithms pose an individual's privacy challenge in the big data era. However, it is extraordinarily difficult to preserve the individual's privacy during big data analysis. There are several solutions proposed, based on homomorphic encryption [217], [218] and differential privacy [154], to preserve the user's privacy during big data analysis. In addition, the homomorphic encryption-based schemes [219], [220], [221] increase communication and computation overhead. In contrast, differential privacy-based schemes [222], [223], [224], [225], [226] are constructed on centralized data storage. Further, the fog computing paradigm is decentralized, therefore fog computing-based IoT network demands an approach to perform the analysis of big data while preserving the privacy of end-users.

V. CONCLUSION

In the last few decades, academia and the research community have put their attention on the emerging idea of IoT. It can connect various smart devices, technologies, and applications, enhancing the overall quality of life. However, it encounters several research challenges, including issues related to high latency, low storage, processing capabilities, and network failure. Thus, the paradigm of fog computing has emerged to bring resources nearer to IoT devices. However, the fog-based IoT network is confronted with traditional real-time security challenges for end-users. However, a comprehensive survey is presented in the paper, aiming to ensure secure and reliable services for IoT applications. Firstly, the layered architecture of the fog-based IoT network is presented along with an explanation of how IoT applications operate under the paradigm of fog computing. Then, we have demonstrated the literature on real-time security challenges, such as authentication, authorization, end-user privacy-preserving, instruction detection and prevention, and trust management. In addition, the existing possible solutions to these real-time security challenges are also discussed. Lastly, several research challenges and outlines of future directions are discussed concerning security and privacy issues within the communication environment of fog-based IoT.

ACKNOWLEDGMENT

The authors are highly grateful to their affiliated Universities and Institutes for providing research facilities.

REFERENCES

[1] N. K. Giang, S. Kim, D. Kim, M. Jung, and W. Kastner, "Extending the EPCIS with building automation systems: A new information system for the Internet of Things," in *Proc. 8th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.*, Jul. 2014, pp. 364–369.

[2] H. F. Atlam, A. Alenezi, R. K. Hussein, and G. B. Wills, "Validation of an adaptive risk-based access control model for the Internet of Things," *Int. J. Comput. Netw. Inf. Secur.*, vol. 10, no. 1, pp. 26–35, Jan. 2018.

[3] P. K. Malik, R. Sharma, R. Singh, A. Gehlot, S. C. Satapathy, W. S. Alnumay, D. Pelusi, U. Ghosh, and J. Nayak, "Industrial Internet of Things and its applications in industry 4.0: State of the art," *Comput. Commun.*, vol. 166, pp. 125–139, Jan. 2021.

[4] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha, "Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10474–10498, Jul. 2021.

[5] T. Anitha, S. Manimurugan, S. Sridhar, S. Mathupriya, and G. C. P. Latha, "A review on communication protocols of industrial Internet of Things," in *Proc. 2nd Int. Conf. Comput. Inf. Technol. (ICCIT)*, Jan. 2022, pp. 418–423.

[6] M. Burhan, R. Rehman, B. Khan, and B.-S. Kim, "IoT elements, layered architectures and security issues: A comprehensive survey," *Sensors*, vol. 18, no. 9, p. 2796, Aug. 2018.

[7] T. A. Ahanger, A. Aljumah, and M. Atiquzzaman, "State-of-the-art survey of artificial intelligent techniques for IoT security," *Comput. Netw.*, vol. 206, Apr. 2022, Art. no. 108771.

[8] M. S. Rajan, J. R. Arunkumar, A. Ramasamy, and B. Sisay, "A comprehensive study of the design and security of the IoT layer attacks," in *Proc. 6th Int. Conf. Commun. Electron. Syst. (ICCES)*, Jul. 2021, pp. 538–543.

[9] A. Whitmore, A. Agarwal, and L. D. Xu, "The Internet of Things—A survey of topics and trends," *Inf. Syst. Frontiers*, vol. 17, no. 2, pp. 261–274, Apr. 2015.

[10] N. Arunkumar, V. Pandimurugan, M. S. Hema, H. Azath, S. Hariharasitaraman, M. Thilagaraj, and P. Govindan, "A versatile and ubiquitous IoT-based smart metabolic and immune monitoring system," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–11, Mar. 2022.

[11] D. Zhang, L. T. Yang, M. Chen, S. Zhao, M. Guo, and Y. Zhang, "Real-time locating systems using active RFID for Internet of Things," *IEEE Syst. J.*, vol. 10, no. 3, pp. 1226–1235, Sep. 2016.

[12] G. Khadka, B. Ray, N. C. Karmakar, and J. Choi, "Physical-layer detection and security of printed chipless RFID tag for Internet of Things applications," *IEEE Internet Things J.*, vol. 9, no. 17, pp. 15714–15724, Sep. 2022.

[13] R. Want, "Near field communication," *IEEE Pervasive Comput.*, vol. 10, no. 3, pp. 4–7, Jul. 2011.

[14] S. A. Alshqaqi, A. A. Al-Khulaidi, A. Y. Al-Mutawkkil, and M. M. Zayed, "A survey in IoT for healthcare applications," in *Proc. 6th Int. Congr. Inf. Commun. Technol.* Singapore: Springer, 2022, pp. 229–241.

[15] P. McDermott-Wells, "What is Bluetooth?" *IEEE Potentials*, vol. 23, no. 5, pp. 33–35, Jan. 2005.

[16] A. Barua, M. A. Al Alamin, M. S. Hossain, and E. Hossain, "Security and privacy threats for Bluetooth low energy in IoT and wearable devices: A comprehensive survey," *IEEE Open J. Commun. Soc.*, vol. 3, pp. 251–281, 2022.

[17] M. Paulon J. V., B. J. O. de Souza, and M. Endler, "Exploring data collection on Bluetooth mesh networks," *Ad Hoc Netw.*, vol. 130, May 2022, Art. no. 102809.

[18] E. Ferro and F. Potorti, "Bluetooth and Wi-Fi wireless protocols: A survey and a comparison," *IEEE Wireless Commun.*, vol. 12, no. 1, pp. 12–26, Feb. 2005.

[19] M. Gupta and S. Singh, "A survey on the ZigBee protocol, It's security in Internet of Things (IoT) and comparison of ZigBee with Bluetooth and Wi-Fi," in *Applications of Artificial Intelligence in Engineering*. Singapore: Springer, 2021, pp. 473–482.

[20] G. V. Crosby and F. Vafa, "Wireless sensor networks and LTE–A network convergence," in *Proc. 38th Annu. IEEE Conf. Local Comput. Netw.*, Oct. 2013, pp. 731–734.

[21] S. Li, M. Iqbal, and N. Saxena, "Future industry Internet of Things with zero-trust security," *Inf. Syst. Frontiers*, vol. 8, pp. 1–14, Mar. 2022.

[22] I. U. Khan, M. U. Shahzad, and M. A. Hassan, "Internet of Things (IoTs): Applications in home automation," *IJSEAT*, vol. 5, pp. 79–84, Jan. 2017.

[23] R. Yadav, N. Yadav, K. Gupta, R. Priyadarshini, S. Chakraborty, and P. Kumar, "Home automation using Internet of Things: An extensive review," in *Proc. 1st Int. Conf. Comput. Electron. Wireless Commun.* Singapore: Springer, 2022, pp. 441–449.

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

[25] R. Huo, S. Zeng, Z. Wang, J. Shang, W. Chen, T. Huang, S. Wang, F. R. Yu, and Y. Liu, "A comprehensive survey on blockchain in industrial Internet of Things: Motivations, research progresses, and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 88–122, 1st Quart., 2022.

[26] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities: The Internet of Things is the backbone," *IEEE Consum. Electron. Mag.*, vol. 5, no. 3, pp. 60–70, Jul. 2016.

[27] A. R. Khan, M. F. Jamlos, N. Osman, M. I. Ishak, F. Dzaharudin, Y. K. Yeow, and K. A. Khairi, "DSRC technology in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) IoT system for intelligent transportation system (ITS): A review," in *Recent Trends in Mechatronics Towards Industry*. Germany: Springer, 2022, pp. 97–106.

[28] Z. Hu and H. Tang, "Design and implementation of intelligent vehicle control system based on Internet of Things and intelligent transportation," *Sci. Program.*, vol. 2022, pp. 1–11, Jan. 2022.

[29] M. H. Memon, W. Kumar, A. Memon, B. S. Chowdhry, M. Aamir, and P. Kumar, "Internet of Things (IoT) enabled smart animal farm," in *Proc. 3rd Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2016, pp. 2067–2072.

[30] M. Zorawski, T. Brito, J. Castro, J. P. Castro, M. Castro, and J. Lima, "An IoT approach for animals tracking," in *Proc. Int. Conf. Optim., Learn. Algorithms Appl.* Cham, Switzerland: Springer, Jul. 2021, pp. 269–280.

[31] Z. Bi, Y. Liu, J. Krider, J. Buckland, A. Whiteman, D. Beachy, and J. Smith, "Real-time force monitoring of smart grippers for Internet of Things (IoT) applications," *J. Ind. Inf. Integr.*, vol. 11, pp. 19–28, Sep. 2018.

[32] D. Evans. (2011) *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*. [Online]. Available: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[33] F. Köylü, A. O. Ali, M. M. Hassan, M. M. Sabriye, A. A. Osman, A. A. Hilal, and Q. Abdullah, "Review of Internet of Things of security threats and challenges," Jul. 2021, *arXiv:2107.10733*.

[34] J. Camhi, *Former Cisco CEO John Chambers Predicts 500 Billion Connected Devices by 2025*. New York, NY, USA: Business Insider, 2015.

[35] H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, "IoT-based big data storage systems in cloud computing: Perspectives and challenges," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 75–87, Feb. 2017.

[36] P. Shah, A. K. Jain, T. Mishra, and G. Mathur, "IoT-based big data storage systems in cloud computing," in *Proc. 2nd Int. Conf. Smart Energy Commun.* Singapore: Springer, 2021, pp. 323–333.

[37] H. F. Atlam, A. Alenezi, A. Alharthi, R. J. Walters, and G. B. Wills, "Integration of cloud computing with Internet of Things: Challenges and open issues," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jun. 2017, pp. 670–675.

[38] S. Mishra and A. K. Tyagi, "The role of machine learning techniques in Internet of Things-based cloud applications," In *Artificial Intelligence-based Internet of Things Systems* Cham, Switzerland: Springer, 2022, pp. 105–135.

[39] N. S. Baqer, H. A. Mohammed, A. S. Albahri, A. A. Zaidan, Z. T. Al-Qaysi, and O. S. Albahri, "Development of the Internet of Things sensory technology for ensuring proper indoor air quality in hospital facilities: Taxonomy analysis, challenges, motivations, open issues and recommended solution," *Measurement*, vol. 192, Mar. 2022, Art. no. 110920.

[40] Y. Ai, M. Peng, and K. Zhang, "Edge computing technologies for Internet of Things: A primer," *Digit. Commun. Netw.*, vol. 4, no. 2, pp. 77–86, Apr. 2018.

[41] L. Haghnegahdar, S. S. Joshi, and N. B. Dahotre, "From IoT-based cloud manufacturing approach to intelligent additive manufacturing: Industrial Internet of Things—An overview," *Int. J. Adv. Manuf. Technol.*, vol. 119, pp. 1461–,

[42] A. Botta, W. Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of Things: A survey," *Future Generat. Comput. Syst.*, vol. 56, pp. 684–700, Mar. 2016.

[43] H. Li, M. Dong, and K. Ota, "Radio access network virtualization for the social Internet of Things," *IEEE Cloud Comput.*, vol. 2, no. 6, pp. 42–50, Nov. 2015.

[44] SP Thought Leadership Team, "Cisco Global Cloud Index: Forecast and methodology, 2014–2019," Cisco, San Jose, CA, USA, White Paper 23, 2014, p. 46.

[45] C. Cisco, *Cisco Global Cloud Index: Forecast and Methodology, 2016–2021*. San Jose, CA, USA: Cisco, 2018.

[46] M. Satyanarayanan, "A brief history of cloud offload: A personal journey from Odyssey through cyber foraging to cloudlets," *GetMobile, Mobile Comput. Commun.*, vol. 18, no. 4, pp. 19–23, Jan. 2015.

[47] M. Babar, M. S. Khan, F. Ali, M. Imran, and M. Shoaib, "Cloudlet computing: Recent advances, taxonomy, and challenges," *IEEE Access*, vol. 9, pp. 29609–29622, 2021.

[48] S. S. Gill, "AI for next generation computing: Emerging trends and future directions," *Internet Things*, vol. 19, Aug. 2022, Art. no. 100514.

[49] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 964–975, Jan. 2018.

[50] M. M. Sadeeq, N. M. Abdulkareem, S. R. M. Zeebaree, D. M. Ahmed, A. S. Sami, and R. R. Zebari, "IoT and cloud computing issues, challenges and opportunities: A review," *Qubahan Academic J.*, vol. 1, no. 2, pp. 1–7, Mar. 2021.

[51] F. Computing, "The Internet of Things: Extend the cloud to where the things are," Cisco, San Jose, CA, USA, White Paper 13, 2015, p. 13.

[52] L. M. Vaquero and L. Rodero-Merino, ''Finding your way in the fog: Towards a comprehensive definition of fog computing,'' *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 5, pp. 27–32, Oct. 2014.

[53] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, ''Fog computing and its role in the Internet of Things,'' in *Proc. 1st, Ed., MCC Workshop Mobile Cloud Comput.*, Aug. 2012, pp. 13–16.

[54] C.-M. Chen, S. A. Chaudhry, K.-H. Yeh, and M. N. Aman, ''Security, trust and privacy for cloud, fog and Internet of Things,'' *Secur. Commun. Netw.*, vol. 2022, pp. 1–2, Jan. 2022.

[55] S. Yi, Z. Hao, Z. Qin, and Q. Li, ''Fog computing: Platform and applications,'' in *Proc. 3rd IEEE Workshop Hot Topics Web Syst. Technol. (HotWeb)*, Nov. 2015, pp. 73–78.

[56] A. A. A. Sen and M. Yamin, ''Advantages of using fog in IoT applications,'' *Int. J. Inf. Technol.*, vol. 13, no. 3, pp. 829–837, Jun. 2021.

[57] M. Saad, ''Fog computing and its role in the Internet of Things: Concept, security and privacy issues,'' *Int. J. Comput. Appl.*, vol. 180, no. 32, pp. 7–9, Apr. 2018.

[58] S. Rani, A. Kataria, and M. Chauhan, ''Fog computing in industry 4.0: Applications and challenges—A research roadmap,'' in *Energy Conservation Solutions for Fog-Edge Computing Paradigms*. Singapore: Springer, 2022, pp. 173–190.

[59] I. Stojmenovic, ''Fog computing: A cloud to the ground support for smart things and machine-to-machine networks,'' in *Proc. Australas. Telecommun. Netw. Appl. Conf. (ATNAC)*, Nov. 2014, pp. 117–122.

[60] S. J. Stolfo, M. B. Salem, and A. D. Keromytis, ''Fog computing: Mitigating insider data theft attacks in the cloud,'' in *Proc. IEEE Symp. Secur. Privacy Workshops*, May 2012, pp. 125–128.

[61] M. Iorga, L. Feldman, R. Barton, M. J. Martin, N. S. Goren, and C. Mahmoudi, *Fog Computing Conceptual Model*, document Special Publication (NIST SP)-500-325, 2018.

[62] R. Mahmud, R. Kotagiri, and R. Buyya, R., 2018, ''Fog computing: A taxonomy, survey and future directions,'' in *Internet Everything*. Singapore: Springer, 2018, pp. 103–130.

[63] R. Roman, J. Lopez, and M. Mambo, ''Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges,'' *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018.

[64] M. Y. Mehmood, A. Oad, M. Abrar, H. M. Munir, S. F. Hasan, H. Muqeet, and N. A. Golilarz, ''Edge computing for IoT-enabled smart grid,'' *Secur. Commun. Netw.*, vol. 2021, Jul. 2021, Art. no. 5524025.

[65] H. Atlam, R. Walters, and G. Wills, ''Fog computing and the Internet of Things: A review,'' *Big Data Cognit. Comput.*, vol. 2, no. 2, p. 10, Apr. 2018.

[66] P. Zhang, J. K. Liu, F. R. Yu, M. Sookhak, M. H. Au, and X. Luo, ''A survey on access control in fog computing,'' *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 144–149, Feb. 2018.

[67] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, ''Fog computing: A platform for Internet of Things and analytics,'' in *Big Data and Internet of Things: A Roadmap for Smart Environments*. Cham, Switzerland: Springer, 2014, pp. 169–186.

[68] A. V. Dastjerdi and R. Buyya, ''Fog computing: Helping the Internet of Things realize its potential,'' *Computer*, vol. 49, no. 8, pp. 112–116, Aug. 2016.

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

[70] K. Zhang, X. Liang, R. Lu, K. Yang, and X. S. Shen, ''Exploiting mobile social behaviors for Sybil detection,'' in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2015, pp. 271–279.

[71] Z. Zhang, M. C. Y. Cho, C. Wang, C. Hsu, C. Chen, and S. Shieh, ''IoT security: Ongoing challenges and research opportunities,'' in *Proc. IEEE 7th Int. Conf. Service-Oriented Comput. Appl.*, Nov. 2014, pp. 230–234.

[72] R. L. Kumar, F. Khan, S. Kadry, and S. Rho, ''A Survey on blockchain for industrial Internet of Things,'' *Alexandria Eng. J.*, vol. 61, no. 8, pp. 6001–6022, 2022.

[73] L. P. Rondon, L. Babun, A. Aris, K. Akkaya, and A. S. Uluagac, ''Survey on enterprise Internet-of-Things systems (E-IoT): A security perspective,'' *Ad Hoc Netw.*, vol. 125, Feb. 2022, Art. no. 102728.

[74] S. Bhatt and P. R. Ragiri, ''Security trends in Internet of Things: A survey,'' *Social Netw. Appl. Sci.*, vol. 3, no. 1, pp. 1–14, Jan. 2021.

[75] Y. Shi, G. Ding, H. Wang, H. E. Roman, and S. Lu, ''The fog computing service for healthcare,'' in *Proc. 2nd Int. Symp. Future Inf. Commun. Technol. Ubiquitous HealthCare (Ubi-HealthTech)*, May 2015, pp. 1–5.

[76] H. Sabireen and V. Neelanarayanan, ''A review on fog computing: Architecture, fog with IoT, algorithms and research challenges,'' *ICT Exp.*, vol. 7, no. 2, pp. 162–176, Jun. 2021.

[77] J. Ni, K. Zhang, X. Lin, and X. Shen, ''Securing fog computing for Internet of Things applications: Challenges and solutions,'' *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 601–628, 1st Quart., 2018.

[78] M. Mukherjee, L. Shu, and D. Wang, ''Survey of fog computing: Fundamental, network applications, and research challenges,'' *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1826–1857, 3rd Quart., 2018.

[79] M. Aazam and E. Huh, ''Fog computing micro datacenter based dynamic resource estimation and pricing model for IoT,'' in *Proc. IEEE 29th Int. Conf. Adv. Inf. Netw. Appl.*, Mar. 2015, pp. 687–694.

[80] M. Aazam and E. Huh, ''Fog computing and smart gateway based communication for cloud of things,'' in *Proc. Int. Conf. Future Internet Things Cloud*, Aug. 2014, pp. 464–470.

[81] M. Muntjir, M. Rahul, and H. A. Alhumyani, ''An analysis of Internet of Things (IoT): Novel architectures, modern applications, security aspects and future scope with latest case studies,'' *Int. J. Eng. Res. Technol*, vol. 6, pp. 422–447, Jun. 2017.

[82] V. K. Sehgal, A. Patrick, A. Soni, and L. Rajput, ''Smart human security framework using Internet of Things, cloud and fog computing,'' in *Intelligent Distributed Computing*. Cham, Switzerland: Springer, 2015, pp. 251–263.

[83] V. Gazis, ''A survey of standards for machine-to-machine and the Internet of Things,'' *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 482–511, 1st Quart., 2017.

[84] E. Ahmed and M. H. Rehmani, ''Mobile edge computing: Opportunities, solutions, and challenges,'' *Future Gener. Comput. Syst.*, vol. 70, pp. 59–63, May 2017.

[85] F. Jalali, K. Hinton, R. Ayre, T. Alpcan, and R. S. Tucker, ''Fog computing may help to save energy in cloud computing,'' *IEEE J. Sel. Areas Commun.*, vol. 34, no. 5, pp. 1728–1739, May 2016.

[86] A. V. Dastjerdi, H. Gupta, R. N. Calheiros, S. K. Ghosh, and R. Buyya, ''Fog computing: Principles, architectures, and applications,'' in *Internet Things*. San Mateo, CA, USA: Morgan Kaufmann, 2016, pp. 61–75.

[87] M. Taneja and A. Davy, ''Resource aware placement of IoT application modules in fog-cloud computing paradigm,'' in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, May 2017, pp. 1222–1228.

[88] G. Peralta, M. Iglesias-Urkia, M. Barcelo, R. Gomez, A. Moran, and J. Bilbao, ''Fog computing based efficient IoT scheme for the industry 4.0,'' in *Proc. IEEE Int. Workshop Electron., Control, Meas., Signals Their Appl. Mechatronics (ECMSM)*, May 2017, pp. 1–6.

[89] S. Chen, T. Zhang, and W. Shi, ''Fog computing,'' *IEEE Internet Comput.*, vol. 21, no. 2, pp. 4–6, Mar. 2017.

[90] L. Loffi, C. M. Westphall, L. D. Grüdtner, and C. B. Westphall, ''Mutual authentication with multi-factor in IoT-fog-cloud environment,'' *J. Netw. Comput. Appl.*, vol. 176, Feb. 2021, Art. no. 102932.

[91] S. Chandrasekhar and M. Singhal, ''Efficient and scalable query authentication for cloud-based storage systems with multiple data sources,'' *IEEE Trans. Services Comput.*, vol. 10, no. 4, pp. 520–533, Jul. 2017.

[92] S. C. Seo and T. Y. Youn, ''TIM: A trapdoor hash function-based authentication mechanism for streaming applications,'' *KSII Trans. Internet Inf. Syst.*, vol. 12, no. 6, pp. 1–24, 2018.

[93] S. Chandrasekhar and M. Singhal, ''Multi-trapdoor hash functions and their applications in network security,'' in *Proc. IEEE Conf. Commun. Netw. Secur.*, Oct. 2014, pp. 463–471.

[94] V. Odelu, A. K. Das, M. Wazid, and M. Conti, ''Provably secure authenticated key agreement scheme for smart grid,'' *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1900–1910, May 2018.

[95] R. Canetti and H. Krawczyk, ''Analysis of key-exchange protocols and their use for building secure channels,'' in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2001, pp. 453–474.

[96] S. Sourav, V. Odelu, and R. Prasath, and S. eptember. 2., ''Enhanced session initiation protocols for emergency healthcare applications,'' in *Proc. Int. Symp. Secur. Comput. Commun.* Singapore: Springer, Sep. 2019, pp. 278–289.

[97] J. Tsai and N. Lo, ''Secure anonymous key distribution scheme for smart grid,'' *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 906–914, Mar. 2016.

[98] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, ''An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks,'' *J. Netw. Comput. Appl.*, vol. 76, pp. 37–48, Dec. 2016.

[99] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Inf. Sci.*, vol. 321, pp. 263–277, Nov. 2015.

[100] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Royal Soc. London A, Math. Phys. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.

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

[102] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[103] W. Zhang, K. M. Hansen, and T. Kunz, "Enhancing intelligence and dependability of a product line enabled pervasive middleware," *Pervas. Mobile Comput.*, vol. 6, no. 2, pp. 198–217, Apr. 2010.

[104] Y. Bi, G. Han, C. Lin, Q. Deng, L. Guo, and F. Li, "Mobility support for fog computing: An SDN approach," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 53–59, May 2018.

[105] A. Muthanna, A. A. Ateya, A. Khakimov, I. Gudkova, A. Abuarqoub, K. Samouylov, and A. Koucheryavy, "Secure IoT network structure based on distributed Fog computing, with SDN/blockchain," TENCON, Malta, U.K., Tech. Rep. 216, 2019.

[106] C. Li, Z. Qin, E. Novak, and Q. Li, "Securing SDN infrastructure of IoT–fog networks from MitM attacks," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1156–1164, Oct. 2017.

[107] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 7, pp. 3339–3348, Sep. 2013.

[108] J. Zhou, X. Lin, X. Dong, and Z. Cao, "PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributedm-healthcare cloud computing system," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 6, pp. 1693–1703, Jun. 2015.

[109] D. Pointcheval and O. Sanders, "Short randomizable signatures," in *Proc. Cryptographers' Track RSA Conf.* Cham, Switzerland: Springer, Feb. 2016, pp. 111–126.

[110] K. LeFevre, D. J. DeWitt, and R. Ramakrishnan, "Incognito: Efficient full-domain K-anonymity," in *Proc. ACM SIGMOD Int. Conf. Manage. Data*, Jun. 2005, pp. 49–60.

[111] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, Jan. 2012.

[112] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks," *Comput. Commun.*, vol. 166, pp. 110–124, Jan. 2021.

[113] S. Manimurugan, "IoT-fog-cloud model for anomaly detection using improved Naïve Bayes and principal component analysis," *J. Ambient Intell. Humanized Comput.*, pp. 1–10, Jan. 2021.

[114] K. Gupta and S. Shukla, "Internet of Things: Security challenges for next generation networks," in *Proc. Int. Conf. Innov. Challenges Cyber Secur. (ICICCS-INBUSH)*, Feb. 2016, pp. 315–318.

[115] S. Salonikias, I. Mavridis, and D. Gritzalis, "Access control issues in utilizing fog computing for transport infrastructure," in *Proc. Int. Conf. Crit. Inf. Infrastructures Secur.* Cham, Switzerland: Springer, Oct. 2016, pp. 15–26.

[116] C. Hu, J. Zhang, and Q. Wen, "An identity-based personal location system with protected privacy in IoT," in *Proc. 4th IEEE Int. Conf. Broadband Netw. Multimedia Technol.*, Oct. 2011, pp. 192–195.

[117] T. D. Dang and D. Hoang, "A data protection model for fog computing," in *Proc. 2nd Int. Conf. Fog Mobile Edge Comput. (FMEC)*, May 2017, pp. 32–38.

[118] Y. Zhang and X. Wu, "Access control in Internet of Things: A survey," 2016, *arXiv:1610.01065*.

[119] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2011, pp. 568–588.

[120] J. B. Dennis and E. C. Van Horn, "Programming semantics for multiprogrammed computations," *Commun. ACM*, vol. 9, no. 3, pp. 143–155, Mar. 1966.

[121] J. L. Hernández-Ramos, A. J. Jara, L. Marin, and A. E. Skarmeta, "Distributed capability-based access control for the Internet of Things," *J. Internet Services Inf. Secur. (JISIS)*, vol. 3, pp. 1–16, Nov. 2013.

[122] X. Yao, H. Kong, H. Liu, T. Qiu, and H. Ning, "An attribute credential based public key scheme for fog computing in digital manufacturing," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2297–2307, Apr. 2019.

[123] J. Bernal Bernabe, J. L. Hernandez Ramos, and A. F. S. Gomez, "TACIoT: Multidimensional trust-aware access control system for the Internet of Things," *Soft Comput.*, vol. 20, no. 5, pp. 1763–1779, May 2016.

[124] P. N. Mahalle, P. A. Thakre, N. R. Prasad, and R. Prasad, "A fuzzy approach to trust based access control in Internet of Things," in *Proc. Wireless VITAE*, Jun. 2013, pp. 1–5.

[125] W. B. Daoud, M. S. Obaidat, A. Meddeb-Makhlouf, F. Zarai, and K.-F. Hsiao, "TACRM: Trust access control and resource management mechanism in fog computing," *Hum.-Centric Comput. Inf. Sci.*, vol. 9, no. 1, pp. 1–18, Dec. 2019.

[126] A. K. Junejo, N. Komninos, and J. A. McCann, "A secure integrated framework for fog-assisted Internet-of-Things systems," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6840–6852, Apr. 2021.

[127] J. Zhang, T. Li, Z. Ying, and J. Ma, "Trust-based secure multi-cloud collaboration framework in cloud-fog-assisted IoT," *IEEE Trans. Cloud Comput.*, vol. 11, no. 2, pp. 1546–1561, Apr./Jun. 2023.

[128] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the Internet of Things: Security and privacy issues," *IEEE Internet Comput.*, vol. 21, no. 2, pp. 34–42, Mar. 2017.

[129] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-preserving schemes for ad hoc social networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 3015–3045, 4th Quart., 2017.

[130] 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.

[131] Z. Guan, Y. Zhang, L. Wu, J. Wu, J. Li, Y. Ma, and J. Hu, "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT," *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, Jan. 2019.

[132] J. Zhang, Y. Zhao, J. Wu, and B. Chen, "LVPDA: A lightweight and verifiable privacy-preserving data aggregation scheme for edge-enabled IoT," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4016–4027, May 2020.

[133] H. M. Khan, A. Khan, F. Jabeen, and A. U. Rahman, "Privacy preserving data aggregation with fault tolerance in fog-enabled smart grids," *Sustain. Cities Soc.*, vol. 64, Jan. 2021, Art. no. 102522.

[134] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[135] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1999, pp. 223–238.

[136] P. Dingyi, S. Arto, and D. Cunsheng, "*Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*. Singapore: World Scientific, 1996.

[137] S. Ruj, A. Nayak, and I. Stojmenovic, "A security architecture for data aggregation and access control in smart grids," 2011, *arXiv:1111.2619*.

[138] H. Wang, Z. Wang, and J. Domingo-Ferrer, "Anonymous and secure aggregation scheme in fog-based public cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 712–719, Jan. 2018.

[139] G. Castagnos and F. Laguillaumie, "Linearly homomorphic encryption from DDH," in *Proc. Cryptographers' Track RSA Conf.* Cham, Switzerland: Springer, 2015, pp. 487–505.

[140] Y. Huo, C. Hu, X. Qi, and T. Jing, "LoDPD: A location difference-based proximity detection protocol for fog computing," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1117–1124, Oct. 2017.

[141] C. Fontaine and F. Galand, "A survey of homomorphic encryption for nonspecialists," *EURASIP J. Inf. Secur.*, vol. 1, pp. 41–50, Jan. 2009.

[142] V. Nikolaenko, U. Weinsberg, S. Ioannidis, M. Joye, D. Boneh, and N. Taft, "Privacy-preserving ridge regression on hundreds of millions of records," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 334–348.

[143] J. Sen, "Homomorphic encryption: Theory & applications," 2013, *arXiv:1305.5886*.

[144] M. Alkharji, H. Liu, and W. Cua, "Homomorphic encryption algorithms and schemes for secure computations in the cloud," in *Proc. Int. Conf. Secure Comput. Technol.*, 2016, pp. 1–19.

[145] B. Mu and S. Bakiras, "Private proximity detection for convex polygons," *Tsinghua Sci. Technol.*, vol. 21, no. 3, pp. 270–280, Jun. 2016.

[146] R. Yang, Q. Xu, M. H. Au, Z. Yu, H. Wang, and L. Zhou, "Position based cryptography with location privacy: A step for fog computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 799–806, Jan. 2018.

[147] T. Wang, J. Zeng, M. Z. A. Bhuiyan, H. Tian, Y. Cai, Y. Chen, and B. Zhong, "Trajectory privacy preservation based on a fog structure for cloud location services," *IEEE Access*, vol. 5, pp. 7692–7701, 2017.

[148] D. Koo and J. Hur, "Privacy-preserving deduplication of encrypted data with dynamic ownership management in fog computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 739–752, Jan. 2018.

[149] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Proofs of ownership in remote storage systems," in *Proc. 18th ACM Conf. Comput. Commun. Secur.*, Oct. 2011, pp. 491–500.

[150] J. Barreto, L. Veiga, and P. Ferreira, "Hash challenges: Stretching the limits of compare-by-hash in distributed data deduplication," *Inf. Process. Lett.*, vol. 112, no. 10, pp. 380–385, May 2012.

[151] K. Wang, J. Yu, X. Liu, and S. Guo, "A pre-authentication approach to proxy re-encryption in big data context," *IEEE Trans. Big Data*, vol. 7, no. 4, pp. 657–667, Oct. 2021.

[152] M. Du, K. Wang, Z. Xia, and Y. Zhang, "Differential privacy preserving of training model in wireless big data with edge computing," *IEEE Trans. Big Data*, vol. 6, no. 2, pp. 283–295, Jun. 2020.

[153] M. Du, K. Wang, X. Liu, S. Guo, and Y. Zhang, "A differential privacy-based query model for sustainable fog data centers," *IEEE Trans. Sustain. Comput.*, vol. 4, no. 2, pp. 145–155, Apr. 2019.

[154] C. Dwork, "Differential privacy," in *Encyclopedia Cryptography Security*, 2011, pp. 338–340.

[155] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 42–57, Jan. 2013.

[156] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusion detection in power system operations," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1052–1062, May 2013.

[157] Z. Qin, Q. Li, and M. Chuah, "Defending against unidentifiable attacks in electric power grids," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 10, pp. 1961–1971, Oct. 2013.

[158] L. A. Maglaras, J. Jiang, and T. J. Cruz, "Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems," *J. Inf. Secur. Appl.*, vol. 30, pp. 15–26, Oct. 2016.

[159] S. Anwar, J. M. Zain, M. F. Zolkipli, Z. Inayat, S. Khan, B. Anthony, and V. Chang, "From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions," *Algorithms*, vol. 10, no. 2, p. 39, Mar. 2017.

[160] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, "Intrusion detection for grid and cloud computing," *IT Prof.*, vol. 12, no. 4, pp. 38–43, Jul. 2010.

[161] J. Arshad, P. Townend, and J. Xu, "An abstract model for integrated intrusion detection and severity analysis for clouds," *Int. J. Cloud Appl. Comput.*, vol. 1, no. 1, pp. 1–16, Jan. 2011.

[162] H. Hamad and M. Al-Hoby, "Managing intrusion detection as a service in cloud networks," *Int. J. Comput. Appl.*, vol. 41, no. 1, pp. 35–40, Mar. 2012.

[163] A. Houmansadr, S. A. Zonouz, and R. Berthier, "A cloud-based intrusion detection and response system for mobile phones," in *Proc. IEEE/IFIP 41st Int. Conf. Dependable Syst. Netw. Workshops (DSN-W)*, Jun. 2011, pp. 31–32.

[164] J. Jamaluddin, N. Zotou, R. Edwards, and P. Coulton, "Mobile phone vulnerabilities: A new generation of malware," in *Proc. IEEE Int. Symp. Consum. Electron.*, Sep. 2004, pp. 199–202.

[165] A. V. Dastjerdi, K. A. Bakar, and S. G. H. Tabatabaei, "Distributed intrusion detection in clouds using mobile agents," in *Proc. 3rd Int. Conf. Adv. Eng. Comput. Appl. Sci.*, Oct. 2009, pp. 175–180.

[166] G. Ramachandran and D. Hart, "A P2P intrusion detection system based on mobile agents," in *Proc. 42nd Annu. Southeast Regional Conf.*, Apr. 2004, pp. 185–190.

[167] P. Kannadiga, M. Zulkernine, and S. I. Ahamed, "Towards an intrusion detection system for pervasive computing environments," in *Proc. Int. Conf. Inf. Technol., Coding Comput. (ITCC)*, vol. 2, Apr. 2005, pp. 277–282.

[168] P. Kumar, G. P. Gupta, and R. Tripathi, "A distributed ensemble design based intrusion detection system using fog computing to protect the Internet of Things networks," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 10, pp. 9555–9572, Oct. 2021.

[169] C. A. de Souza, C. B. Westphall, R. B. Machado, J. B. M. Sobral, and G. D. S. Vieira, "Hybrid approach to intrusion detection in fog-based IoT environments," *Comput. Netw.*, vol. 180, Oct. 2020, Art. no. 107417.

[170] R. M. Sanjay, "Secure cloud computing based on mutual intrusion detection system," *Int. J. Comput. Appl.*, vol. 1, no. 2, pp. 57–67, 2012.

[171] J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng, and J. Shen, "Secure intelligent traffic light control using fog computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 817–824, Jan. 2018.

[172] B. Waters, A. Juels, J. A. Halderman, and E. W. Felten, "New client puzzle outsourcing techniques for DoS resistance," in *Proc. 11th ACM Conf. Comput. Commun. Secur.*, Oct. 2004, pp. 246–256.

[173] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in *Proc. IEEE INFOCOM 25th IEEE Int. Conf. Comput. Commun.*, Apr. 2006, pp. 1–13.

[174] Z. Yan and S. Holtmanns, "Trust modeling and management: From social trust to digital trust," in *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions* Hershey, PA, USA: IGI Global, 2008, pp. 290–323.

[175] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Comput. Surv.*, vol. 45, no. 4, pp. 47:1–47:33, Aug. 2013.

[176] W. K. Wong, S. O. Cheung, T. W. Yiu, and H. Y. Pang, "A framework for trust in construction contracting," *Int. J. Project Manage.*, vol. 26, no. 8, pp. 821–829, Nov. 2008.

[177] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "TrustCloud: A framework for accountability and trust in cloud computing," in *Proc. IEEE World Congr. Services*, Jul. 2011, pp. 584–588.

[178] K. M. Khan and Q. Malluhi, "Establishing trust in cloud computing," *IT Prof.*, vol. 12, no. 5, pp. 20–27, Sep. 2010.

[179] H. Li and M. Singhal, "Trust management in distributed systems," *Computer*, vol. 40, no. 2, pp. 45–53, Feb. 2007.

[180] H. Yu, Z. Shen, C. Leung, C. Miao, and V. R. Lesser, "A survey of multi-agent trust management systems," *IEEE Access*, vol. 1, pp. 35–50, 2013.

[181] J.-H. Cho, A. Swami, and I.-R. Chen, "Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 1001–1012, May 2012.

[182] T. Eissa, S. A. Razak, R. H. Khokhar, and N. Samian, "Trust-based routing mechanism in MANET: Design and implementation," *Mobile Netw. Appl.*, vol. 18, no. 5, pp. 666–677, Oct. 2013.

[183] Z. Liu, A. W. Joy, and R. A. Thompson, "A dynamic trust model for mobile ad hoc networks," in *Proc. 10th IEEE Int. Workshop Future Trends Distrib. Comput. Syst. (FTDCS)*, May 2004, pp. 80–85.

[184] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 279–298, 2nd Quart., 2012.

[185] A. M. Shabut, K. P. Dahal, S. K. Bista, and I. U. Awan, "Recommendation based trust model with an effective defence scheme for MANETs," *IEEE Trans. Mobile Comput.*, vol. 14, no. 10, pp. 2101–2115, Oct. 2015.

[186] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol," in *Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Jun. 2002, pp. 226–236.

[187] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Aug. 2000, pp. 255–265.

[188] Z. Wei, H. Tang, F. R. Yu, M. Wang, and P. Mason, "Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning," *IEEE Trans. Veh. Technol.*, vol. 63, no. 9, pp. 4647–4658, Nov. 2014.

[189] J. Pearl, "*Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Amsterdam, The Netherlands: Elsevier, 2014.

[190] G. Shafer and J. Pearl, *Readings Uncertain Reasoning*. San Mateo, CA, USA: Morgan Kaufmann, 1990.

[191] B. Yu and M. P. Singh, "An evidential model of distributed reputation management," in *Proc. 1st Int. Joint Conf. Auto. Agents Multiagent Syst. (AAMAS)*, 2002, pp. 294–301.

[192] H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, "Sensor fusion using Dempster–Shafer theory [for context-aware HCI]," in *Proc. IMTC 19th IEEE Instrum. Meas. Technol. Conf.*, May 2002, pp. 7–12.

[193] J. Cho, A. Swami, and I. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 562–583, 4th Quart., 2011.

[194] Q. Li, A. Malip, K. M. Martin, S. Ng, and J. Zhang, "A reputation-based announcement scheme for VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 9, pp. 4095–4108, Nov. 2012.

[195] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "SACRM: Social aware crowdsourcing with reputation management in mobile sensing," *Comput. Commun.*, vol. 65, pp. 55–65, Jul. 2015.

[196] E. Ayday and F. Fekri, "An iterative algorithm for trust management and adversary detection for delay-tolerant networks," *IEEE Trans. Mobile Comput.*, vol. 11, no. 9, pp. 1514–1531, Sep. 2012.

[197] I. Chen, F. Bao, M. Chang, and J. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 5, pp. 1200–1210, May 2014.

[198] W. J. Adams, G. C. Hadjichristofi, and N. J. Davis, "Calculating a node's reputation in a mobile ad hoc network," in *Proc. 24th IEEE Int. Perform., Comput., Commun. Conf.*, Apr. 2005, pp. 303–307.

[199] F. Yunfang, "Adaptive trust management in MANET," in *Proc. Int. Conf. Comput. Intell. Secur. (CIS)*, Dec. 2007, pp. 804–808.

[200] S. Ruohomaa and L. Kutvonen, "Trust management survey," in *Proc. Int. Conf. Trust Manag.* Berlin, Germany: Springer, 2005, pp. 77–92.

[201] S. Ruohomaa, L. Kutvonen, and E. Koutrouli, "Reputation management survey," in *Proc. 2nd Int. Conf. Availability, Rel. Secur. (ARES)*, Apr. 2007, pp. 103–111.

[202] M. Agrawal and P. Mishra, "A comparative survey on symmetric key encryption techniques," *Int. J. Comput. Sci. Eng.*, vol. 4, no. 5, p. 877, 2012.

[203] C. Bösch, P. Hartel, W. Jonker, and A. Peter, "A survey of provably secure searchable encryption," *ACM Comput. Surv.*, vol. 47, no. 2, pp. 18:1–18:51, Aug. 2014.

[204] O. G. Abood and S. K. Guirguis, "A survey on cryptography algorithms," *Int. J. Sci. Res. Publications (IJSRP)*, vol. 8, no. 7, pp. 495–516, Jul. 2018.

[205] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2005, pp. 457–473

[206] C. Chu, S. S. M. Chow, W. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 468–477, Feb. 2014.

[207] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Proc. Int. Workshop Public Key Cryptogr.* Berlin, Germany: Springer, Feb. 2013, pp. 162–179.

[208] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Inf. Syst.*, vol. 48, pp. 132–150, Mar. 2015.

[209] M. A. Muhammad, "A behaviour profiling based technique for network access control systems," *Int. J. Cyber-Security Digit. Forensics*, vol. 8, no. 1, pp. 23–30, 2019.

[210] H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills, and J. Daniel, "Developing an adaptive risk-based access control model for the Internet of Things," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jun. 2017, pp. 655–661.

[211] M. Muhammad, A. U. Daniel, A. A. Abdullahi, and P. Radanliev, "Device-type profiling for network access control systems using clustering-based multivariate Gaussian outlier score," in *Proc. Int. Conf. Future Netw. Distrib. Syst.* 2021, pp. 270–279.

[212] J. R. Douceur, "The Sybil attack," in *Proc. Int. Workshop Peer Peer Syst.* Berlin, Germany: Springer, 2002, pp. 251–260.

[213] A. Arshad, Z. M. Hanapi, S. Subramaniam, and R. Latip, "A survey of Sybil attack countermeasures in IoT-based wireless sensor networks," *PeerJ Comput. Sci.*, vol. 7, p. e673, Sep. 2021.

[214] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support," *Secur. Commun. Netw.*, vol. 6, no. 4, pp. 523–538, Apr. 2013.

[215] X. Lin, "LSR: Mitigating zero-day Sybil vulnerability in privacy-preserving vehicular peer-to-peer networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 237–246, Sep. 2013.

[216] X. Liang, X. Lin, and X. S. Shen, "Enabling trustworthy service evaluation in service-oriented mobile social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 310–320, Feb. 2014.

[217] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. 41st Annu. ACM Symp. Theory Comput.*, May 2009, pp. 169–178.

[218] D. M. Van, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2010, pp. 24–43.

[219] L. Li, R. Lu, K. R. Choo, A. Datta, and J. Shao, "Privacy-preserving-outsourced association rule mining on vertically partitioned databases," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1847–1861, Aug. 2016.

[220] L. Zhang, W. Wang, and Y. Zhang, "Privacy preserving association rule mining: Taxonomy, techniques, and metrics," *IEEE Access*, vol. 7, pp. 45032–45047, 2019.

[221] K. Zhang, X. Liang, J. Ni, K. Yang, and X. Shen, "Exploiting social network to enhance human-to-human infection analysis without privacy leakage," *IEEE Trans. Depend. Secure Comput.*, vol. 15, no. 4, pp. 607–620, Jul. 2018.

[222] X. Liu, R. H. Deng, Y. Yang, H. N. Tran, and S. Zhong, "Hybrid privacy-preserving clinical decision support system in fog–cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 825–837, Jan. 2018.

[223] M. Abadi, A. Chu, I. H. B. G. McMahan, I. T. K. Mironov, and L. Zhang, "Deep learning with differential privacy," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.* 2016, pp. 308–318.

[224] T. Zhang and Q. Zhu, "Dynamic differential privacy for ADMM-based distributed classification learning," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 172–187, Jan. 2017.

[225] Ú. Erlingsson, V. Pihur, and A. Korolova, "RAPPOR: Randomized aggregatable privacy-preserving ordinal response," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2014, pp. 1054–1067.

[226] Z. Qin, Y. Yang, T. Yu, I. Khalil, X. Xiao, and K. Ren, "Heavy hitter estimation over set-valued data with local differential privacy," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 192–203.

MUHAMMAD BURHAN received the B.S. degree in information technology from the University of the Punjab, Pakistan, in 2016, and the M.S. degree in computer science from the National University of Computer and Emerging Sciences, Pakistan, in 2019, under the supervision of Dr. Rana Asif Rehman. He is currently a Lecturer with the Department of Information Technology, University of the Punjab. His research interests include the design and development of efficient routing and forwarding protocols, wireless networks, named-data networks-based vehicular ad hoc networks, and software-defined networks.

HINA ALAM received the master's degree in computer science from the National University of Computer and Emerging Sciences (FAST-NUCES), Lahore, Pakistan, in 2019. She is currently a Lecturer with the Informatics and Systems Department, University of Management and Science, Lahore. Her research interests include edge computing, the Internet of Things, cloud computing, and machine learning.

AHMAD ARSALAN received the M.S. degree in computer science from the National University of Computer and Emerging Sciences, Islamabad, Pakistan, in 2018. He is currently pursuing the Ph.D. degree in computer science with COMSATS University, Lahore Campus, Pakistan. He is a full-time Senior Lecturer with the University of Central Punjab, Lahore Campus, Pakistan. His research interests include the design and development of future internet architectures, cross-layer design for wireless networks, and efficient forwarding and routing protocols for named data networking-based software-defined networks. He is also serving as a reviewer for IEEE Access, the *Journal of Future Generation Computer Systems* (Elsevier), and the *International Journal of Communication Systems* (Wiley).

RANA ASIF REHMAN (Senior Member, IEEE) received the M.Sc. degree in computer science from Bahauddin Zakariya University, Multan, Pakistan, in 2010, the M.S. degree in computer science from International Islamic University, Islamabad, Pakistan, in 2012, and the Ph.D. degree in electronics and computer engineering from Hongik University, South Korea, under the supervision of Prof. Byung-Seo Kim, in 2016. In 2013, he was a Lecturer with the University of the Sargodha, Lahore Campus, Pakistan. From July 2016 to August 2021, he was an Assistant Professor with the Department of Computer Science, FAST-NUCES, Chiniot-Faisalabad Campus, Pakistan. After that, he joined FAST-NUCES, Lahore Campus, as an Assistant Professor, from September 2021 to June 2022. He is currently an Associate Professor with the FAST School of Computing, National University of Computer and Emerging Sciences, Lahore Campus. He is also a Cisco Certified Network Associate and a Microsoft Certified Professional. Moreover, he is also a HEC-approved Ph.D. Supervisor in Pakistan. His research interests include the design and development of energy-efficient routing protocols, cross-layer architectures, caching and forwarding for cognitive radio ad hoc networks, and named data networking-based wireless networks. He is also a member of KSII, the IEEE Computer Society, the IEEE Communication Society, the IEEE Signal Processing Society, and the IEEE Young Professionals.

MUHAMMAD ANWAR received the Ph.D. degree in computer science from the University of Technology Malaysia (UTM), in 2019. He is currently an Assistant Professor of information technology with the University of Education, Lahore, Pakistan. He has over 15 years of professional experience on different ICT projects in public and private sector organizations. He is a certified Project Management Professional (PMP), Microsoft Certified Professional (MCP), and Cisco Certified Network Professional (CCNP). He has various research publications in high-impact factor journals and conferences. His research interests include sensor networks, green computing, the Internet of Things, machine learning, and blockchain. He is a member of reviewer panels of various journals. He is serving as guest editor of special issues in different journals.

MUHAMMAD FAHEEM received the B.Sc. degree in computer engineering from the Department of Computer Engineering, University College of Engineering and Technology, Bahauddin Zakariya University, Multan, Pakistan, in 2010, the M.S. degree in computer science from the Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia, in 2012, and the Ph.D. degree in computer science from the Faculty of Engineering, Universiti Teknologi Malaysia, Johor Bahru, Malaysia, in 2021. He was a Lecturer with the COMSATS Institute of Information and Technology, Pakistan, from 2012 to 2014. He was also an Assistant Professor with the Department of Computer Engineering, Abdullah Gul University, Turkey, from 2014 to 2022. He is currently a Senior Researcher with the School of Computing (Innovations and Technology), University of Vaasa, Vaasa, Finland. He has authored several papers in refereed journals and conferences and served as a reviewer for numerous journals in IEEE, Elsevier, Springer, Willey, Hindawi, and MDPI. His research interests include cybersecurity, blockchain, smart grid, smart cities, and industry 4.0.

MUHAMMAD WAQAR ASHRAF received the Ph.D. degree from the School of Electrical Engineering, Universiti Teknologi Malaysia (UTM), Malaysia. He is working as an Assistant Professor with the Department of Computer Engineering, Bahauddin Zakariya University, Multan, Pakistan. His research interests include routing and monitoring in wireless sensor networks, optical networks, network survivability, and disaster-aware routing. He has authored several papers in refereed journals and has been serving as a reviewer for numerous journals, such as *International Journal of Communication Systems*, IEEE Access, *Wireless Networks*, *Wireless Personal Communication*, and *Peer-to-Peer Networking*.