Received: 12 November 2020 | Revised: 26 November 2020 | Accepted: 9 December 2020

DOI: 10.1002/spy2.145

RESEARCH ARTICLE

WILEY

Fog computing security and privacy for the Internet of Thing applications: State-of-the-art

Yehia I. Alzoubi | **Valmira H. Osmanaj** | **Ashraf Jaradat** | **Ahmad Al-Ahmad**

Management Information Systems Department, College of Business Administration, American University of the Middle East, Egaila, Kuwait

Correspondence
Yehia I. Alzoubi, Management Information Systems Department, College of Business Administration, American University of the Middle East, Egaila, Kuwait.
Email: yehia.alzoubi@aum.edu.kw

Abstract

Fog nodes are implemented near to end-users Internet of Things (IoT) devices, which mitigate the impact of low latency, location awareness, and geographic distribution unsupported features of many IoT applications. Moreover, Fog computing decreases the data offload into the Cloud, which decreases the response time. Despite these benefits, Fog computing faces many challenges in meeting security and privacy requirements. These challenges occur due to the limitations of Fog computing resources. In fact, Fog computing may add new security and privacy issues. Although many papers have discussed the Fog security and privacy issues recently, most of these papers have discussed these issues at a very high level. This paper provides a comprehensive understanding of Fog privacy and security issue. In this survey, we review the literature on Fog computing to draw the state-of-the-art of the security and privacy issues raised by Fog computing. The findings of this survey reveal that studying Fog computing is still in its infant stage. Many questions are yet to be answered to address the privacy and security challenges of Fog computing.

KEYWORDS

fog computing, Internet of Things, privacy, security

1 | INTRODUCTION

Recently, the Internet of Things (IoT) has become an important and dominated part of many application areas like smart homes, smart businesses, and smart cities.[1] According to Abbasi and Shah,[2] 50 billion devices will be connected to the Internet (ie, each person will have 6.58 connected devices, on average) by 2020 and the number may reach 500 billion by 2025. These IoT devices produce a huge amount of heterogeneous data to be analyzed that require huge storage capacity, computing resources, and network bandwidth. Moreover, many IoT applications require high velocity or real-time analysis (eg, gaming, augmented reality, and big data analysis). The Cloud data centers are geographically centralized which makes it non-effective to deal with the processing and storage demands of highly distributed IoT devices.[3] Therefore, managing and processing such data represent a challenge facing network administrators while managing network infrastructure.

The Fog computing concept was introduced by Cisco in 2012 to enhance the network infrastructure to meet the requirements of a huge amount of data and to boost the efficiency of processing power. Moreover, it was introduced to overcome the issues that face Cloud computing like a real-time response, distribution environment complexity, mobility, and location awareness of IoT applications.[4] Fog computing is expected to make up to 45% of generated data using IoT applications.[5] It has been adopted by many applications such as health care, transportation, energy lattices, mobile big data analytics, MediFog (medical applications), FoAgro (Agriculture and Farming), connected parking system, UXFog (implemented in the centralized shopping centers which witness a huge footfall on a regular basis).[6] Yet, it will be gradually implemented in many other applications.[5]

Fog is a decentralized infrastructure located close to IoT devices to enable management, storage, and communication to the IoT devices. Fog intermediates the IoT-Cloud architecture and extends the Cloud services; however, it does not replace Cloud.[7] It provides on-demand applications and services to IoT devices. Fog node helps resource-constrained IoT devices to conduct computational processing that needs more resources and power. This enables these devices to meet the delay-sensitive requirements of some applications and overcome the issue of bandwidth constraints.

As an extension to Cloud computing, Fog computing inherits some issues from the Cloud, especially security and privacy issues.[8-10] Due to the resource-constrained nature, IoT devices are easy victims.[11,12] To protect these devices, the Fog environment has to provide the required solutions. The current solutions available on the Cloud can help; however, these solutions may not work properly or not applicable in the Fog environment.[13] This is due to the unique features of Fog computing like different providers of Fog nodes, the decentralized infrastructure of the Fog architecture, and the resource-constrained nature of Fog nodes.[14,15]

Therefore, security and privacy issues can be mitigated by providing novel solutions that can meet the special requirements of Fog computing. Recently, many papers have discussed the state-of-the-art of Fog security and privacy issues (eg, [16-23]). However, most of these papers have discussed these issues at a very high level.[24,25] Therefore, more work is still needed in this context to provide a more comprehensive understanding of Fog privacy and security issue. This paper contributes to providing state-of-the-art about the security and privacy issues that face Fog computing, the recommended solutions to mitigate these issues, and the open questions and future directions of Fog security and privacy. This was done by reviewing the available literature. Hence, this paper aims to answer the following research questions:

RQ1: What are the security and privacy issues that face Fog computing?
RQ2: What are the solutions to mitigate the security and privacy issues of Fog computing?
RQ3: What are the future research directions for Fog computing security and privacy?

This paper identified three categories of Fog security and privacy challenges: network services and communications (the network and communication-related issues among IoT-Fog-Cloud architecture), data processing (inside Fog node), and IoT device's privacy (end-user device). Under each of these categories, a number of challenges were identified. This paper reveals that while most of the challenges still need more work to be addressed, some challenges seem to be very critical such as trust management, fault tolerance, computation, big data analysis, forensics, and IoT device location privacy.

The rest of this paper is organized as follows. Section 2 presents the background of Fog computing architecture and applications. Section 3 discusses the state-of-the-art of security and privacy challenges due to the use of Fog computing. Section 4 discusses the open issues and future research on security and privacy. Finally, Section 5 concludes this paper.

2 | BACKGROUND

Cloud computing has definitely improved the information technology era. Cloud computing emerged as an effective method for data processing. However, there are some intrinsic problems with cloud computing including relative expensive cost, scalability, long latency, bandwidth limitations, mobility support, location awareness, and dependability.[19] As a centralized system, cloud computing can perform many computation processes and services. However, for huge amounts of data, the bandwidth of the network can represent a big challenge for cloud computing. This leads to long latency (ie, time for data to travel from one point to another).[16] This issue is very clear when the number of devices increased, especially with applications that require a short time to be conducted. Moreover, the distributed nature of IoT devices has created other issues for Cloud computing related to support mobility and location awareness.[26]

Fog computing was introduced to deal with most of the issues of Cloud computing. It is close to IoT devices, which helps these devices in many issues such as long latency, communication, storage, control, services, and computations.[27] Fog nodes are distributed which helps in solving the issue of mobility and scalability as well as smooth interruptions in the bandwidth of the network. In short, Fog computing can provide many benefits including saving of bandwidth, support of mobility, low latency, Heterogeneity, geographical distribution, and low energy consumption.

2.1 | Fog computing architecture

Fog computing research has not presented a unified architecture that can be reused in different applications.[28] In this paper, the architecture provides a holistic view of the Fog computing-IoT architecture based on the available literature. In this architecture, as shown in Figure 1, each user's device can be connected to one Fog node through wired or wireless access media such as WiFi, Bluetooth, 5G, or ZigBee. Fog nodes communicate with each other through wired or wireless media as well. All Fog nodes are connected to the Cloud by IP core network.[23,29] Network virtualization and traffic engineering are achieved using virtualization technologies such as software-defined network and network functions virtualization.[5,30] In this architecture, three layers can be identified; device layer, Fog layer, and Cloud layer.[31,32] These three layers can be connected directly or indirectly with public authorities such as key generation center and certificate authority.[7,13]

Device layer: In general, the devices in this layer are geographically distributed and have low computation capabilities and limited storage resources. These devices collect and send raw data to the upper layer (Fog layer) for processing and storage.[33]

Fog layer: It is located close to the device layer and it is composed of a large distributed number of Fog nodes. The Fog nodes consist of network equipment (mobile or static) with higher storage and computation resources than the device layer capabilities such as gateways, routers, access points, switches, access points, and so on. This layer tends to extend Cloud computing to the device layer. The Fog layer provides many services and real-time analysis to IoT devices data. In fact, the Fog layer has more capabilities than IoT devices in terms of computing, temporarily storing, and transmitting a summary of the IoT devices data to the Cloud layer. Fog data center contributes toward achieving multi-tenant virtualization, enhance computation, storage, and other resource sharing requirements to meet user demands. It also isolates the data and IoT applications.[15,31,34] The computation power in this layer reduces the processing load on the limited resources IoT devices and helps in computation offloading to the Cloud servers. Since Fog nodes are connected to the Cloud data center, more powerful computing and storage capabilities can be provided to IoT devices.[35] Fog nodes send data collected from IoT devices to the Cloud and send information, services, and other data to IoT. So, Fog plays the role of the Hub in this architecture.

Cloud layer: The Cloud layer consists of multiple high-performance servers and permanent storage of an enormous amount of data. It provides many applications and services such as smart power distribution and smart transportation.[28,36] These services are accessible at any time and from anywhere through the internet connection. The Cloud performs the global analysis on the data submitted by Fog nodes and the data from other sources to gain deeper insight and improve business performance in IoT applications.[9,36,37] However, in this architecture, not all computing and storage tasks go through the Cloud since Fog will execute the light analysis as discussed above. The Cloud layer is efficiently managed by some control strategies to improve the utilization of Cloud resources.[38] By sending policies to the Fog nodes, the Cloud enhances and improves the quality of latency-sensitive services offered by Fog nodes.[29]

2.2 | Fog to enhance security and privacy of IoT applications

Unlike Cloud computing, Fog computing has its own characteristics such as distributed nature, resource-constrained, and remote operation.[39,40] These characteristics have created a unique environment in the IoT applications' security and privacy context. While the Fog can deploy and provide more computing powers to secure and protect IoT devices, it poses additional security and privacy challenges, often encountered as a consequence of these characteristics. That is, it can enhance the security of the IoT layer as a whole since it provides certain local security and privacy services such as local monitoring and threat detection.[41,42] Based on the current literature, majority of the studies reported that Fog decreases the security and privacy of the IoT applications. However, some researchers conclude that in comparison with the Cloud, Fog can enhance security and privacy of the IoT applications. In this section, an overview of how Fog can enhance IoT security is presented, while the new security and privacy issues arise due to the implementation of Fog computing are further discussed in Section 4.

Fog computing facilitates the local data storage and analysis of time-sensitive data. This reduces the amount and the distance of data transmitted to the Cloud and consequently reduces the impact of security and privacy issues of IoT applications.[5,43] Fog computing improves time to action and reduces response time, thus responding faster and locally to security and privacy threats.[44,45] Moreover, Fog nodes can serve as proxies of the IoT devices. These proxies

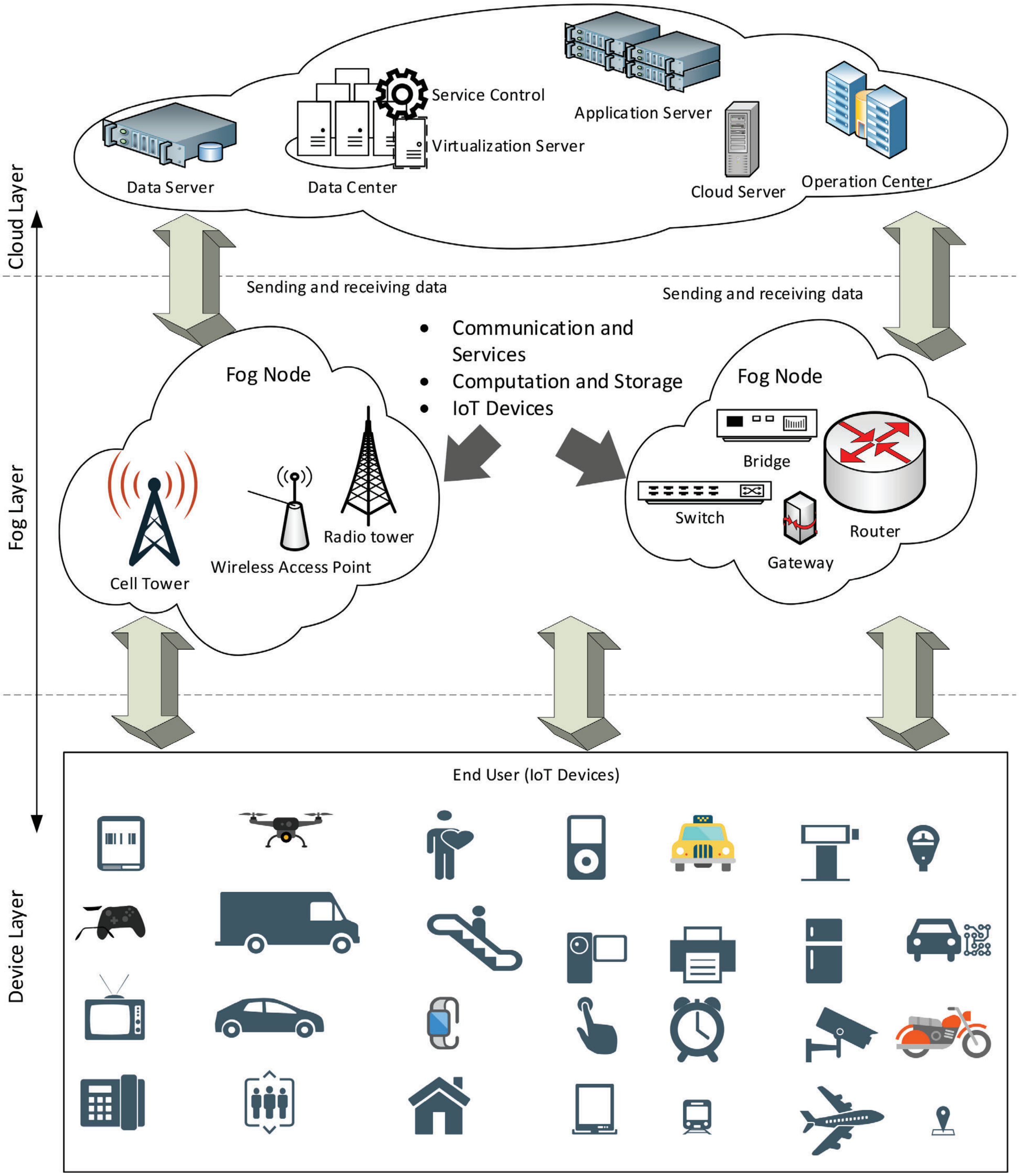

FIGURE 1 Fog computing three layer architecture

can manage and update authorization procedures, and eliminate the need to communicate to the Cloud to update these procedures.[14,46]

According to Alrawais et al,[47] using Fog computing will enhance the security and privacy of IoT applications. The authors developed a mechanism that aims to enhance the security and privacy of IoT devices by employing the Fog to improve the distribution of certificate revocation information among IoT devices. In a study conducted by Wang et al,[48] the authors were able to develop an approach that deploys Fog server with fine-grained data access control to enhance Cloud data privacy. According to Prakash et al[49] and due to the local security applicability, Fog computing provides a defined and better security compared to Cloud computing. The authors argue that Fog nodes are managed by Fog data services, which serve various purposes such as data control, data security, data reduction, data virtualization, and data analysis.

In addition to the IoT application security and privacy benefits, Gai et al[50] argue that Fog computing characteristics can be used to enhance the security and privacy of IoT users. The authors proposed a model called Fog-based Multi-Layer Access Control that utilizes the computation and storage facilities in the Fog server. This model is responsible for deploying the access control strategies for each application. It also helps in avoiding using limited computing resources of IoT devices and achieves a changeable access control strategy that enables meeting the requirements of multiple manipulation environments.

In another research conducted by Wang et al,[51] the authors argue that Fog computing can enhance security in the Cloud environment by minimizing the attacks' impact. For instance, in the case of man-in-the-middle, attack impacts can consume few resources in Fog nodes. Only gateways that serve as Fog nodes may be compromised or replaced by fake ones. So, only gateways need to be protected as we have a large number of Fog nodes. Moreover, Fog computing can help in monitoring data access in the Cloud. Combining user behavior profiling and Decoy technology helps in recognizing the legitimate users or masquerades. If the user's behavior deviates from the user baseline, Decoy technology is applied to return large amounts of decoy information to confuse the attackers. In addition, Decoy technology can send the legitimate user information about attackers such as attacker IP or server name, which can be reported for further actions.[51,52]

3 | RQ1 AND RQ2—SECURITY AND PRIVACY ISSUES AND SOLUTIONS OF FOG COMPUTING

To answer the research questions the following steps were followed. (a) We reviewed the major databases to identify the most significant literature in the field of Fog computing. Then, the different issues related to security and privacy of Fog computing were categorized. (b) Each identified challenge was then deeply defined and explained. The subcategories of the main challenge themes were derived and explained. (c) Finally, the proposed and suggested solutions in the future were matched to each of the specific challenges.

What are the security and privacy issues that face Fog computing?

What are the solutions to mitigate the security and privacy issues of Fog computing?

As mentioned in the above section, Fog computing has created a new dilemma of security and privacy-related issues due to its notable characteristics of distribution, heterogeneity, mobility, and limited resources. It would be difficult for the Fog to execute a full suite of security solutions that can detect and prevents attacks due to its relatively low computing power.[53] Also, due to its location (ie, close to IoT devices which means protection and surveillance are relatively weak), the Fog will be easier and more accessible than the Cloud, which increases the probability of attacks. In addition, Fog will be an attractive target to many attacks, due to its ability to obtain sensitive data from both IoT devices and the Cloud, and due to the amount of throughput data.[54,55]

Therefore, Fog nodes may encounter several malicious attacks (eg, man-in-the-middle, authentication, distributed denial of services DDOS attacks, access control, and fault tolerance) and new security and privacy challenges.[28] Moreover, while the Cloud has standard security and privacy measures and certifications, the Fog does not have such standards. Hence, the available security and privacy solutions that work for the Cloud may not work efficiently for the Fog.[56] In the following sections, the state-of-the-art of the Fog security and privacy threats, security and privacy requirements, and security and privacy challenges and solutions are discussed. The challenges framework is shown in Figure 2.

3.1 | Security and privacy threats

Since the Fog is an extension to Cloud computing, it inherits many threats from the Cloud.[57] Moreover, Fog nodes are "honest but curious" in general.[29] This is because these nodes are deployed by Fog vendors who are honest in providing certain services to end-users. However, they may snoop on the content and personal data of the end-users. The providers of Fog may ask the end-users for personal information in order to maintain or fix some issues, which might lead to leakage in the user's privacy. In addition, Fog nodes are an attractive target for many types of attacks. Table 1 summarizes the different attacks that may occur on Fog nodes.[5,29,58,59]

TABLE 1 Security and privacy threats in Fog computing

Threats	Description
Forgery	The attackers imitate their identities to deceive victims by generating fake information. This attack decreases the network performance by consuming energy, storage and bandwidth due to the fake data packets.
Tampering	The attackers modify, delay, or drop the transmitted data over the network to degrade and disrupt the performance and efficiency of Fog computing.
Spam	Unwanted message, created and flooded by attackers. Spam is a serious security concern as it can consume vital resources and deliver malware.
Sybil	Using fake identities to control and compromise Fog nodes. This attack generates fake crowd-sensing reports and can expose the user's personal information.
Jamming	A severe Denial-of-Service attack against wireless medium by emitting radio frequency signals with a large amount of data packets to jam or consume the transmission channels or its resources in order to restrict the legitimate user from having access to the network.
Eavesdropping	Also known as a sniffing and spoofing attack. It occurs when the attackers steal information that computers, smartphones, or other devices transmit over a network, without users' consent.
Denial-of-Service (DoS)	Flood the Fog nodes with a large number of fake requests to make them unavailable for legitimate users. DoS consumes network resources such as bandwidth and battery which decrease the Fog performance.
Collusion	Two or more groups collude together to trick, cheat, or mislead a group of Fog nodes or Fog nodes with IoT nodes or acquire legal advantages.
Man-in-the-middle	The attacker secretly relays and possibly alters the communications between the nodes without discloser to legitimate users.
Impersonation	An attack in which the attacker behaves like a legitimate user or genuine server that offers fake or malicious services to legitimate users.
Manipulation	The attackers manipulate the traffic traversing to compromise the integrity of the communication and services on the Fog. Malicious IoT devices can report incorrect or fake values to disrupt services or calculations.
Rogue Fog node	A Fog device that pretends to be a legitimate node and persuades IoT users to connect to it. The attackers control the Fog node (eg, server, gateway) and its services. They forge false infrastructure, direct the information flow to their rogue data center, inject infrastructure with traffic. The attackers impersonate the authenticator in order to force the IoT device to perform authentication with them.
Privilege escalation	The attackers take advantage of Fog node configuration oversight and programming errors, exploit bugs, or using any vulnerability in a system to gain access to Fog node. Then, the attackers can abuse the users' privileges as a legitimate administrator or can manipulate the services.
Identity privacy	Providing user identity attributes such as name, mobile number, address, visa id, and other details to Fog nodes to grant access to the Fog node services.
Data privacy	Exposing data while communicating on Fog nodes due to attack, unintended loss, or misuse. This may lead to use different users' vital information by unauthorized parties. The risk is high because of the Fog nodes location (near to the end-users).
Usage privacy	Refers to the patterns or order with which the user uses the Fog services such as the sleeping time, time at home, the time users are not home, usual using certain service, and so on.
Location privacy	Refers to users' current or saved locations. The location of users is at risk in the Fog environment because of the spatial correlation between Fog nodes and IoT devices.

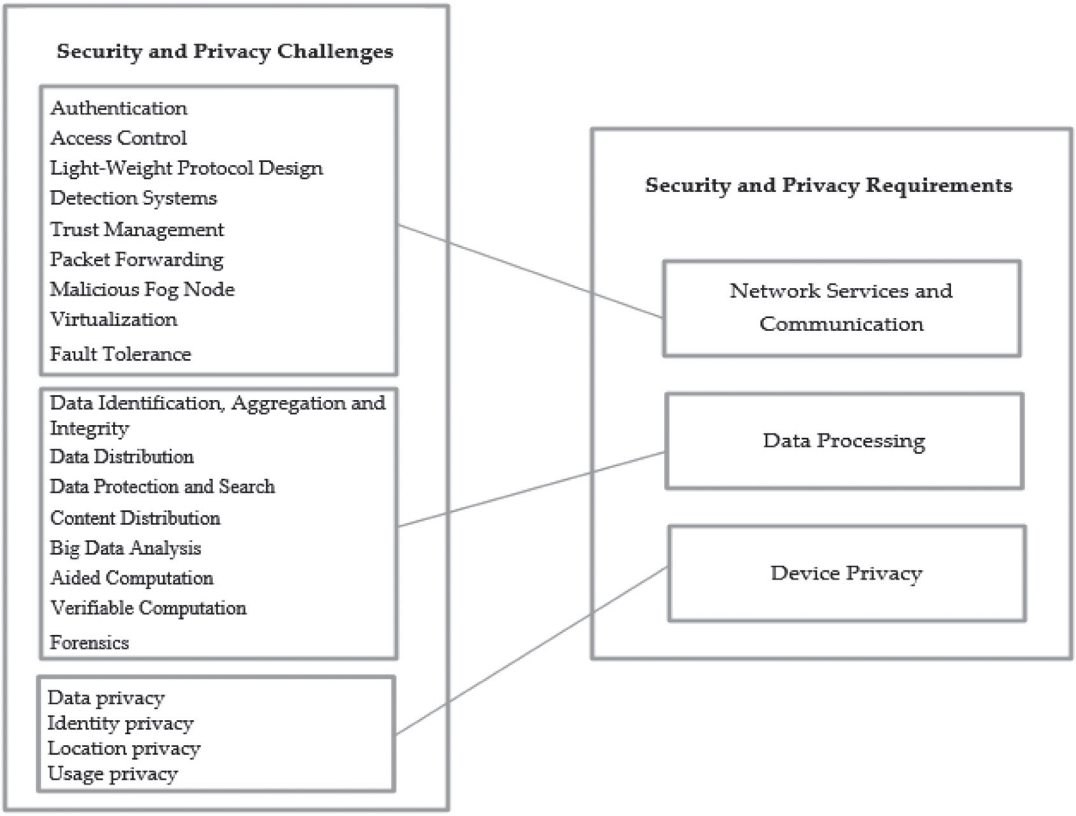

FIGURE 2 Security and privacy challenges of Fog computing

3.2 | Security and privacy requirements

The three essential requirements of security and privacy are confidentiality of data transmission and storage, the integrity and availability of data. Confidentiality ensures that only the data owner (ie, IoT device user) can access the data. This prevents unauthorized access while data are transmitted or received among the device layer, Fog layer, core network, and when data are stored or processed in Fog or Cloud data centers.[60] Confidentiality can be attained by data encryption.[28] Integrity ensures that the data delivered is correct and consistent without distortion or undetected modification. It also prevents the data stored from modification or distortion. Data integrity checking mechanisms can be used to ensure the consistency between sent data and received data.[28,61] Availability ensures that the data are available and accessible by authorized parties (eg, anywhere and anytime) as per users' requirements.[3]

To achieve these requirements, different tools, techniques, procedures, and strategies (eg, authentication, encryption) should be applied in different layers during data transmission and storing. Based on the available literature (eg, [5,29,59,62]) and the Fog computing architecture in Section 2, this paper identifies three distinguished categories to achieve the above requirements, namely; Fog network services and communication, Fog data processing (storage and computation), and IoT devices privacy. Under each of these categories, certain security and privacy measurements need to be applied to meet the above-mentioned requirements.

3.2.1 | Network services and communication

Fog nodes are equipped with mini data centers (ie, some storage and computing capabilities). This layer of the Fog node provides network and communication, management, and other services to the IoT devices. It enables communications with the Cloud and with IoT devices through many devices such as routers, switches, base stations, bridges, and so on. Since Fog intermediates IoT devices and the Cloud, it provides many communication functions to both the Cloud and IoT devices (eg, packet forwarding and routing, data aggregation).[24] Fog node collects data from IoT devices and then either processes it or sends it to the Cloud after aggregation.[63] It also shares the data and other services that come from the Cloud with the IoT devices.[23,64] Fog nodes are equipped with computing resources and local servers, which enable it to provide storage, data processing, computation, and analysis to IoT device's data.[64] This enables the Fog to run real-time processing of the data collected. As a result, real-time processing may help in the decision-making process, especially for time-sensitive applications such as healthcare and traffic lights systems.

For network services and communication category, the privacy and security requirements should be met through authentication, access control, light-weight protocol design, detection systems, trust management, packet forwarding, detecting malicious Fog node, virtualization capability, and fault tolerance capability.[5,8,29] Table 2 summarizes these requirements.

3.2.2 | Data processing

The transient Fog storage has the capability to temporarily maintain the data collected from IoT devices, which allows IoT devices to maintain the frequently accessed data and achieves quick updates of data.[29] The collected data are usually kept in the Fog for a short time (ie, 1-2 hours) before submitting to the Cloud. Thus, the transient Fog storage help in reducing the communication overhead with the Cloud and the response time to access and update the data.[8] Moreover, this storage enables performing decentralized data computation among multiple Fog nodes cooperatively. This means, Fog nodes can assist IoT devices to conduct heavy computational operations on behalf of the Cloud, which decreases the data offloaded on both IoT devices and the Cloud.[29]

Fog can assist in many IoT applications such as file maintenance, shopping cart management, and software and credentials updating.[47] Also, Fog data centers serve the purpose of multi-tenant virtualization.[5] For data processing category, the privacy and security requirements should be met through data identification, aggregation and integrity, secure data distribution, data protection and search, content distribution, big data analysis, aided computation, verifiable computation, and forensics. Table 3 summarizes these requirements.

3.2.3 | IoT devices privacy

For device privacy, the requirements should be met through identity privacy, data privacy, location privacy, and usage privacy. Table 4 summarizes these requirements. Each IoT device has a unique identity that shares with the Fog node. It also shares the location and data. Fog nodes share IoT identity, location, and sometimes data for analysis with other nodes or when sent to the Cloud. In addition, the usage pattern of the IoT device can be used to identify that IoT device. For example in the smart grid, a lot of information can be disclosed when reading the smart meter such as the time the TV is on, the time people are at home, and so on.[58] This leads to a breach of IoT device privacy.

3.3 | Security and privacy issues and solutions

The real-time services provided by the Fog do not come with no expense; security and privacy would be the major challenges in this context.[5] Since the Fog is deployed near to the end-users of IoT devices, some places would not be highly protected. This issue increases the probability of malicious attacks. Moreover, the distributed nature and the multi-level collaboration among Fog nodes increase the privacy issues.[24] Furthermore, the resources constraints make the privacy situation even worse in the Fog environment. To mitigate the impact of these issues, some solutions have been proposed in the literature. Following the categories as in Figure 2, the privacy and security challenges, as well as the solutions and their limitations are presented in this section.

3.3.1 | Network services and communication

In the Fog environment, the IoT devices communicate with the Fog node for processing or storage requirements. Fog nodes communicate with each other in order to process specific tasks, manage resources, or transfer data to the upper level (ie, the Cloud). So, communication between IoT devices and Fog nodes and between Fog nodes should be secured.[53,65,66]

TABLE 2 Network services and communication requirements in Fog computing

Challenge category	Challenge	Description
Network services and communication	Authentication	• Authentication is the process that ensures the identity of the IoT devices is true (ie, it is a process of establishing proof of the user's identity).[59] • Authentication in Fog is done in order to access personnel devices locally and not relying on Cloud servers.[62] • The user must be able to identify himself/herself in the Fog.[65]
	Access control	• Access control uses control strategies that enable all security and privacy entities. It determines who can access the resources (authentication) and the kind of actions can perform such as reading (confidentiality) and writing (integrity).[59] • Access control systems ensure that a particular Fog node has the right to authorize IoT devices.[2] • Usually, access control is defined for the same domain; however, it is defined cryptographically in Fog environment due to its distributive nature.[132]
	Light-weight protocol design	• Communicating and processing IoT device service should be done in real-time (short time). Therefore, lightweight communication protocols between the IoT and Fog node should be used.[29]
	Detection systems	• The systems that can detect/predict and warn the administrator in advance about the malicious attacks such as Virus and Trojan attacks.[2]
	Trust management	• Ensures that all parties in the Fog environment are fully trusted. Fog nodes should establish different trust levels with other Fog nodes.[133] • In Fog environment, trust should be a two-way process between Fog node and the IoT devices.[65]
	Packet forwarding	• Fog nodes act as intermediate media to forward data from IoT devices or other Fog nodes to the upper Fog levels or from upper levels to IoT devices.[29]
	Malicious Fog node	• Malicious Fog node (ie, acts as a legitimate node, but it is rather a compromised node) will affect the data integrity, security, privacy. It may decrease the efficiency of the entire Fog platform, create back doors, and damage the end-users' data.[104] • Malicious Fog node is used to execute many insider attacks.[8] • Fog nodes that are authenticated by the Cloud should trust the Cloud and no Fog node should manage another node.[133]
	Virtualization	• This attack occurs due to executing all virtual machines (VMs) in a virtualized environment which affects adversely Fog users, data, and services. Virtualization issues include attacks such as Hypervisor attacks, VM-based attacks, weak or no logical segregation, and side channel-attacks.[104] • The malicious VM may manipulate the services and it may overtake the control of the underlying hardware and operating system of the Fog node to launch attacks.[2]
	Fault tolerance	• Fog node should provide services normally if an individual sensor, service, network, platform, or application fail. IoT device should be able to switch to other adjacent nodes when the service fails.[62]

TABLE 3 Data processing requirements in Fog computing

Challenge category	Challenge	Description
Data processing	Data identification, aggregation, and integrity	• IoT devices cannot identify and distinguish sensitive and important data out of the huge amount of generated data. • The users lose their possession of the data when the data are maintained on Fog nodes, and the data on Fog nodes may be modified. The processed data will be unknown to its owner.[67] • During the process of data encryption, and before sending data to Fog nodes, secure data aggregation is critical to prevent data leakage and reduce communication overhead on Fog nodes (Fog nodes temporarily store the received data or deliver it to the Cloud).[29] • IoT devices send data to the nearest Fog nodes (the data are divided into some parts and sent to several Fog nodes) to process it. Then, the processed data is merged from different nodes, which put the integrity of the data at risk; especially if some nodes were malicious.[133]
	Data distribution	• Once the data are encrypted before uploaded to Fog nodes, it is impossible for other entities to read them, except the data owner who cannot share it with other entities after encryption.[5] • Due to privacy and security issues, stakeholders rarely share data.[87]
	Data protection and search	• It is hard for the IoT devices to distinguish sensitive data before uploading, so Fog node should first identify the sensitive data in order to protect it.[29] • Once data are sent to Fog, it should be encrypted. This makes it hard for the data owner to retrieve it. To enable data search, owners should build a secure index when they upload data to Fog nodes.[8] • Not like Cloud computing; different keywords will be used to search the data after processing by the Fog node.[67]
	Content distribution	• It refers to define who and what kind of broadcasting content to share in order to ensure information protection.[67] • When users join a new service, the secret key used to distribute content should be updated to prevent the new joiner user from learning the previous content.[29]
	Big data analysis	• Fog nodes enable an on-demand decentralized analysis of big data, which is important for time-sensitive IoT applications.[116] • Decentralized big data analysis in Fog computing is pretty critical and challenging.[59] • Fog nodes store and aggregate data generated by many IoT devices temporarily (transient storage), so sensitive data should be identified before processing to decrease processing complexity.[66]
	Aided computation	• Fog nodes can run complicated computing tasks (ie, secret computation using insecure auxiliary devices) on behalf of IoT devices to improve the computational efficiency.[29] • Some of the sensitive information such as user's secret keys may be exposed when data are sent to the Fog node to conduct some tasks.[5] • Since the user does not have full control over computations in distributed Fog environments, privacy and security issues will occur.[8]
	Verifiable computation	• Verifiable computing enables a device to offload the computation to the Fog node.[58] • Whether the returned computational results from the Fog are correct or not, they cannot be guaranteed since there is no mechanism to check the correctness of the returned results.[29]
	Forensics	• Any attack will leave certain evidence behind, which can be used to reveal information about the attackers and their methods.[8] • Fog forensics is partially related to Cloud forensics. However, the Fog has its specific challenges due to limited resources and distributed nature of Fog nodes.[51] • It is reasonable to retrieve some evidence about Fog operation and incidents from the services deployed in the Fog.[69]

TABLE 4 Device privacy requirements in Fog computing

Challenge category	Challenge	Description
Device privacy	Data privacy	• Guarantee that the data are secret under the honest but curious adversaries.[59] • Illegal access to the database may compromise Fog system's data (ie, data loss, data breach, data ownership, data replication, and data sharing).[104] • This issue includes attacks such as SQL injection, cross-site scripting, cross-site request forgery, and session/account hijacking.[104]
	Identity privacy	• Guarantee that the user's identity is secret under the honest but curious adversaries.[59] • The trusted but curious adversaries might collect the identity of data generated during the auditing process.[66] • Multi-level collaboration in Fog environment results in a large number of privacy problems, mainly identity management.[62]
	Location privacy	• Guarantee that the user's location is secret under the honest but curious adversaries.[59] • The communication streams in the Fog do not isolate device identity from its location.[88] • Fog node and the Cloud can learn the location of the user. If the user utilizes or consumes many Fog services, one can easily identify the path of the data.[132]
	Usage privacy	• Guarantee that the habitual or regular user's usage pattern of IoT device is secret under the honest but curious adversaries.[132] • Usage pattern may also refer to the frequency of data being sent to the Fog nodes.[89] • The adversary can infer sensitive information (eg, Smart grid) such as at what times the user is unavailable at home and switch on and off certain appliances.[5]

The traditional cryptographic techniques cannot be effective in Fog environment due to its unique characteristics. New techniques and solutions were proposed in the literature to enable secure communication and service sharing in the IoT-Fog architecture; however, these solutions come with many limitations. Table 5 summarizes the network services and communication challenges solutions and their limitations.

3.3.2 | Data processing

Similar to Cloud computing, the same security and privacy threats are introduced in the Fog environment as the user's data are handed to the Fog node. This occurs because data may be lost, incorrectly modified, or abused by unauthorized people. To address this issue in the Cloud, auditable data storage was proposed. It includes public audibility, supporting data dynamics, and batch verification requirements.[55,58]

Even though, these techniques used in the Cloud, they cannot be directly applied in the Fog environment since the data stored in the Fog data center is not the same as the user's data (ie, the data are processed by Fog node). In the Cloud, the data stored is the same as the user's data.[67] New techniques and solutions were proposed in the literature to enable secure data processing in the Fog environment. Yet, they come with many limitations. Table 6 summarizes the data processing requirements challenges solutions and their limitations.

3.3.3 | IoT devices privacy

IoT user's privacy such as identity, data, and location should be paid high attention when using services like Cloud or Fog computing. In the Fog environment, the privacy-preserving is more challenging than Cloud due to the distribution

TABLE 5 Network services and communication challenges and solutions in Fog computing

Challenge	Available solutions	Limitations
Authentication	• Identity, cooperative, and anonymous authentication.[29] • Associating an incoming request with a set of identifying credentials in the Fog environment.[134] • Public Key Infrastructure based technique and biometric-based authentication.[58] • Decoy technique.[2,135] • Single-domain authentication, cross-domain authentication, and handover authentication.[91]	• None of the previous works have given a holistic solution.[62] • Heterogeneity of Fog nodes and IoT nodes makes the authentication protocols unsuitable for Fog systems.[87] • Extra communication and delay due to users' mobility.[89] • Authentication overhead, redundant authentication and poor scalability.[58] • Decoy technique needs extra storage, and cannot differentiate between false positive and false negative.[2] • Cooperation of Fog nodes and privacy preservation is required.[134] • Response delay is not acceptable for real-time services.[5] • The users' mobility and de-anonymization attacks represent major challenges of anonymous authentication.[29]
Access control	• Policy-driven security management framework.[102] • Fog-based Privacy aware Role-Based Access Control.[131] • Decoy technique.[2] • Attribute-Based Encryption access control.[132] • Policy-based access control mechanism.[132] • Public key-based solutions to achieve fine-grained access control.[58] • Leakage-resilient functional encryption schemes.[87] • Device and key management.[29]	• There must be consistent access policy for each user employing different devices to access the Fog services.[5] • More data security countermeasures decrease the computational power and consumes more storage resources.[104] • Strong credential handling policies, distributed access control architecture, multiple device management, and key management are needed.[5] • Different requirements and regulations are used.[66] • Human errors, management system, and wrong decisions can hinder the security.[2]
Light-weight protocol design	• Lightweight elliptic curve cryptosystem.[29] • Light-weight encryption algorithms or masking techniques.[62] • Hash functions and stream chippers.[5]	• Need to design efficient lightweight protocols to support real time services.[5]
Detection systems	• Signature based, Artificial Intelligence based, neural network based, association rule based, fuzzy logic and support vector machine based.[2] • Lightweight countermeasure utilizing Bloom Filters.[87] • Host-based, network, and distributed detection systems.[29]	• It is challenging to design robust, reliable and efficient detection systems in heterogeneous, decentralized, and distributed Fog architecture.[59] • Local and global detection systems are needed in Fog computing.[8] • Basic user's information are required to differentiate between legitimate and Sybil user, which leads to privacy breaches.[5] • More processing and memory capacity are used.[104] • Latency requirement might not be met due to Fog computing characteristics.[58]
Trust management	• Trusted execution environment.[58] • Region-Based Trust-Aware.[131] • Self-managed trust management system, quantitative trust management component, and Bayesian network-based trust model.[8,136] • Evidence-based trust model, monitoring-based trust model, and reputation management.[29] • Trusted Platform Module.[88] • Trusted distributed platform over the edge devices.[134]	• Heterogeneity of Fog nodes and IoT nodes makes the trust model unsuitable for Fog computing.[87] • Situational trust matrices are needed for various services and applications.[65] • Adaptive, scalable, and consistent trust management design is needed due to IoT device mobility.[5] • Trade-off between computation cost and security requirements.[91] • Compatibility issues with resource-constrained IoT devices.[91]

Continues

TABLE 5 Continued

Challenge	Available solutions	Limitations
Packet forwarding	• Privacy-preserving packet forwarding.[29] • End-to-end connectivity requires cooperation of other nodes to enable message delivery.[29]	• Consumes the nodes limited resources.[5] • Malicious node may join and perform malicious data packets.[5]
Malicious Fog node	• Deploy detection systems.[58] • Trust-based routing mechanism.[5]	• Fake Fog node is hard to be addressed due to the complexity of the trust situation that requires different trust management schemes, dynamic creating, deleting of virtual machine instance that make it hard to maintain a blacklist of rogue nodes.[58] • Scalability issues, message overhead, slow convergence.[114]
Virtualization	• Virtual machine monitor between the host operating system and the guest virtual machines.[2] • Isolation policies, network abstraction, hypervisor hardening, and separation of roles and virtual machines.[8] • Multi-factor or mutual authentication, host and network detection system, user-based permissions model, private networks and process.[104]	• Efficient resource policies are needed.[104] • Restriction of physical access might be difficult to implement.[8] • Performance overhead.[133]
Fault tolerance	• Integration of various mechanisms and strategies (eg, redundant operations, failover capabilities, disaster recovery mechanisms) to enable the service infrastructure to continue its intended operation.[8] • Proactive fault tolerance and hybrid failure handling method.[115]	• Various infrastructure providers might be available at the same location.[116] • Since services are provided at a local level, there may be situations where no replacement is available.[8] • Failure prediction accuracy is high in proactive fault tolerance.[115]

and closeness of Fog nodes to IoT devices. So, it is hard to enable centralized control and may result in collecting more sensitive data such as usage utility, location, and identity.[65,68] Therefore, the privacy-preserving techniques used in the Cloud will not be effective in the Fog environment. In this section, the proposed techniques and solutions in the literature that may enable privacy-preserving in the Fog environment are discussed. However, these solutions also come with many limitations which will be also discussed in this section. Table 7 summarizes the IoT device's privacy challenges solutions and their limitations.

4 | RQ3—CHALLENGES AND FUTURE DIRECTIONS

What are the future research directions for Fog computing security and privacy?

In general, Cloud computing is protected by Cloud providers; however, security and privacy solutions applied to Cloud computing cannot be easily extended to Fog computing.[65] Moreover, the solutions provided by literature to protect the Fog environment have oversimplified the real ecosystem nature of Fog computing (ie, considering the Fog environment as a single Cloud provider).[29] Fog environment involves multiple interacting service providers, services, and infrastructures that belong to different trust domains.[69] Therefore, innovative solutions are required to meet the security and privacy-preserving requirements for the Fog environment. These solutions should ease the collaboration between different components in this complex environment.

This section reveals the open questions, research challenges, and researchers' recommendations to mitigate Fog computing security and privacy challenges. The following is a summary of the recommendations that can help to achieve security and privacy in the Fog environment.[65,69-80]

TABLE 6 Data processing challenges and solutions in Fog computing

Challenge	Available solutions	Limitations
Data identification, aggregation, and integrity	• Trusted Platform Module.[137] • Homomorphic encryption, one-way trapdoor permutation, key distribution, and homomorphic signature.[29] • Combination of homomorphic encryption and searchable encryption.[58] • Symmetric encryption, asymmetric encryption, and provable data possession.[29]	• Overhead of duplicating and identifying sensitive data.[104] • Different requirements in IoT applications.[29] • Data aggregation requirements vary due to heterogeneous IoT application.[5] • Difficult to check the integrity of data due to transient storage, user mobility and variety of keys used by IoT devices.[66] • Data integrity verification management is needed.[5]
Data distribution	• Fine-grained access control and authorization revocation.[67] • Proxy re-encryption, attribute-based encryption, and key-aggregate encryption.[5]	• The efficiency is low in secure data sharing due to time-consuming bilinear pairing.[67] • Access policy may change after the Fog node processes the ciphertexts.[67]
Data protection and search	• Combination of homomorphic encryption and searchable encryption.[58] • Symmetric and asymmetric searchable encryption.[29] • Secure ranked keyword search scheme, attribute-based keyword search scheme, dynamic search method, proxy re-encryption with keyword search approach.[59] • Hybrid key and data encryption schema used for single keyword search.[4]	• Identifying sensitive data is needed, which is very hard.[29] • Difficult to protect sensitive data due to the large number of IoT devices.[66] • Computational overhead.[5] • Confidentiality of the underlying keywords is needed, which cannot be achieved in Fog.[67]
Content distribution	• Secure service discovery.[138] • Broadcast and anonymous encryptions.[139] • Verifiable computational scheme.[140]	• Key management and broadcast encryption are challenging.[29] • Simultaneous secure service discovery and anonymous broadcast encryption are needed.[5]
Big data analysis	• Fully homomorphic encryption and differential privacy.[29] • Certificate-less proxy re-encryption scheme.[141] • Hilbert curve-based cryptographic transformation technique.[142]	• Computational overhead. • Designing decentralized big data analysis is challenging with differential privacy.[66]
Aided computation	• Server aided exponentiation, verification, encryption, function evaluation, and key exchange.[29]	• Extra cost and resources.[91] • Execution of complex computational tasks heavier than exponentiation, encryption/decryption, and signature verification.[91] • Smaller multiple Fog nodes are more powerful than a single server.[5]
Verifiable computation	• Combination of homomorphic encryption and searchable encryption.[58] • Privately verifiable and publicly verifiable computation.[143,144]	• No mechanism to check the correctness of the processed data from the Fog.[29] • Mostly based on theoretical approaches.[58] • Due to distributed architecture of Fog computing, an error may be spread to other nodes resulting in incorrect results.[5] • Verification of results is needed.[8] • Tracing of compromised Fog node is needed.[5]

Continues

TABLE 6 Continued

Challenge	Available solutions	Limitations
Forensics	• Keep track of changes of data location among regions using Mobility Service and the Location Register Database.[131]	• Need more resources and computational processing.[8] • Fog forensics requires international legislation, jurisdictions, and application level logging.[65] • Storing trusted evidence in a distributed ecosystem with multiple trust domains is needed.[116] • Difficult to acquire the log data from Fog devices.[51]

TABLE 7 IoT devices privacy challenges and solutions in Fog computing

Challenge	Available solutions	Limitations
Data privacy	• Lightweight encryption algorithms or masking techniques.[62,81] • Encryption methods like Home-Area Network (HAN).[49] • Identity obstruction techniques.[132,145] • Homomorphic encryption and differential privacy.[58] • Identity-based encryption, attribute-based encryption, proxy re-encryption, homomorphic encryption.[91]	• Memory and processing overhead due to fixed and predefined large sized keys.[5] • High computational cost and communicational overhead.[91]
Identity privacy	• Encryption methods like HAN.[49] • Identity obstruction techniques.[132] • Use identity-based encryption.[91] • Mobility management service to handle changes of users and Fog devices' locations.[131] • Pseudonym techniques.[5]	• The available protection needs third party in Cloud which increase the cost and response delay. Therefore, the low latency of Fog computing will be violated.[89] • Difficult identity authentication realization due to decentralized nature of Fog computing.[62] • Periodic pseudonyms may lead to heavy computation cost in resource constraint IoT domain.[5]
Location privacy	• Identity obfuscation.[58] • Secure homomorphic protocol for fast data encryption and decryption.[87]	• Cloud can know the location of device as it knows the actual location of the Fog nodes.[58]
Usage privacy	• Identity obstruction techniques.[132] • Creates dummy tasks and offloads them to multiple Fog nodes to hide the real among the dummy ones.[58]	• Increase the Fog client's payment and waste resources and energy.[58] • The real tasks are hidden behind fake ones.[58] • Privacy-preserving mechanisms cannot be applied in Fog computing directly due to the lack of a trusted third party.[58]

- Provide the basic services of authentication, authorization, and access control of all components involved in the Fog environment. These services will help to establish secure communication channels among these components even if they belong to different security domains.
- Provide fundamental security mechanisms required by the virtualization infrastructure, such as which virtualization services to use, control which resources they can access, and so on.
- Monitor the status of infrastructure using situational awareness mechanisms.
- Fog computing must provide privacy services for both IoT devices and the service providers since they are part of the Fog environment.
- Fog should have digital evidence management (Forensics).

- Blockchain technology can be highly helpful in the Fog since it enables transparent and verifiable evidence and enhances trust and data sharing decisions. Recently, a tremendous number of publications claim that blockchain can mitigate the impact of many of the above privacy and security challenges (eg, [50,73,76,80-86]). Their findings will be included in the following discussion.

4.1 | Network services and communication

The heterogeneity and dynamic nature of the Fog nodes and IoT devices, and the numerous limitations to the available solutions, as previously shown in Table 5, make these solutions unsuitable to be applied in the Fog environment.[87] IoT device very often joins and leaves Fog nodes.[88] Also, the Fog node frequently joins and leaves another layer. Consequently, there is no guarantee that the service is not going to be interrupted when a new Fog joins or leaves the Fog layer. Therefore, handling the security and privacy issues when a Fog node joins or leaves the Fog layer is a critical issue that has not been addressed yet.[65]

While some authors provide some recommendations or practices to be used, the majority of authors still doubt if the available solutions will meet the security and privacy requirements in the Fog environment. We discuss the recommendations and future opportunities to mitigate network services and communication challenges in the Fog environment in the following subsections.

4.1.1 | Authentication and lightweight protocol design

Authentication at different levels of gateways and nodes is one of the major concerns in Fog computing. It requires further attention to proposing new mechanisms and authentication solutions.[8,69] Authors have provided many recommendations to enable effective authentication in the Fog environment such as the deployment of advanced cryptographic mechanisms, cooperative and lightweight authentication, key agreement protocols, and blockchain technology.[29,65,69,76,81,85,89-96]

Mahmood et al[97] used elliptic curve cryptography and proposed a three-factor remote user authentication scheme for IoT. They used a fuzzy extractor tool to avoid the noisy biometric of a legitimate user. This scheme can modify the user's old password without the help of the server as well as it can cancel a missing smartcard. The authors claimed that this scheme resists major security issues, delivers important security features, sustains less communication and processing costs, and less storage cost than other authentication schemes. Accordingly, results in more resource effectiveness and enhance security.[98] Moreover, Kamil and Ogundoyin[99] proposed a scheme that addressed the shortcomings of the communication in vehicular ad hoc network (VANET) scheme such as signature-forgery attacks by a type II adversary. The authors proposed a demonstrated CLAS scheme with full aggregation for VANET. The authors claimed that the new proposed scheme is secure against both types I and II adversaries as well as more efficient compared to previously proposed schemes.

Varied authentication challenges can be identified and observed that should be exploited in future Fog computing researches.[89] One of these challenges is how to achieve scalable authentication and billing mechanisms in the context of a dynamic Fog computing-based radio access network, where a light-weight and end-to-end authentication are equally important.[65] Identifying and authenticating world-wide infrastructure members of interconnected Fog data centers owned by different companies and individuals is a major challenge to be investigated and analyzed.[8] Design a cross-domain, handover, and mutual authentication between the same entities in different trust domains or between different entities in the same domain is still challenging and needs more work.[91] Moreover, there is a big need to design lightweight protocols that support real-time services and meet different providers' requirements.[29,87]

4.1.2 | Access control

Several useful access control approaches were proposed in the Cloud computing platform, yet they need to be extended and modified to match the distribution, decentralization, and heterogeneity nature in Fog computing.[65,100] For instance, a new level of security was proposed for the Cloud to reduce the stolen information of the users. This proposal was based on designing and delivering decoy information based on user behavior profiling.[61] In order to apply this proposal at the

Fog networks, two issues should be addressed accordingly.[58] The first issue is to determine where to place the decoy in the Fog layer. While the second issue is related to the on-demand design of the decoy information. Other authors have suggested using blockchain technology.[63,81,101]

Some recommendations were provided in the literature to enhance access control in the Fog environment such as using fine-grained access control and authorization infrastructure in each trusted domain, using Fog servers that support multi-layer access control, and implementing a policy-driven security management framework.[8,91,102-105] However, a lot of work needs to be done in this field with regard to design distributed and cross-domain access control mechanisms that support collaboration between heterogeneous resources in the Fog environment.[29,62,65]

4.1.3 | Detection systems

Another issue is related to the deployment and coordination of the perimeter IDSs components inside the Fog system.[89] Challenges such as real-time notification, alarm control, and correct responses have arisen due to the deployment of IDS mechanisms within each level in the Fog architecture.[65] Literature provides some recommendations to deal with the detection systems challenges. One recommendation is using tools to offer partial network monitoring and enable a balance between local and global defense mechanisms, which are able to exchange information with each other.[8,29,104] However, more work should be conducted to design Fog systems that consider the potential of underlying operating systems, coordinate different detection components, and monitor multiple layers or trust domains.[8,65,104]

4.1.4 | Trust management

Due to the openness, vulnerability, and a lack of centralized management, handling trust issues in the Fog network is more challenging compared to the Cloud computing environment.[65] Accordingly, to design a trust model for the Fog, establishing a two-way requirement of trust in Fog, and maintaining trusted relations and interactions with the Fog nodes are intimidating challenges. There is no trusted party that regulates service reliability, network operation, and stability due to the corruption of Fog nodes.[29] Many questions are yet to be addressed[29,58]:

- How to achieve decentralized, situation-aware, scalable, and consistent trust management mechanisms?
- How to achieve a persistent, unique, and distinct identity?
- How to treat intentional and accidental misbehavior?
- How to conduct punishments and redemptions of reputation?

Authors have provided some recommendations that can help in addressing, at least partially, the issue of trust in the Fog environment such as using blockchain technology to maintain the log files, which has the records of events and messages exchanging in Fog nodes in a distributed way.[84,106-111] So, if a Fog node misbehaves, other trusted nodes can discover that. In other words, using Blockchain can enable a trustworthy IoT-Fog-Cloud architecture.[5,69,73,80,109,112] Moreover, deployment of Fog-based middleware, such that a trusted agent estimates the interpersonal trust between a Fog node and the Cloud is required.[59]

4.1.5 | Malicious Fog node and packet forwarding

Applying strong access control to enable good protection to the Fog node, detecting fake, rogue, or compromised Fog nodes and IoT devices is still a big challenge.[87] Reusing Cloud computing's intrusion detection and protection systems can help to detect external attacks with a certain probability only.[29,113] Therefore, further researches on the detection and protection methods from rogue and compromised Fog nodes and IoT devices are an urgent need in Fog computing.[29,87] Moreover, packet forwarding is another big issue in the Fog environment. If one of the intermediate nodes were compromised or identified as untrusted, how can we prevent privacy during packet forwarding[29]?

4.1.6 | Virtualization

According to Nath et al,[114] there is a need to modify the virtualization process in Fog computing to be lightweight. The modification is requested due to resource limitation and to enable automated resource monitoring capability. The authors have provided some recommendations to enhance virtualization process security. This enhancement will be obtained by preventing the honest-but-curious service providers, by considering resource ownership such as giving extra resources for certain virtual machines if they have certain privileges and by applying network isolation among tenants in the virtualization infrastructure.[8,69] Nevertheless, it is essential to develop a new set of security mechanisms to validate the correct deployment, operation, and migration of virtualized services.[69]

4.1.7 | Fault tolerance

According to Naha et al,[115] the hybrid failure handling method can be the best available solution to deal with fault tolerance in the Fog environment. Moreover, in a research conducted by Wen et al,[116] the authors recommend to incorporate redundant replications and user-transparent and deploy fault-tolerant and execution techniques in Fog orchestration design. However, other authors (eg, Abbasi and Shah[2]) reported that the fault tolerance issue has not been paid enough attention in the literature. Moreover, Zhang et al[59] emphasize the need to design new novel methods that can offer sufficient caching capabilities and consume fewer resources.

4.2 | Data processing (storage and computation)

Usually, Fog nodes receive data from IoT devices and send them to the Cloud after processing or forwarding data received from the Cloud to IoT devices. The data sent to the Cloud from the Fog nodes would never be the same data sent by IoT devices due to the processing stage (eg, data will be of different size, structure, or validity).[67] Also, Fog nodes come from different providers, which means some of these nodes are not trustable. Therefore, many privacy and security issues come to the surface after data processing. This section provides an overview of the authors' recommendations and future research opportunities to mitigate data processing challenges in the Fog computing environment.

4.2.1 | Data identification, aggregation, and integrity

The data sent from the Fog to the Cloud will be modified. Hence, identification and integrity of the data will be hard to be achieved. Guan et al[67] identified some properties that should be met by the Fog to achieve identification and integrity. Four properties are outlined as follows: (a) Integrity verification: if the data are modified in the Fog, the IoT device user will never be able to verify the correctness and integrity of data stored in the Cloud. Therefore, the Cloud should be able to verify the received data and to check the validity and integrity of the data. (b) Minimum overhead: this means Fog computing should not request extra burden by IoT users and the Cloud should achieve integrity verification. (c) Public auditing: this means Fog computing should have the ability of public verification especially when the IoT user and the Cloud cannot achieve consensus on the data to be stored in the Cloud. (d) Support dynamics: this means that Fog should support the dynamic environment that corresponds to the dynamic change of IoT users and data updating by IoT users.

Other authors recommend identifying sensitive data and using appropriate mechanisms to protect it, applying a multi-key homomorphic signature for data aggregation, blockchain, and deploying backup and recovery mechanisms.[29,67,104,117] However, there is a need to design secure and private offloading and load balancing mechanisms, secure provable data possession protocols to guarantee data integrity, and to focus on dynamic batch auditing and low complexity mechanisms in future research.[29,87,91]

4.2.2 | Data and content distribution

The powerful cryptographic primitives such as attribute-based encryption used in the Cloud cannot be directly used in the Fog since the access policy of ciphertexts will be different after processing by the Fog nodes, hence Fog computing should guarantee that the access policy remains the same after ciphertexts are processed by the Fog nodes.[67] Moreover, deployment of the social network, enabling IoT users to make the decision of data sharing, and deployment of the blockchain technology need to be considered.[3,69,72,91,118-122]

Establishing secure and private fine-grained data sharing within the heterogeneous environment is one of the motivating tasks that need to be considered in Fog computing research.[29,69] Therefore, exploring different data distribution strategies, as entities federation, and efficient encryption scheme for unified and secure integration of current protocols and standards become a necessity for achieving secure and private data distribution network.[69] Moreover, investigating new approaches for service discovery and anonymous broadcast encryption should be considered in future research.[29]

4.2.3 | Data protection and search

Since the data sent to the Fog are processed before sending it to the Cloud, how the IoT device can search for the required data? For a healthy Fog computing development, issues related to secure search need to be addressed in future Fog computing researches.[29] Such issues are focusing on how to design a secure keyword search schema, a secure and efficient index, a scalable and decentralized secure infrastructure, and practical publicly verifiable computation schemes suitable for IoT applications.[59,67]

4.2.4 | Data computation (aided, verifiable, and big data analysis)

Many valuable solutions were provided for data computation service in the Cloud. However, these solutions cannot be applied directly in the Fog, especially verification solutions. The end-user sends tasks to the local Fog nodes and obtains the computation. Whether the returned results are correct or not, results cannot be guaranteed since the Fog and the Cloud cannot be trusted. There are no mechanisms in place to check the correctness of the returned results. Many questions are yet to be addressed in future research[29,59,87]:

- How to design decentralized big data analysis with differential privacy in Fog computing?
- How to build secure verifiable computing among different trust domains? How to design practical publicly verifiable computation schemes suitable for IoT applications in Fog computing?
- How can Fog nodes assist IoT devices to perform aided computation tasks to satisfy different features and goals in IoT applications?
- How to build a scalable, efficient, and decentralized secure infrastructure in Fog computing?

4.2.5 | Forensics

Evidence management at the Fog is a very complex issue due to the different infrastructures, technologies, actors, and scenarios involved.[8] Therefore, an important task that needs to be addressed in future Fog computing researches is overcoming cross-border legislation challenges.[2] This task is required by Fog forensics due to the need for international legislation and jurisdictions and application-level logging.[65] Moreover, issues such as mobile forensics, virtualization forensics, storage forensics, and the management of evidence in IoT paradigms need to be further investigated.[8,65]

4.3 | IoT device privacy

Due to the distribution of Fog nodes and its closeness to IoT devices, centralized control system like what we have in the Cloud is not possible. Therefore, new innovative techniques and solutions are required to enhance IoT users and data privacy in the Fog environment[24,123,124] such as using the blockchain technology.[26,27,125-128] This section discusses the recommendations and future opportunities to mitigate this issue.

4.3.1 | Data privacy

Due to the fact that people are not willing to extremely expose their sensitive information to an untrusted party, techniques like using blockchain, anonymity system between different Fog nodes layers, enabling IoT users to determine the most suitable mechanism to protect their data, enabling IoT device to facilitate the application of some privacy techniques, and decreasing the complexity of the cryptographic algorithm can be utilized to balance the trade-off between the functional benefits of data computation and the privacy perspective.[8, 50, 57, 69, 82, 89, 91, 129, 130] Nevertheless, more efforts should be paid toward extending these techniques and designing new efficient and effective privacy-preserving solutions. These solutions should be able to divide the applications that ensure the usage of distributed resources and minimize the disclosing of private information. Moreover, there is a need to design a new lightweight, dynamic, and distributed secure data storage system based on several functional encryption methods to cope with the Fog computing data privacy nature.[29,58,91]

4.3.2 | Identity privacy

Maintaining anonymity and tracing the IoT users with their true identity if the misbehave is a big challenge in the Fog environment.[65] Authors have reported some recommendations to enhance identity privacy in the Fog environment by using an anonymous and stateless process to keep user's identity private and defining some levels of privacy protection in data combination.[29,104] However, further studies on identity privacy should be carried out, which should focus on aspects like designing new privacy-preserving methods, mechanisms that allow users to identify their own privacy requirements, mechanisms to identify the misbehaved users, and dynamic fine-grained identity privacy-preserving schemes.[8,69,90,91]

4.3.3 | Location privacy

The user's location is always exposed to Fog computing, even if a proper anonymity technique is utilized to hide the user's identity.[29] As a result, it is difficult to protect users' location privacy since a curious Cloud can always learn about the rough regions of users according to the geographic locations of Fog nodes.[90] Development of mobility management services that handle changes of users and Fog node location, and using the anonymity system between the Fog nodes are some of the recommendations to mitigate the leakage of location privacy.[89,131] However, further studies on location privacy should be carried out, where aspects like global location privacy and local location privacy need to be further investigated. Furthermore, techniques that focus on fine-grained location privacy should be developed.[60,70]

4.3.4 | Usage privacy

Due to the lack of a trusted third party, privacy-preserving mechanisms cannot be directly applied in Fog computing. Using anonymity systems in the Fog environment was recommended to hide the usage behavior of IoT devices.[90] Nevertheless, an alternative solution would be by designing a smart way of partitioning the application to make sure the offloaded resource usages do not disclose the privacy of the information.[58]

5 | CONCLUSIONS AND FUTURE DIRECTIONS

Although Fog computing can provide more local security services to IoT devices as a whole, the characteristics of Fog computing such as homogeneity, distribution, resource-constraints, and remotely operated system pose new security and privacy issues compared to centralized Cloud computing. The privacy and security solutions that are effective in Cloud computing cannot be applied directly to Fog computing due to the above characteristics. Therefore, new solutions are required to mitigate these issues in the Fog environment.

The poor security and privacy system lead to a significant performance problem. Hence, security and privacy solutions should be integrated with the Fog environment. However, sometimes involving a high level of security and privacy countermeasures can compromise the performance of the Fog node. In other words, a trade-off between Fog node performance and the level of these countermeasures is expected. Thus, a balance between the Fog performance and the privacy and security level is required.

This paper reviewed the available literature on the issues of security and privacy in the Fog environment, the solutions, and the recommendations to mitigate the impact of these issues. Moreover, future research opportunities and unanswered questions regarding these issues were critically discussed. This paper identified three categories of Fog security and privacy challenges: network services and communications, data processing, and IoT device's privacy. Under each of these categories, a number of challenges were identified. This paper reveals that while most of the challenges still need more work to be addressed, some challenges seem to be very critical such as trust management, fault tolerance, computation, big data analysis, forensics, and IoT device location privacy. Future research needs to investigate other tools and techniques that should be applied in Fog computing environment that suit its own nature. Moreover, new innovative solutions should be proposed.

ACKNOWLEDGMENT

Open access funding enabled and organized by Projekt DEAL.

ORCID

Yehia I. Alzoubi https://orcid.org/0000-0003-4329-4072

REFERENCES

1. Li C, Qin Z, Novak E, Li Q. Securing SDN infrastructure of IoT–fog networks from MitM attacks. *IEEE Internet Things J*. 2017;4:1156-1164.
2. Abbasi BZ, Shah MA. Fog computing: security issues, solutions and robust practices. Paper presented at: Proceedings of 2017 23rd International Conference on Automation and Computing (ICAC); 2017: 1–6.
3. Kouicem DE, Bouabdallah A, Lakhlef H. Internet of things security: a top-down survey. *Comput Netw*. 2018;141:199-221.
4. Xiao M, Zhou J, Liu X, Jiang M. A hybrid scheme for fine-grained search and access authorization in fog computing environment. *Sensors*. 2017;17:1423.
5. Tariq N, Asim M, Al-Obeidat F, et al. The security of big data in fog-enabled IoT applications including blockchain: a survey. *Sensors*. 2019;19:1788.
6. Kunal S, Saha A, Amin R. An overview of cloud-fog computing: architectures, applications with security challenges. *Secur Privacy*. 2019;2:e72.
7. Dastjerdi AV, Gupta H, Calheiros RN, Ghosh SK, Buyya R. Fog computing: principles, architectures, and applications. *Internet of Things*. Netherlands: Elsevier; 2016:61-75.
8. Roman R, Lopez J, Mambo M. Mobile edge computing, Fog et al.: a survey and analysis of security threats and challenges. *Future Gener Comput Syst*. 2018;78:680-698.
9. Kartheek D, Bhushan B. Security issues in fog computing for internet of things. *Architecture and Security Issues in Fog Computing Applications*. Pennsylvania: IGI Global; 2020:53-63.
10. Elazhary H. Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: disambiguation and research directions. *J Netw Comput Appl*. 2019;128:105-140.
11. Khalid T, Abbasi MAK, Zuraiz M, et al. A survey on privacy and access control schemes in fog computing. *Int J Commun Syst*. 2019;34(2):1-39.
12. Hussain A, Kiah MLM, Anuar NB, Md Noor R, Ahmad M. Performance and security challenges digital rights management (DRM) approaches using fog computing for data provenance: a survey. *J Med Imaging Health Inform*. 2020;10:2404-2420.
13. Puthal D, Mohanty SP, Bhavake SA, Morgan G, Ranjan R. Fog computing security challenges and future directions [energy and security]. *IEEE Consum Electron Mag*. 2019;8:92-96.
14. Chiang M, Zhang T. Fog and IoT: an overview of research opportunities. *IEEE Internet Things J*. 2016;3:854-864.
15. Sittón-Candanedo I, Alonso RS, Corchado JM, Rodríguez-González S, Casado-Vara R. A review of edge computing reference architectures and a new global edge proposal. *Future Gener Comput Syst*. 2019;99:278-294.
16. Mukherjee M, Ferrag MA, Maglaras L, Derhab A, Aazam M. Security and privacy issues and solutions for fog. *Fog and Fogonomics: Challenges and Practices of Fog Computing, Communication, Networking, Strategy, and Economics*. Hoboken, NJ: Wiley; 2020:353-374.
17. Ashi Z, Al-Fawa'reh M, Al-Fayoumi M. Fog computing: security challenges and countermeasures. *Int J Comput Appl*. 2020;975:8887.
18. Ali A, Ahmed M, Imran M, Khattak HA. Security and privacy issues in fog computing. *Fog Computing: Theory and Practice*. Hoboken, NJ: Wiley; 2020:105-137.
19. Desai S, Vyas T, Jambekar V. Security and privacy issues in fog computing for healthcare 4.0. *Fog Computing for Healthcare 4.0 Environments*. Cham: Springer; 2020:291-314.

20. Tange K, De Donno M, Fafoutis X, Dragoni N. A systematic survey of industrial internet of things security: requirements and fog computing opportunities. *IEEE Commun Surv Tutorials*. 2020;22:2489-2520.
21. Caiza G, Saeteros M, Oñate W, Garcia MV. Fog computing at industrial level, architecture, latency, energy, and security: a review. *Heliyon*. 2020;6:e03706.
22. Karthika P, Babu RG, Karthik P. Fog computing using interoperability and IoT security issues in health care. *Micro-Electronics and Telecommunication Engineering*. Singapore: Springer; 2020:97-105.
23. Neware R, Shrawankar U. Fog computing architecture, applications and security issues. *Int J Fog Comput (IJFC)*. 2020;3:75-105.
24. Shen X, Zhu L, Xu C, Sharif K, Lu R. A privacy-preserving data aggregation scheme for dynamic groups in fog computing. *Inform Sci*. 2020;514:118-130.
25. Sengupta J, Ruj S, Bit SDA. Comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *J Netw Comput Appl*. 2020;149:102481.
26. Ashik MH, Maswood MMS, Alharbi AG. Designing a Fog-Cloud architecture using blockchain and analyzing security improvements. Paper presented at: Proceedings of 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE); 2020: 1–6.
27. Kumar T, Harjula E, Ejaz M, et al. BlockEdge: blockchain-edge framework for industrial IoT networks. *IEEE Access*. 2020;8:154166-154185.
28. Hu P, Ning H, Qiu T, Song H, Wang Y, Yao X. Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things. *IEEE Internet Things J*. 2017;4:1143-1155.
29. Ni J, Zhang K, Lin X, Shen XS. Securing fog computing for internet of things applications: challenges and solutions. *IEEE Commun Surv Tutorials*. 2017;20:601-628.
30. Habibi P, Farhoudi M, Kazemian S, Khorsandi S, Leon-Garcia A. Fog computing: a comprehensive architectural survey. *IEEE Access*. 2020;8:69105-69133.
31. Mouradian C, Naboulsi D, Yangui S, Glitho RH, Morrow MJ, Polakos PA. A comprehensive survey on fog computing: state-of-the-art and research challenges. *IEEE Commun Surv Tutorials*. 2017;20:416-464.
32. Haouari F, Faraj R, AlJa'am JM. Fog computing potentials, applications, and challenges. Paper presented at: Proceedings of 2018 International Conference on Computer and Applications (ICCA); 2018: 399–406.
33. Hassan MA, Xiao M, Wei Q, Chen S. Help your mobile applications with fog computing. Paper presented at: Proceedings of 2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking-Workshops (SECON Workshops); 2015: 1–6.
34. Fernández-Caramés TM, Fraga-Lamas P. Towards next generation teaching, learning, and context-aware applications for higher education: a review on blockchain, IoT, fog and edge computing enabled smart campuses and universities. *Appl Sci*. 2019;9:4479.
35. Elkhatib Y, Porter B, Ribeiro HB, Zhani MF, Qadir J, Rivière E. On using micro-clouds to deliver the fog. *IEEE Internet Comput*. 2017;21:8-15.
36. Bellavista P, Berrocal J, Corradi A, Das SK, Foschini L, Zanni A. A survey on fog computing for the internet of things. *Pervasive Mobile Comput*. 2019;52:71-99.
37. Achouri M. Smart fog computing for efficient situations management in smart health environments. *J Inform Commun Technol*. 2020;17:537-567.
38. Aazam M, Zeadally S, Harras KA. Fog computing architecture, evaluation, and future research directions. *IEEE Commun Mag*. 2018;56:46-52.
39. Rashmi R, Kumar RA. Possible solutions on security and privacy issues in fog computing. Paper presented at: Proceedings of International Conference on Emerging Trends In Science & Technologies For Engineering Systems (ICETSE); 2019.
40. Toor A, ul Islam S, Sohail N, et al. Energy and performance aware fog computing: a case of DVFS and green renewable energy. *Future Gener Comput Syst*. 2019;101:1112-1121.
41. Chiang M, Ha S, Chih-Lin I, Risso F, Zhang T. Clarifying fog computing and networking: 10 questions and answers. *IEEE Commun Mag*. 2017;55:18-20.
42. Amor AB, Abid M, Meddeb A. Secure fog-based E-learning scheme. *IEEE Access*. 2020;8:31920-31933.
43. Pallas F, Raschke P, Bermbach D. Fog Computing as Privacy Enabler. arXiv preprint arXiv:1910.04032; 2019.
44. Jain A, Singhal P. Fog computing: driving force behind the emergence of edge computing. Paper presented at: Proceedings of 2016 International Conference System Modeling & Advancement in Research Trends (SMART); 2016: 294–297.
45. Sarkar S, Chatterjee S, Misra S. Assessment of the suitability of fog computing in the context of internet of things. *IEEE Trans Cloud Comput*. 2015;6:46-59.
46. Khan WZ, Ahmed E, Hakak S, Yaqoob I, Ahmed A. Edge computing: a survey. *Future Gener Comput Syst*. 2019;97:219-235.
47. Alrawais A, Alhothaily A, Hu C, Cheng X. Fog computing for the internet of things: security and privacy issues. *IEEE Internet Comput*. 2017;21:34-42.
48. Wang X, Wang L, Li Y, Gai K. Privacy-aware efficient fine-grained data access control in Internet of medical things based fog computing. *IEEE Access*. 2018;6:47657-47665.
49. Prakash P, Darshaun K, Yaazhlene P, Ganesh MV, Vasudha B. Fog computing: issues, challenges and future directions. *Int J Electr Comput Eng*. 2017;7:3669.
50. Gai K, Wu Y, Zhu L, Xu L, Zhang Y. Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. *IEEE Internet Things J*. 2019;6:7992-8004.

51. Wang Y, Uehara T, Sasaki R. Fog computing: issues and challenges in security and forensics. Paper presented at: Proceedings of 2015 IEEE 39th Annual Computer Software and Applications Conference; 2015: 53–59.
52. Wang Y. A blockchain system with lightweight full node based on dew computing. *Internet Things*. 2020;11:100184.
53. Yassine A, Singh S, Hossain MS, Muhammad G. IoT big data analytics for smart homes with fog and cloud computing. *Future Gener Comput Syst*. 2019;91:563-573.
54. Aljumah A, Ahanger TA. Fog computing and security issues: a review. Paper presented at: Proceedings of 2018 7th International Conference on Computers Communications and Control (ICCCC); 2018: 237–239.
55. Yakubu J, Christopher HA, Chiroma H, Abdullahi M. Security challenges in fog-computing environment: a systematic appraisal of current developments. *J Reliab Intell Environ*. 2019;5:209-233.
56. Khan MA. A survey of security issues for cloud computing. *J Netw Comput Appl*. 2016;71:11-29.
57. Kong Q, Su L, Ma M. Achieving privacy-preserving and verifiable data sharing in vehicular fog with Blockchain. *IEEE Trans Intell Transp Syst*. 2020:1-10.
58. Yi S, Qin Z, Li Q. Security and privacy issues of fog computing: a survey. Paper presented at: Proceedings of International Conference on Wireless Algorithms, Systems, and Applications; 2015: 685–695.
59. Zhang P, Zhou M, Fortino G. Security and trust issues in fog computing: a survey. *Future Gener Comput Syst*. 2018;88:16-27.
60. El Kafhali S, Chahir C, Hanini M, Salah K. Architecture to manage Internet of Things data using blockchain and fog computing. Paper presented at: Proceedings of Proceedings of the 4th International Conference on Big Data and Internet of Things; 2019: pp. 1–8.
61. Maheswari KU, Bhanu SMS, Nickolas SA. Survey on data integrity checking and enhancing security for cloud to fog computing. Paper presented at: Proceedings of 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA); 2020: 121–127.
62. Hu P, Dhelim S, Ning H, Qiu T. Survey on fog computing: architecture, key technologies, applications and open issues. *J Netw Comput Appl*. 2017;98:27-42.
63. McGhin T, Choo K-KR, Liu CZ, He D. Blockchain in healthcare applications: research challenges and opportunities. *J Netw Comput Appl*. 2019;135:62-75.
64. Hao Z, Novak E, Yi S, Li Q. Challenges and software architecture for fog computing. *IEEE Internet Comput*. 2017;21:44-53.
65. Mukherjee M, Matam R, Shu L, et al. Security and privacy in fog computing: challenges. *IEEE Access*. 2017;5:19293-19304.
66. Tian H, Nan F, Chang C-C, Huang Y, Lu J, Du Y. Privacy-preserving public auditing for secure data storage in fog-to-cloud computing. *J Netw Comput Appl*. 2019;127:59-69.
67. Guan Y, Shao J, Wei G, Xie M. Data security and privacy in fog computing. *IEEE Netw*. 2018;32:106-111.
68. Sousa PR, Antunes L, Martins R. The present and future of privacy-preserving computation in fog computing. *Fog Computing in the Internet of Things*. Cham: Springer; 2018:51-69.
69. Rios R, Roman R, Onieva JA, Lopez J. From SMOG to Fog: a security perspective. Paper presented at: Proceedings of 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC); 2017: 56–61.
70. Tuli S, Mahmud R, Tuli S, Buyya R. Fogbus: a blockchain-based lightweight framework for edge and fog computing. *J Syst Softw*. 2019;154:22-36.
71. Jang S-H, Guejong J, Jeong J, Sangmin B. Fog computing architecture based blockchain for industrial IoT. Paper presented at: Proceedings of International Conference on Computational Science; 2019: 593–606.
72. Cech HL, Großmann M, Krieger UR. A fog computing architecture to share sensor data by means of blockchain functionality. Paper presented at: Proceedings of 2019 IEEE International Conference on Fog Computing (ICFC); 2019: 31–40.
73. Lei K, Du M, Huang J, Jin T. Groupchain: towards a scalable public blockchain in fog computing of IoT services computing. *IEEE Trans Serv Comput*. 2020;13:252-262.
74. Muthanna A, A Ateya A, Khakimov A, et al. Secure and reliable IoT networks using fog computing with software-defined networking and blockchain. *J Sens Actuator Netw*. 2019;8:15.
75. Nadeem S, Rizwan M, Ahmad F, Manzoor J. Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture. *Int J Adv Comput Sci Appl*. 2019;10:288-295.
76. Huang X, Ye D, Yu R, Shu L. Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design. *IEEE/CAA J Autom Sin*. 2020;7:426-441.
77. Islam N, Faheem Y, Din IU, Talha M, Guizani M, Khalil M. A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services. *Future Gener Comput Syst*. 2019;100:569-578.
78. Mohanta BK, Jena D, Panda SS, Sobhanayak S. Blockchain technology: a survey on applications and security privacy challenges. *Internet Things*. 2019;8:100107.
79. Yang J, Lu Z, Wu J. Smart-toy-edge-computing-oriented data exchange based on blockchain. *J Syst Architect*. 2018;87:36-48.
80. Bonadio A, Chiti F, Fantacci R, Vespri V. An integrated framework for blockchain inspired fog communications and computing in internet of vehicles. *J Ambient Intell Human Comput*. 2020;11:755-762.
81. Guo R, Zhuang C, Shi H, Zhang Y, Zheng D. A lightweight verifiable outsourced decryption of attribute-based encryption scheme for blockchain-enabled wireless body area network in fog computing. *Int J Distrib Sens Netw*. 2020;16:1550147720906796.
82. Butt TA, Iqbal R, Salah K, Aloqaily M, Jararweh Y. Privacy management in social internet of vehicles: review, challenges and blockchain based solutions. *IEEE Access*. 2019;7:79694-79713.
83. Sharma V, You I, Palmieri F, Jayakody DNK, Li J. Secure and energy-efficient handover in fog networks using blockchain-based DMM. *IEEE Commun Mag*. 2018;56:22-31.

84. Wu B, Xu K, Li Q, Ren S, Liu Z, Zhang Z. Toward blockchain-powered trusted collaborative services for edge-centric networks. *IEEE Netw*. 2020;34:30-36.
85. Almadhoun R, Kadadha M, Alhemeiri M, Alshehhi M, Salah K. A user authentication scheme of IoT devices using blockchain-enabled fog nodes. Paper presented at: Proceedings of 2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA); 2018: 1–8.
86. Firoozjaei MD, Lu R, Ghorbani AA. An evaluation framework for privacy-preserving solutions applicable for blockchain-based internet-of-things platforms. *Secur Privacy*. 2020;3:e131.
87. Yousefpour A, Fung C, Nguyen T, et al. All one needs to know about fog computing and related edge computing paradigms: a complete survey. *J Syst Architect*. 2019;98:289-330.
88. Shirazi SN, Gouglidis A, Farshad A, Hutchison D. The extended cloud: review and analysis of mobile edge computing and fog from a security and resilience perspective. *IEEE J Sel Areas Commun*. 2017;35:2586-2595.
89. Abubaker N, Dervishi L, Ayday E. Privacy-preserving fog computing paradigm. Paper presented at: Proceedings of 2017 IEEE Conference on Communications and Network Security (CNS); 2017: 502–509.
90. Yu S, Wang G, Liu X, Niu J. Security and privacy in the age of the smart internet of things: an overview from a networking perspective. *IEEE Commun Mag*. 2018;56:14-18.
91. Zhang J, Chen B, Zhao Y, Cheng X, Hu F. Data security and privacy-preserving in edge computing paradigm: survey and open issues. *IEEE Access*. 2018;6:18209-18237.
92. Luong NC, Jiao Y, Wang P, Niyato D, Kim DI, Han Z. A machine-learning-based auction for resource trading in fog computing. *IEEE Commun Mag*. 2020;58:82-88.
93. Kaur K, Garg S, Kaddoum G, Gagnon F, Ahmed SH. Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure. Paper presented at: Proceedings of 2019 IEEE International Conference on Communications Workshops (ICC Workshops); 2019: 1–6.
94. Jangirala S, Das AK, Vasilakos AV. Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment. *IEEE Trans Ind Inform*. 2019;16(11):7081–7093.
95. Chen C-M, Huang Y, Wang K-H, Kumari S, Wu M-E. A secure authenticated and key exchange scheme for fog computing. *Enterprise Inform Syst*. 2020;1-16.
96. Wang L, An H, Chang Z. Security enhancement on a lightweight authentication scheme with anonymity for fog computing architecture. *IEEE Access*. 2020;8:97267–97278.
97. Mahmood K, Akram W, Shafiq A, Altaf I, Lodhi MA, Islam SH. An enhanced and provably secure multi-factor authentication scheme for Internet-of-Multimedia-Things environments. *Comput Electr Eng*. 2020;88:106888.
98. Sureshkumar V, Amin R, Obaidat MS, Karthikeyan I. An enhanced mutual authentication and key establishment protocol for TMIS using chaotic map. *J Inform Secur Appl*. 2020;53:102539.
99. Kamil IA, Ogundoyin SO. On the security of privacy-preserving authentication scheme with full aggregation in vehicular ad hoc network. *Secur Privacy*. 2020;3:e104.
100. Alhaidari FA, Alqahtani EJ. Securing communication between fog computing and IoT using constrained application protocol (CoAP): A survey. *J Commun*. 2020;15(1):14–30.
101. Ren Y, Zhu F, Qi J, Wang J, Sangaiah AK. Identity management and access control based on blockchain under edge computing for the industrial internet of things. *Appl Sci*. 2019;9:2058.
102. Dsouza C, Ahn G-J, Taguinod M. Policy-driven security management for fog computing: preliminary framework and a case study. Paper presented at: Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014); 2014: 16–23.
103. Gai K, Qiu M, Liu M. Privacy-preserving access control using dynamic programming in fog computing. Paper presented at: Proceedings of 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS); 2018: 126–132.
104. Khan S, Parkinson S, Qin Y. Fog computing security: a review of current applications and security solutions. *J Cloud Comput*. 2017;6:19.
105. Kayes A, Rahayu W, Watters P, Alazab M, Dillon T, Chang E. Achieving security scalability and flexibility using fog-based context-aware access control. *Future Gener Comput Syst*. 2020;107:307-323.
106. Iqbal S, Malik AW, Rahman AU, Noor RM. Blockchain-based reputation management for task offloading in micro-level vehicular fog network. *IEEE Access*. 2020;8:52968-52980.
107. Alshehri M, Panda B. A blockchain-encryption-based approach to protect fog federations from rogue nodes. Paper presented at: Proceedings of 2019 3rd Cyber Security in Networking Conference (CSNet); 2019: 6–13.
108. Kochovski P, Gec S, Stankovski V, Bajec M, Drobintsev PD. Trust management in a blockchain based fog computing platform with trustless smart oracles. *Future Gener Comput Syst*. 2019;101:747-759.
109. Cinque M, Esposito C, Russo S. Trust management in fog/edge computing by means of blockchain technologies. Paper presented at: Proceedings of 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData); 2018: 1433–1439.
110. Al-Khafajiy M, Baker T, Asim M, et al. COMITMENT: a fog computing trust management approach. *J Parallel Distrib Comput*. 2020;137:1-16.
111. Alemneh E, Senouci S-M, Brunet P, Tegegne T. A two-way trust management system for fog computing. *Future Gener Comput Syst*. 2020;106:206-220.

112. Jayasinghe U, Lee GM, MacDermott Á, Rhee WS. TrustChain: a privacy preserving blockchain with edge computing. *Wirel Commun Mobile Comput*. 2019;2019:1-17.
113. Sadaf K, Sultana J. Intrusion detection based on autoencoder and isolation Forest in fog computing. *IEEE Access*. 2020;8:167059-167068.
114. Nath SB, Gupta H, Chakraborty S, Ghosh SK. A survey of fog computing and communication: current researches and future directions. arXiv preprint arXiv:1804.04365; 2018.
115. Naha RK, Garg S, Georgakopoulos D, et al. Fog computing: survey of trends, architectures, requirements, and research directions. *IEEE Access*. 2018;6:47980-48009.
116. Wen Z, Yang R, Garraghan P, Lin T, Xu J, Rovatsos M. Fog orchestration for internet of things services. *IEEE Internet Comput*. 2017;21:16-24.
117. Ren Y, Leng Y, Cheng Y, Wang J. Secure data storage based on blockchain and coding in edge computing. *Math Biosci Eng*. 2019;16:1874-1892.
118. Debe M, Salah K, Rehman MHU, Svetinovic D. IoT public fog nodes reputation system: a decentralized solution using Ethereum blockchain. *IEEE Access*. 2019;7:178082-178093.
119. Bhattacharya P, Tanwar S, Shah R, Ladha A. Mobile edge computing-enabled blockchain framework—a survey. Paper presented at: Proceedings of ICRIC 2019, Springer; 2020: 797–809.
120. Xiong Z, Feng S, Wang W, Niyato D, Wang P, Han Z. Cloud/fog computing resource management and pricing for blockchain networks. *IEEE Internet Things J*. 2018;6:4585-4600.
121. Liu M, Yu FR, Teng Y, Leung VC, Song M. Distributed resource allocation in blockchain-based video streaming systems with mobile edge computing. *IEEE Trans Wirel Commun*. 2018;18:695-708.
122. Debe M, Salah K, Rehman MHU, Svetinovic D. Monetization of services provided by public fog nodes using blockchain and smart contracts. *IEEE Access*. 2020;8:20118-20128.
123. Rupa C, Patan R, Al-Turjman F, Mostarda L. Enhancing the access privacy of IDaaS system using SAML protocol in fog computing. *IEEE Access*. 2020;8:168793-168801.
124. Losavio M. Fog computing, edge computing and a return to privacy and personal autonomy. *Procedia Comput Sci*. 2020;171:1750-1759.
125. Khan NS, Chishti MA. Security challenges in fog and IoT, blockchain technology and cell tree solutions: a review. *Scalable Comput*. 2020;21:515-542.
126. Ferrag MA, Shu L, Yang X, Derhab A, Maglaras L. Security and privacy for green IoT-based agriculture: review, Blockchain solutions, and challenges. *IEEE Access*. 2020;8:32031-32053.
127. Baniata H, Kertesz A. A survey on Blockchain-fog integration approaches. *IEEE Access*. 2020;8:102657-102668.
128. Rivera AV, Refaey A, Hossain EA. Blockchain framework for secure task sharing in multi-access edge computing. *IEEE Netw*. 2020;1-8.
129. Qu Y, Gao L, Luan TH, et al. Decentralized privacy using blockchain-enabled federated learning in fog computing. *IEEE Internet Things J*. 2020;7:5171-5183.
130. Li M, Zhu L, Lin X. Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. *IEEE Internet Things J*. 2019;6:4573-4584.
131. Dang TD, Hoang D. A data protection model for fog computing. Paper presented at: Proceedings of 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC); 2017: 32–38.
132. Kumar P, Zaidi N, Choudhury T. Fog computing: common security issues and proposed countermeasures. Paper presented at: Proceedings of 2016 International Conference System Modeling & Advancement in Research Trends (SMART); 2016: 311–315.
133. Lee K, Kim D, Ha D, Rajput U, Oh H. On security and privacy issues of fog computing supported Internet of Things environment. Paper presented at: Proceedings of 2015 6th International Conference on the Network of the Future (NOF); 2015: 1–3.
134. Moysiadis V, Sarigiannidis P, Moscholios I. Towards distributed data management in fog computing. *Wirel Commun Mobile Comput*. 2018;2018:1-14.
135. Madavi KB, Vijayakarthick P. Decoy technique for preserving the privacy in fog computing. *Evolutionary Computing and Mobile Sustainable Networks*. Singapore: Springer; 2020:89-94.
136. Iqbal R, Butt TA, Afzaal M, Salah K. Trust management in social internet of vehicles: factors, challenges, blockchain, and fog solutions. *Int J Distrib Sensor Netw*. 2019;15:1550147719825820.
137. Lu D, Ma J, Sun C, Wu Q, Sun Z, Xi N. Building a secure scheme for a trusted hardware sharing environment. *IEEE Access*. 2017;5:20260-20271.
138. Czerwinski SE, Zhao BY, Hodes TD, Joseph AD, Katz RH. An architecture for a secure service discovery service. Paper presented at: Proceedings of MobiCom; 1999: 24–35.
139. Park JH, Kim HJ, Sung MH, Lee DH. Public key broadcast encryption schemes with shorter transmissions. *IEEE Trans Broadcast*. 2008;54:401-411.
140. Papamanthou C, Shi E, Tamassia R. Signatures of correct computation. Paper presented at: Proceedings of Theory of Cryptography Conference; 2013: 222–242.
141. Xu L, Wu X, Zhang X. CL-PRE: a certificateless proxy re-encryption scheme for secure data sharing with public cloud. Paper presented at: Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security; 2012: 87–88.
142. Kim H-I, Hong S, Chang J-W. Hilbert curve-based cryptographic transformation scheme for spatial query processing on outsourced private data. *Data Knowl Eng*. 2016;104:32-44.
143. Gennaro R, Gentry C, Parno B. Non-interactive verifiable computing: outsourcing computation to untrusted workers. Paper presented at: Proceedings of Annual Cryptology Conference; 2010: 465–482.

144. Parno B, Howell J, Gentry C, Raykova M. Pinocchio: nearly practical verifiable computation. Paper presented at: Proceedings of 2013 IEEE Symposium on Security and Privacy; 2013: 238–252.
145. Farjana N, Roy S, Mahi MJN, Whaiduzzaman M. An identity-based encryption scheme for data security in fog computing. Paper presented at: Proceedings of International Joint Conference on Computational Intelligence; 2019: 215–226.

How to cite this article: Alzoubi YI, Osmanaj VH, Jaradat A, Al-Ahmad A. Fog computing security and privacy for the Internet of Thing applications: State-of-the-art. *Security and Privacy*. 2020;e145. https://doi.org/10.1002/spy2.145