The Security and Privacy Issues of Fog Computing

Sultan Algarni
Department of Information System, Faculty of
Computing and Information Technology
King Abdulaziz University
Jeddah, Saudi Arabia
saalgarni@kau.edu.sa

Khalid Almarhabi
Department of Computer Science, College of Computing
in Al-Qunfudah
Umm Al-Qura University
Makkah, Saudi Arabia
kamarhabi@uqu.edu.sa

Ahmed M. Alghamdi
Department of Software Engineering, College of
Computer Science and Engineering
University of Jeddah
Jeddah, Saudi Arabia
amalghamdi@uj.edu.sa

Asem Alradadi
Department of Computer Science, College of Computing
in Al-Qunfudah
Umm Al-Qura University
Makkah, Saudi Arabia
aaradadi@uqu.edu.sa

Abstract
Fog computing diversifies cloud computing by using edge devices to provide computing, data storage, communication, management, and control services. As it has a decentralised infrastructure that is capable of amalgamating with cloud computing as well as providing real-time data analysis, it is an emerging method of using multidisciplinary domains for a variety of applications; such as the IoT, Big Data, and smart cities. This present study provides an overview of the security and privacy concerns of fog computing. It also examines its fundamentals and architecture as well as the current trends, challenges, and potential methods of overcoming issues in fog computing.

Keywords:
Security, Privacy, Fog, Computing, Filter, IoT.

1. Introduction

End-to-end delays; which cause traffic and congestion and, ultimately, increases the cost of communication; can be attributed to the distance between the end user and the cloud server. In order to overcome this issue, Cisco Systems, Inc. developed fog networking, which creates a framework that allows applications to run on millions of interconnected IoT devices at the edge of the network. Fog computing supports geographical distribution, end-device mobility, real-time applications, heterogeneity, awareness, location, and low latency. Its scalable open architecture is designed to support interoperability. As such, the OpenFog consortium standardises and creates awareness of the multitude of potential uses of fog computing in various fields.

Over the years, cloud computing has provided a variety of computing services and eased the burden of managing localised data centres. However, these services are still plagued by end-to-end delays, which are not suitable for latency or time sensitive tasks. Fog computing also provides heterogeneity as edge devices; such as user devices, routers, switches, and access points; are heterogeneous. Location awareness, geographic distribution, low latency, decentralised infrastructure, cloud integration capacity, IoT application support, mobility, heterogeneity, and real-time analytics are some of the vital characteristics of fog computing infrastructure [1].

Edge and fog computing share a common purpose; to decrease latency and congestion by transferring computation tasks to edge devices. Although both these terms are often used interchangeably, they actually differ in terms of how they process data and where the controls and computations are placed [2]. Edge computing processes data locally instead of having each edge send data to the cloud for processing while fog computing enables edge devices to decide if they want to process data from multiple resources locally or send them to the cloud for processing. Edge computing also does not support many cloud-related services that are easily applied in fog networks.

Fog computing provides applications a variety of services; such as Big Data analytics, web content delivery, and gaming to name a few; due to the numerous fog nodes implementations that are available thanks to advancements in cloud technology and virtualisation.

Manuscript received April 5, 2023
Manuscript revised April 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.4.4

Three-Tier Architecture

Figure 1 depicts the three main tiers of architecture that are used in fog computing.

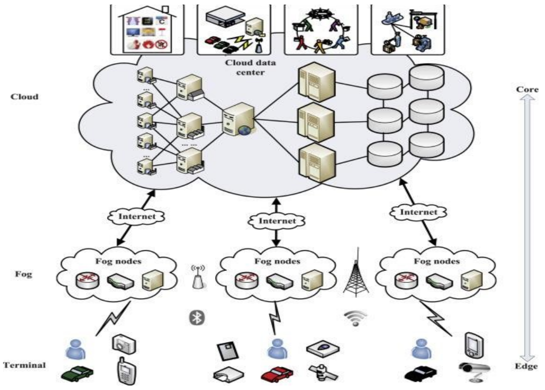

Figure 1: Fog computing architecture.[3]

Tier-1: Contains end devices or terminal nodes; such as IoT-enabled devices, smart handheld devices, and sensors to name a few.

Tier-2: Contains the main fog computation layer that consists of nodes and may contain routers, switches, set-up boxes, access points, cellular base stations, and roadside units that have limited storage and computation capabilities.

Tier-3: Contains traditional cloud infrastructure with large storage and computation capabilities.

2. Literature review

At present, fog computing is only in the development stage. As such, its privacy and security concerns have not been as extensively investigated as that of cloud computing and virtual machines. Nevertheless, this present study provides a brief overview of studies that have addressed the security and privacy concerns of fog computing.

Rauf et al. [4] examined the privacy and security concerns of the IoT and fog computing as well as outlined solutions. It provides a solid outline of fog computing characteristics and their correlation with the IoT as well as a model based on the risks of the IoT. Meanwhile, Dsouza et al. [5] examined the security concerns of fog computing and developed a policy-driven privacy management framework that was tested on a case study. The study highlights the importance of incorporating policy management as an essential security management module in fog infrastructure. However, the proposed framework does not address policy conflict detection and correction or how to avoid them. Ibrahim et al. [6] presented a mutual authentication scheme that is located at the other end of the network. It contains fog servers, that are controlled by a cloud service provider, that fog users can access using an authentication key. Fog users only need to store this single master key once in the registration phase. When new fog servers are added to the network, the cloud service provider authenticates existing fog users. This eliminates the need to register with the newly added fog servers as well as decreases overhead costs. The proposed scheme is better suited for smart cards and devices with low computation power. Although the scheme could withstand a man-in-the-middle (MitM) attack, at a specific period of the protocol, it was vulnerable to interruptions that desynchronise communications between the fog server and fog user.

Hu et al. [7] proposed a privacy and security scheme that prioritised the preservation of facial recognition as well as addressed multiple security and privacy concerns. The study used session and key agreement schemas to address security issues and data integrity preservation mechanisms to address privacy and security concerns. Meanwhile, Yi et al. [8] examined the concept of fog computing as well as its application and prevailing issues. The study found that fog computing does enhance the performance of IoT based real-time applications and improve overall service quality. Multiple studies have examined the use of data aggregation to preserve privacy, primarily on homogeneous IoT devices. One such study by Lu et al. [9] developed a technique that used single way hash chain to demonstrate the privacy preservation capabilities of data aggregation, which is more commonly called lightweight privacy-preserving data aggregation (LPDA). The sole purpose of this method was to enhance computing security and privacy. The role of cloud computing in the provision of reliable infrastructure for vehicle transportation cannot be overlooked. Basudan et al. [10] developed a privacy preserving protocol that monitors systems and provides reliable and safe vehicle transportation services to clients.

3. Security and privacy issues: A critical Analysis & Discussion

A. *Security Management and Threats*

As fog computing is the future of cloud computing, many of its privacy and security concerns are inherited from its predecessor. The following table provides an overview of some of the main cyber-attacks on fog computing infrastructure. Cyber hacks can be classified as active or passive; active attacks execute malicious code, modify messages, or create fake messages that mislead or damage communications while passive attacks obtain and collect network traffic data.

Table 1 provides a brief overview of privacy and security issues as well as solutions and limitations.

TABLE 1: PRIVACY AND SECURITY THREATS OF FOG COMPUTING.

	Attack	*Description*	*Threat*
1	Jamming	Injects bogus information to freeze communication networks.	Delays service provision, denies service provision (DoS), overuses resource etc.
2	Denial-of-service (DoS)	Sends superfluous requests to fog nodes.	Denies service, misuses resource.
3	MitM	Man-in-the-middle attack.	Invades privacy, provides misleading information.
4	Eavesdropping	Intrudes and listens to communications.	Leaks sensitive information.
5	Tampering	Maliciously drops, delays, and modifies data transmissions.	Degrades efficiency.

B. Authentication

The authentication of end-user devices, especially those connected to fog services, is a priority as it addresses the privacy and security concerns of fog computing.

Authentication is considered the first line of protection as it ensures that all communicating entities are trusted. The authentication process takes place before the fog network provides access to services. Therefore, each device has to be authenticated and prove its legitimacy to access the services offered by the fog network. This prevents malicious node attacks from occurring. Multiple studies have proposed several methods of ensuring effective authentication. These methods can be classified into three main categories; (1) identity authentication, (2) cooperative authentication, and (3) anonymous authentication [1]. Several identity authentication methods have been proposed to ensure identity confirmation on ad-hoc networks and smart grids [14], [15]. A combination of authentication methods is used when the authentication processes require multiple fog nodes in order to handle the increasing number of users and to decrease overheads. As such, they are integral to the provision of smooth and real-time services. Meanwhile, anonymous authentication enables fog nodes to authenticate end-device users without revealing their identity. Several anonymity techniques have been developed to authenticate user messages while hiding their identities; such as pseudonyms [16]. Nevertheless, the distinct and varied requirements of low latency and fog network components are significant issues that warrant consideration to reap the full benefits of these techniques for fog-assisted IoT applications. Most of the existing IoT and cloud computing authentication methods cannot be directly applied in fog computing as computation devices are typically situated at the edge of a fog network and most solutions do not consider the mobility of the end devices. Apart from that, the heterogeneous nature of fog devices further complicates network security and privacy.

C. Intrusion Detection

As fog devices are situated at different locations at the edge of a network, a proper intrusion detection system (IDS) is needed to detect and prevent malicious activity. According to [17], fog computing can function as an IDS. A fog node could work together with its neighbouring fog apex as well as nodes at the upper levels of a network to detect malicious activities that target a wide number of services. The IDS that have been developed for smart grids can also be used in fog computing. Valenzuela et al. [18] proposed detecting intrusions by monitoring power system operations. The study was able to maintain data integrity by monitoring power inputs and outputs that change in the presence of an intruder. The proposed algorithm used principal component analysis (PCA) to detect irregular and regular patterns of incoming power flows. These patterns were then examined to determine if the expected power data integrity had or had not been preserved. Paharia et al. [19] proposed a filter fog that acts as a defence mechanism by detecting a distributed denial-of-service (DDoS) attack on the cloud. This was accomplished by filtering packets according to internet protocol rules. Simulations were conducted to determine the efficiency of the proposed defence mechanism. However, as the parameters of the experiment had to be manually selected, the proposed solution does not support automated parameter adaption. It also needs to be enhanced in order to use in larger projects. An IDS is either classified a host-based system (HIDS) or a network-based system (NIDS) according to its location. A HIDS is located on a single host and monitors its characteristics and events [20] while a NIDS [21] is located at the edge of a network and monitors the network traffic of a specific network or a set of devices then analyses the network traffic to detect malicious activity. However, these IDS cannot be reliably used in a fog computing as fog computing has a distributed infrastructure [12]. Therefore, further efforts are required to overcome these issues.

As every fog node concurrently provides local services to its users as well as some real-time application services to end users, equilibrium between global and local security measures needs to be maintained. Therefore, fog nodes and end devices have to be detected autonomously and behavioural features have to be shared between the cooperating fog nodes in order to maintain the security of distributed infrastructure.

D. Access Control

Fog users and IoT devices require authorisation mechanisms that prevent unauthorised users from gaining administrative access rights and exploiting them to interfere with normal services and alter personal information. Access controls can be used to guarantee that resources and services are only granted to authorised users. Role-based (RBAC) and attribute-based (ABAC) are the most commonly used access control policies in the provision of traditional web services [1], [22].

Role-based access control (RBAC) policies enable administrators to grant users the right to access specific resources based on their roles. More specifically, users are only granted access to the resources that they require to complete their assigned tasks. Therefore, the role of a user dictates his or her level of access. This ensures that normal users cannot access sensitive information or perform advanced tasks. According to [22], RBAC policies are more scalable than discretionary and mandatory access control policies and, therefore, more appropriate for the fog-computing environment. Attribute-based access control (ABAC) policies are also widely used as they enable administrators to grant users the right to access specific resources based on their attributes or characteristics. More specifically, users are only granted access to resource or services if they fulfil pre-defined attribute-based policies.

However, although fog computing requires distributed access control policies to meet the demands of mobile users that travel from one fog node to another, it is not advisable to directly apply RBAC and ABAC policies to a fog computing due to its decentralised nature. Therefore, device access policies have to be redefined so that, when users have multiple devices connected to a single user account, the fog nodes authenticate the user account rather than the user device. This requires designing key management schemes and device management policies at fog nodes to provide users with smooth access [1].

E. Privacy

The outflow of confidential data is a concern in fog computing [23] as fog nodes are responsible for collecting, transmitting, processing, and sharing sensitive user data. Users, naturally, do not want their sensitive data leaked to third-parties.

Multiple studies have examined the privacy issues of fog computing [1], [2], [23]. The most common privacy issues of fog computing are discussed below:

1. Identity privacy

In fog computing, IoT devices submit sensitive user data to fog nodes for authentication. However, fog nodes that are adjacent to these IoT devices can also gather this sensitive user data and reveal the real identity of the user. Therefore, effective and suitable data privacy preservation methods need to be applied on fog nodes and end-user devices to prevent the leakage of user identity data.

2. Sensitive Data Segregation

It is unwise to encrypt the large amount of data that IoT devices generate without first segregating it according to sensitive and insensitive data. Therefore, there is an urgent need to develop methods of encrypting sensitive data to decrease the computation burden on IoT devices as well as the cost of communication. Furthermore, as the data that is temporarily stored on the fog node is also vulnerable to data integrity threats, methods of determining which data should be deleted and which should be permanently stored on the cloud need to be developed.

3. Location Privacy

Preserving the location privacy of a fog client is another key challenge as attackers can easily determine its location based on the fog resource utilisation patterns of a user. More specifically, user tasks are always sent to closest fog nodes for execution. Therefore, if the majority of a user's tasks are frequently sent to a specific set of fog nodes, it inadvertently reveals the location of the user. Wang et al. [24] used trusted fog nodes to create third-parties that faked positions to preserve the location privacy of users. This is because, when a fog client repeatedly uses the same set of fog nodes, it creates a pattern that cyber-attackers can exploit and breach location privacy. Yang et al. [25] proposed an enhanced fog network for location-based services that limits the ingress of end users outside the area of the protected fog nodes. The k-nearest neighbours' algorithm was used to match the locations without revealing any location information. However, although the anonymity technique can be used to conceal the location of end user on the fog network, their device locations are vulnerable to exposure if it frequently connects to the same set of fog nodes or if de-anonymisation attacks are used [1].

F. *Network Security*

Fog network security is a significant concern as these networks largely consists of wireless applications that are vulnerable to attacks; such as sniffer and jamming attacks. Therefore, several factors have to be taken into consideration when running fog networks. Firstly, network administrators have to manually configure the fog networks as well as manually segregate network management traffic from regular data traffic. As such, network administrators are overburdened by fog network configuration and data segregation tasks as the employed fog nodes are located at the edge of the Internet [27]. This increases communication costs as these enormous cloud servers, that are located all over on the edge of the network, need to be maintained and scaled. To that end, software-defined networking (SDN) can be used to ease the management and implementation processes, increase the scalability of the network, and decrease the cost of manually running the fog network.

Although SDN guarantees secure communications in fog computing, fog networking does not oversee the management of all security processes. Some of these processes are managed by IoT devices. As such, methods are required to secure communications between IoT devices [28-29]. In order to provide the most secure communications on fog networks, fog nodes-IoT device communications as well as fog node-fog node communications have to be secured [30-31]. Although newly-added IoT devices can communicate directly with fog nodes to request storage or processing services, meeting the key performance indicators (KPI) of facilitating secure communications remains a significant issue in fog networks. Therefore, inter-fog node communications should be equipped with end-to-end security measures.

Table 2 provides a brief overview of privacy and security issues as well as solutions and limitations.

TABLE 2: PRIVACY AND SECURITY ISSUES AND OPPORTUNITIES.

Issue	**Solution**	**Opportunities/Challenges**
Security management	• Policy-driven security management frameworks [5].	• Policy conflict detection and correction. • Avoiding policy conflicts altogether.
Authentication	• Identity authentication for ad hoc networks in smart grid communications [13], [14]. • Cooperative authentication for cloud and ad hoc networks [15], [16]. • Anonymous authentications; such as pseudonyms for vehicular ad hoc networks (VANETs) [17].	• Distinct fog computing features; such as end user mobility and low latency of real-time services; warrant consideration prior to solution application. • Balancing tracing end users and their true identity while maintaining anonymity.
	• Mutual authentication by sharing single master key. • Securing an authentication scheme that has low overheads but can withstand man-in-the-middle attacks [6].	• At a specific point in the protocol, attackers can interrupt communications (jamming attack) and cause asynchronous communications between the fog server and the fog user.
Access control	• Role-based access control (RBAC) policies [22]. • Attribute-based access control (ABAC) policies [22].	• RBAC is more appropriate for fog-computing. • Designing a distributed access control method that satisfies the demands of fog computing. • Defining device access policies when users have multiple devices. • Designing key management schemes; such as generation, distribution, and storage.
Intrusion detection system (IDS)	• Fog computing can function as an IDS, where a fog node works with neighbouring fog nodes in the upper levels of the network to detect malicious activity [22]. • A filter fog is a part of fog computing that filters packets according to the internet protocols table rules. It can also function as a	• A filter fog does not automatically adapt to the parameters and requires further enhancements prior to implementation in larger-scale projects. • Designing efficient decentralised identifiers (DIDs) that satisfy the demands of fog computing. • Distributed infrastructure security requires the autonomous detection of fog nodes

	defence mechanism as it can detect DDoS attacks in the cloud [19]. In a power system, an IDS could use a principal component analysis (PCA) algorithm to segregate irregular and regular patterns of incoming power flows [23]. • Host-based IDS for cloud computing [20]. • Network-based IDS for mobile phones [21].	and end devices as well the sharing of behavioural features between participating fog nodes. • Balancing local and global IDS security measures.
Privacy	• Using trusted fog nodes as third parties that fake positions to preserve location privacy [24]. • Proposed for enhanced networks in a particular location to limit the accessibility of end users according to the area covered by the fog nodes [25].	• Protection of user identity data. • Effective sensitive data segregation. • Protects user privacy and location as the cloud can identify the approximate area of a user, particularly by the physical positions of their fog nodes. • Even if the fog client uses an anonymity technique, de-anonymisation attacks can still identify users.
Network security	• Software defined networking (SDN) to ease management and implementation processes. • Proposed to increase network scalability and decrease the costs of manually running the fog network.	• SDN requires IoT devices to have some implementation for security purposes.

4. Future Trends and challenges

The ever-increasing wealth of data produced by billions of IoT devices; such as sensors, surveillance cameras, and handheld devices to name a few; as well as the need for real-time data analytics poses significant data computation, communication, storage, privacy, and security challenges that warrant careful consideration from both academia and the industry. However, the adoption of additional security measures; such as encryption and decryption; increases the computation burden of fog nodes. Therefore, it more feasible to only encrypt sensitive and critical data instead of all data. Therefore, sensitive data segregation has to be at the centre of fog computation infrastructure. Apart from that, the ability of efficient network monitoring mechanisms; such as intrusion detection systems (IDS); to detect anomalies and malicious activities warrants further investigation. It is not feasible to filter every incoming and outgoing packet as it increases the use of computational resources. Therefore, it is prudent to invest in data backup and recovery systems to ensure continuous and better-quality service. Fog computing infrastructure only stores the bare minimum amount of data required for utilisation. However, unforeseen circumstances; such as natural disasters; highlight the need for primary and secondary storage systems to quickly recover data as well as provide reliable data services.

5. Conclusion and Future Work

This present study provides an overview of the security and privacy concerns of fog computing. It also examines its fundamentals and architecture as well as critically analyses methods of overcoming privacy and security concerns. Although fog computing is relatively new, it has been readily accepted as it decreases the distance between computations and data and has lower latency than cloud computing. Fog computing is considered an adjunct network that can overcome the high latency, mobility, and location privacy issues that plague cloud computing. Despite only being in the early stages of development, fog computing provides applications a competitive advantage as well as data analytics. Future studies may further investigate one of the abovementioned challenges. This present study could also be extended to fully review the privacy and security concerns, current trends, opportunities, and issues of fog computing infrastructure.

REFERENCES

[1] J. Ni, K. Zhang, X. Lin, and X. S. Shen, “Securing Fog Computing for Internet of Things Applications: Challenges and Solutions,” IEEE Commun.Surv. Tutorials, vol. 20, no. 1, pp. 601–628, 2018.

[2] M. Mukherjee et al., “Security and Privacy in Fog Computing: Challenges,” IEEE Access, vol. 5, pp. 19293–19304, 2017.

[3] P. Hu, S. Dhelim, H. Ning, and T. Qiu, “Survey on fog computing: architecture, key technologies, applications and open issues,” J. Netw. Comput. Appl., vol. 98, no. April, pp. 27–42, 2017.

[4] S. A. Rauf Abdul, Ahmed Shaikh Riaz, “Security and privacy for IoT and Fog Computing Paradigm,” Learn. Technol. Conf. (L&T), 2018 15th IEEE, pp. 96–101, 2018.

[5] C. Dsouza, G. J. Ahn, and M. Taguinod, “Policy-driven security management for fog computing: Preliminary framework and a case study,” Proc. 2014 IEEE 15th Int. Conf. Inf. Reuse Integr. IEEE IRI 2014, pp. 16–23, 2014.

[6] M. H. Ibrahim, “Octopus: An edge-fog mutual authentication scheme,” Int. J. Netw. Secur., vol. 18, no. 6, pp. 1089–1101, 2016.

[7] P. Hu, H. Ning, T. Qiu, Y. Zhang, and X. Luo, “Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things,” IEEE Trans. Ind. Informatics, vol. 13, no. 4, pp. 1910–1920, 2017.

[8] S. Yi, Z. Qin, and Q. Li, “Security and privacy issues of fog computing A Survey,” pp. 1– 10, 2015.

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

[10] S. Basudan, X. Lin, and K. Sankaranarayanan, “A Privacy-Preserving Vehicular Crowdsensing-Based Road Surface Condition Monitoring System Using Fog Computing,” IEEE Internet Things J., vol. 4, no. 3, pp. 772–782, 2017.

[11] C. Li, Z. Qin, E. Novak, Q. Li, and S. Member, “Securing SDN Infrastructure of IoT – Fog Networks from MitM Attacks,” vol. 4, no. 5, pp. 1156–1164, 2017.

[12] V. Odelu, A. K. Das, M. Wazid, M. Conti, and S. Member, “Provably Secure Authenticated Key Agreement Scheme for Smart Grid,” vol. 9, no. 3, pp. 1900–1910, 2018.

[13] A. Wasef and X. S. Shen, “EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks,” vol. 12, no. 1, pp. 78–89, 2013.

[14] J. Zhou, X. Lin, S. Member, X. Dong, Z. Cao, and S. Member, “PSMPA: Patient Self Controllable Cooperative Authentication in Distributed m-Healthcare Cloud Computing System,” IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 6, pp. 1693–1703, 2015.

[15] X. Lin, S. Member, and X. Li, “Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks,” vol. 62, no. 7, pp. 3339–3348, 2013.

[16] R. Lu, X. Lin, and T. H. Luan, “Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs,” no. December 2017, 2012.

[17] R. Roman, J. Lopez, and M. Mambo, “Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges,” Futur. Gener. Comput. Syst., vol. 78, pp. 680– 698, 2018.

[18] J. Valenzuela, J. Wang, and N. Bissinger, “Real-Time Intrusion Detection in Power System Operations,” IEEE Trans. Power Syst., vol. 28, no. 2, pp. 1052–1062, 2013.

[19] B. Paharia, “DDoS Detection and Mitigation in cloud via FogFiter: a defence mechanism,” 2018 9th Int. Conf. Comput. Commun. Netw. Technol., pp. 1–7, 2018.

[20] J. Arshad, P. Townend, and J. Xu, “An Abstract Model for Integrated Intrusion Detection and Severity Analysis for Clouds,” pp. 1–17.

[21] A. Houmansadr, S. A. Zonouz, and R. Berthier, “A Cloud-based Intrusion Detection and Response System for Mobile Phones,” IEEE/IFIP 41st Int. Conf., 2011.

[22] P. Zhang, J. K. Liu, F. R. Yu, M. Sookhak, M. H. Au, and X. Luo, “A Survey on Access Control in Fog Computing,” no. February, pp. 144–149, 2018.

[23] N. Abubaker, L. Dervishi, and E. Ayday, “Privacy-preserving fog computing paradigm,” 2017 IEEE Conf. Commun. Netw. Secur. CNS 2017, vol. 2017–Janua, no. Spc, pp. 502– 509, 2017.

[24] T. Wang et al., “Trajectory Privacy Preservation based on a Fog Structure for Cloud Location Services,” IEEE Access, no. May, p. 1–1. 10, 2017.

[25] L. Service, “A Fine-Grained and Privacy-Preserving Query Scheme for Fog Computing Enhanced Location-Based Service,” 2017.

[26] T. Wang et al., “Trajectory Privacy Preservation based on a Fog Structure for Cloud Location Services,” IEEE Access, no. May, p. 1–1. 10, 2017.

[27] L. Service, “A Fine-Grained and Privacy-Preserving Query Scheme for Fog Computing Enhanced Location-Based Service,” 2017.

[28] A. Alrawais et al., “Fog computing for the internet of things: Security and privacy issues,” IEEE Internet Computing, vol. 21, no. 2, pp. 34–42, 2017.

[29] A. Ali et al., “Security and privacy issues in fog computing,” Fog Computing: Theory and Practice, pp. 105–137, 2020.

[30] Tayyaba, Sahrish Khan, et al. "Software-defined networks (SDNs) and Internet of Things (IoTs): A qualitative prediction for 2020." International Journal of Advanced Computer Science and Applications, vol. 7, no. 11, 2016.

[31] M. Saad, “Fog computing and its role in the internet of things: concept, security and privacy issues,” Int. J. Comput. Appl, vol. 975, no. 32, pp 0975–8887, 2018.

[32] S. El Haddouti et al., "A Secure and Trusted Fog Computing Approach based on Blockchain and Identity Federation for a Granular Access Control in IoT Environments." International Journal of Advanced Computer Science and Applications, vol. 13, no.3, 2022.