electronics

Article

Towards Secure Fog Computing: A Survey on Trust Management, Privacy, Authentication, Threats and Access Control

Abdullah Al-Noman Patwary [1], Ranesh Kumar Naha [2,*], Saurabh Garg [2], Sudheer Kumar Battula [2], Md Anwarul Kaium Patwary [3], Erfan Aghasian [2], Muhammad Bilal Amin [2], Aniket Mahanti [4,5,*] and Mingwei Gong [6,*]

[1] School of Computer Science, Nanjing University of Science and Technology, Nanjing 150001, China; alnoman_sub@hotmail.com
[2] School of Information and Communication Technology, University of Tasmania, Hobart, TAS 7001, Australia; saurabh.garg@utas.edu.au (S.G.); SudheerKumar.Battula@utas.edu.au (S.K.B.); erfan.aghasian@utas.edu.au (E.A.); bilal.amin@utas.edu.au (M.B.A.)
[3] Faculty of Engineering, Computing and Mathematics, University of Western Australia, Perth, WA 6009, Australia; MdAnwarulKaium.Patwary@uwa.edu.au
[4] School of Computer Science, University of Auckland, Auckland 1010, New Zealand
[5] Department of Computer Science, University of New Brunswick, Saint John, NB E2L 4L5, Canada
[6] Faculty of Science and Technology, Mathematics and Computing, Mount Royal University, Calgary, AB T3E 6K6, Canada
* Correspondence: raneshkumar.naha@utas.edu.au (R.K.N.); a.mahanti@auckland.ac.nz (A.M.); mgong@mtroyal.ca (M.G.)

Citation: Patwary, A.A.-N.; Naha, R.K.; Garg, S.; Battula, S.K.; Patwary, M.A.K.; Aghasian, E.; Amin, M.B.; Mahanti, A.; Gong, M. Towards Secure Fog Computing: A Survey on Trust Management, Privacy, Authentication, Threats, and Access Control. *Electronics* **2021**, *10*, 1171. https://doi.org/10.3390/electronics10101171

Academic Editor: Raed A. Abd-Alhameed

Received: 25 March 2021
Accepted: 7 May 2021
Published: 14 May 2021

Abstract: Fog computing is an emerging computing paradigm that has come into consideration for the deployment of Internet of Things (IoT) applications amongst researchers and technology industries over the last few years. Fog is highly distributed and consists of a wide number of autonomous end devices, which contribute to the processing. However, the variety of devices offered across different users are not audited. Hence, the security of Fog devices is a major concern that should come into consideration. Therefore, to provide the necessary security for Fog devices, there is a need to understand what the security concerns are with regards to Fog. All aspects of Fog security, which have not been covered by other literature works, need to be identified and aggregated. On the other hand, privacy preservation for user's data in Fog devices and application data processed in Fog devices is another concern. To provide the appropriate level of trust and privacy, there is a need to focus on authentication, threats and access control mechanisms as well as privacy protection techniques in Fog computing. In this paper, a survey along with a taxonomy is proposed, which presents an overview of existing security concerns in the context of the Fog computing paradigm. Moreover, the Blockchain-based solutions towards a secure Fog computing environment is presented and various research challenges and directions for future research are discussed.

Keywords: Fog security; IoT security; access control; fog computing; authentication; trust management; privacy; threats and attacks; auditing; blockchain

1. Introduction

The computational world has become very broad and complicated as the expectations are going beyond connecting people. We are about to approach a new era, where everything will be connected. With the swift development of technology, many individuals and organizations are starting to provide services to users with the help of their smart devices such as cell phones, home appliances, vehicles, wearable embedded devices, sensors, and actuators. The underlying work is performed by massive-scaled wireless sensor networks and realms of connected devices, which is aptly termed as the Internet of Things (IoT) [1]. IoT has achieved much attention over the last couple of years and has been enumerated as the predestination of the Internet. Gartner highlighted that the total number of connected devices by the end of 2020 [2] would be more than 20 billion devices that exist across various consumers and business organizations. Moreover, Norton security organization predicted that by 2025 there will be more than 21 billion devices [3]. As IoT continues to flourish, a huge number of sensors have been devoted to diversified devices, which are swiftly leading to an increased amount of generated data and storage requirements on a regular basis [4].

IoT application processing is dependent on the cloud. As the exponential growth of IoT devices continues to generate huge amounts of data, these IoT devices cannot be dependent on any central entity such as the cloud computing paradigm to process these huge amounts of data. The Fog computing paradigm is evolving to serve various services while simultaneously managing numerous sensors, actuators, users, processes, and connectivity by placing processing facilities closer to users. In addition, the edge devices generate data from their designated areas and link with each other or transmit to the neighboring Fog nodes for supplementary analytic and decisions. The Fog computing paradigm can solve the time-sensitive application processing limitations of the cloud as well as supporting IoT applications. Fog devices reside at the network edge to facilitate computing services close to the users and deliver services as well as applications for billions of connected devices. This helps to support real-time processing, storage and networking facilities at the edge level [5].

Naha et al. [6] defined Fog as "Fog computing is a distributed computing platform where most of the processing will be done by virtualised and non-virtualised end or edge devices. It is also associated with the cloud for non-latency-aware processing and long-term storage of useful data by residing in between users and the cloud." Bonomi et al. [5] defined Fog as "Fog computing is a highly virtualized platform that provides compute, storage, and networking services between IoT devices and traditional cloud computing data centers, typically, but not exclusively located at the edge of network." Due to the nature of edge processing, Fog computing is useful for various smart applications such as (i) Smart Transportation System, (ii) Smart Vehicle, (iii) Augmented and Virtual Reality, (iv) Smart Healthcare, (v) Smart City, and other interactive smart and time-sensitive applications [6].

Since smart devices or Fog devices are categorized as resource constraints, the Fog computing paradigm will face many challenges such as the limitations of storage, bandwidth, battery, and computation power, which leads to obstruction in the rise of IoT. To overcome the encumbrance of these limitations, the cloud computing paradigm is perceived as a talented computing archetype, which can distribute services to the edge via the cloud in terms of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions which offer applications and services with resilient resources at low costs [7]. Over the last few decades, cloud computing has obtained an immense reputation among researchers. Real-time IoT application services and information access become available anytime and anywhere via this paradigm. Cloud computing also offers diverse features to users such as ease of access to information, cost efficiency, quick deployment, backup and recovery. Although cloud computing has fulfilled most of the demands of modern technology, it may not be a suitable solution as there are still unresolved problems, whereas IoT devices and applications need to be processed swiftly. This is beyond the existing capabilities of cloud computing. Hence, security and privacy, data segregation, mobility support, low latency, location-awareness, geo-distribution and real-time applications are required for IoT applications. Privacy needs to be considered from both the user and provider perspectives. Since Fog application processing is done in the users' devices, preserving the privacy of user data is important. On the other hand, the Fog provider is the processing application in the user devices, hence, preserving the privacy of application data is equally important. While Fog computing offers a much more advantageous system as opposed to cloud-based systems, there are several security issues at hand which can cause interruptions to the way deployment is carried out using Fog computing.

Millions of users are affected because of data breaches in the past decade [8]. Since Fog computation is done in the untrusted devices, security is an important concern. In reality, due to the associated privacy and security risks for cloud-based systems, nearly 74% of Information and communications technology (ICT) executive officers have rejected adopting cloud computing [9]. In this work, the boundary of privacy is mostly authentication while the boundary of confidentiality is access control and trust management. Fog computing is not at a mature stage and continues to face new challenges due to its exclusive features. In the Fog computing environment, most devices are managed and maintained across different users. The Fog computing paradigm uses idle resources generated from user devices. These devices are not audited by any standard body, which raises security concerns in the Fog environment. On the other hand, secure and fast authentication mechanisms are required for Fog since many devices are involved in the Fog application processing. Furthermore, there is a need to be very concerned about access control since most of the application processing is carried out in the user devices. The security issues across various layers of the Fog computing environment are presented in Figure 1.

Text

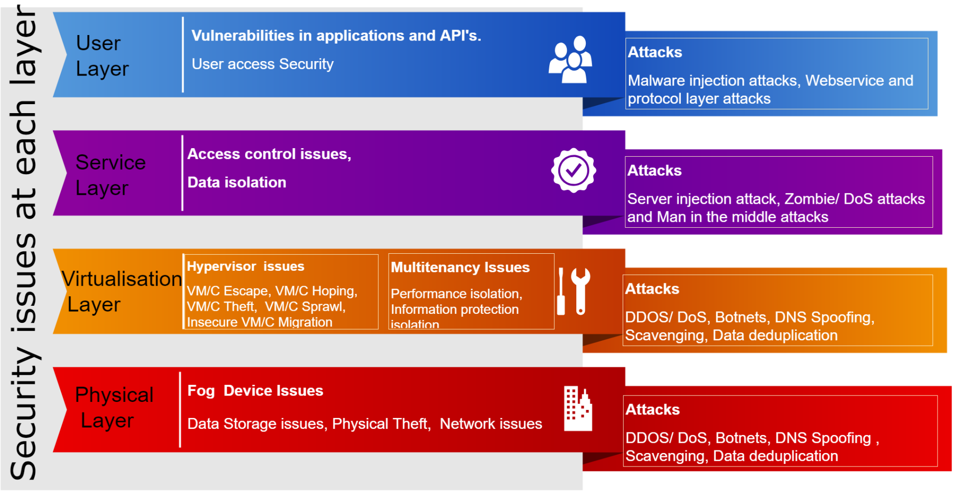
Security issues at each layer
User Layer
Vulnerabilities in applications and API's.
User access Security
Attacks
Malware injection attacks, Webservice and protocol layer attacks
Service Layer
Access control issues,
Data isolation
Attacks
Server injection attack, Zombie/ DoS attacks and Man in the middle attacks
Virtualisation Layer
Hypervisor issues
VM/C Escape, VM/C Hoping, VM/C Theft, VM/C Sprawl, Insecure VM/C Migration
Multitenancy Issues
Performance isolation, Information protection isolation
Attacks
DDOS/ DoS, Botnets, DNS Spoofing, Scavenging, Data deduplication
Physical Layer
Fog Device Issues
Data Storage issues, Physical Theft, Network issues
Attacks
DDOS/ DoS, Botnets, DNS Spoofing , Scavenging, Data deduplication

Figure 1. Security issues and attacks at each layer.

1.1. Research Motivation

Cloud computing is already recognized by its widespread deployment amongst its targeted environment. However, it faces numerous obstacles such as latency, bandwidth, Quality of Service (QoS), trust, security, privacy, trust, threats and attacks during the early stages of its deployment. Therefore, privacy and security are the key challenges for the cloud computing paradigm. In the case of Fog computing, it was inaugurated as a new computing paradigm, which has emerged over the last few years as a bridge between cloud data centers and edge devices or IoT devices. User devices and end devices are the main components for computation in the Fog environment, which is not usually audited by any security standard. Therefore, the key aim of this work is to come up with a methodical review on state-of-the-art approaches and techniques in addressing Fog computing security and privacy issues from the auditing perspective and pinpoint challenges as well as the possible direction for researchers and application developers. One of the main aims of this paper is to verify whether the centralised solutions and distributed solutions are valid in this environment or not. Hence, this study also look into the potential Blockchain technologies and how to utilize them in Fog computing.

1.2. Existing Related Surveys on Fog Computing Security

There has been a variety of techniques proposed in the literature to address the security issues of the emerging Fog computing. Most of these research papers either presented Fog security concerns or merely focused on one aspect of Fog security. Here, we have summarized and given a concise overview with regards to Fog security by combining the opinions across several of these research works.

In the context of Fog security, Yi et al. [10] briefly examined various security issues and tried to identify various challenge domains corresponding to the solutions of the Fog computing environment. Zhang et al. [11] discussed and analyzed the adhering potential security and trust issues, and explored solutions which are currently available for those issues. Khan et al. [12] explored common security gaps in Fog computing from the existing surveys. Alrawais et al. [13] investigated and discussed various privacy and security issues in Fog computing environments. Rauf et al. [14] discussed IoT, Fog and their security issues. Stojmenovic et al. [15] investigated intrusion detection and authentication techniques in Fog computing. Wang et al. [16] presented and discussed the concerns and challenges in Fog forensics and security. Recently, Roman et al. [17] explored potential threats associated with the mobile edge, mobile cloud and Fog computing. Din et al. [18] discussed the importance of trust in the future internet and presented a comprehensive overview of many suitable trust management strategies to verify the techniques are suitable for future IoT. In Hassija et al. [19], a comprehensive analysis of the IoT application threats and security-related issues are presented, and the ways to achieve the trust using different emerging technologies are also discussed. Tariq et al. [20] reviewed and presented the Fog-enabled IoT system applications security requirements and also presented the taxonomy of security threats in IoT-Fog applications. Several authors discussed the trust and privacy issues in Bigdata Fog enabled IoT systems. Bigdata are usually transferred over data transfer protocol and data transfer can be more efficient if we consider security since sensitive data are transferring over these protocols [21–24]. Tange et al. [25] identified the industrial IoT (IIoT) security requirements for efficient Fog computing-based security solutions.

In the current literature, there is a gap in the aggregation of all Fog security-related issues. None of the literary works presented a critical evaluation of all aspects of Fog security, as it has been done in this paper. Neither did they discuss Fog security issues from the auditing perspective. Different studies regarding Fog computing security and privacy did not cover the various security issues related to the Fog computing architecture and its environment. In this paper, authors will explore and explain various security concerns related to the Fog computing environment. Since Fog computing extends to the cloud system, most of the cloud computing security concerns [26] are being inherited and impact Fog computing as well. The authors have focused their attention on significant security, threats and attack issues such as trust management, privacy, authentication and access control. These security concerns are linked with Fog and have explained how these concerns could affect Fog security. In addition, it has discussed how Blockchain could mitigate some Fog related security issues. The authors have systematically focused the attention on significant security and threat-attack issues from several selected sets of papers to provide a detailed landscape in this field.

1.3. Key Contributions

This survey is intended to provide an exhaustive review across current studies by covering all related Fog security issues and challenges. This work also concentrates on constructing a review of Fog computing with a focus on the related challenges and security issues from the auditing perspective. The principal contributions of this study can be recapped as follows:

- Propose a taxonomy based on various security issues such as authentication, access control, privacy preservation, trust management, threats, attacks and security auditing, which are challenging for the Fog environment.

- Highlights and discusses various threats and attacks which might be severe in the Fog environment.
- Discuss probable challenges and future research directions in Fog computing with respect to security.
- Explains how Blockchain and auditing could help to mitigate Fog security challenges.

The rest of the paper is organized in the following manner: research methodology and evaluation are presented in Section 2. Section 3 provides an overview of Fog computing. Section 4 discusses the Fog network and data security issues. Section 5 demonstrates the proposed taxonomy on security issues in Fog computing. Section 6 discussed Blockchain technologies in Fog and presented how Blockchain technology can be utilized to improve Fog security. Sections 7 and 8 present the research challenges, future research directions, and conclusions. All abbreviations used in this paper presented in Table 1.

Table 1. List of abbreviations.

Abbreviation	Explanation	Abbreviation	Explanation
ABAC	Attribute Based Access Control	ABE	Attribute Base Encryption
AC	Access Control	AES	Advance Encryption Standard
AIS	Artificial Immune System	AP	Access Point
API	Application Programming Interface	AR	Attribute Revocation
BMA	Bad Mouthing Attack	BSA	Ballot Stuffing Attack
CCTV	Closed Circuit Television	CDC	Cloud Data Center
CIA	Confidentiality, Integrity, Authenticity	CobiT	Control Objectives of Information and related Technology
CP-ABE	Cipher-text Policy Attribute Based Encryption	CPAs	Certified Public Accountants
CSA	Cloud Security Alliance	DAC	Discretionary Access Control
dApps	Decentralized applications	DDoS	Distributed Denial of Service
DoS	Denial of Service	DSS	Data Security Standard
ECDSA	Elliptic Curve Digital Signature Algorithm	HAN	Home Area Netwrok
IA	Information Assurance	IaaS	Infrastructure as a Service
ICT	Information and Communication Technology	IDS	Intrusion Detection System
IoT	Internet of Things	IP	Internet Protocol
ISACA	Information System Audit and Control Association	$(ISC)^2$	International Information System Security Certification Consortium
ISO	International Organization for Standardization	ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library	KP-ABE	Key Policy Attribute Based Encryption
MAC	Mandatory Access Control	MCC	Mobile Cloud Computing
MEC	Mobile Edge Computing	MITM	Man-in-the-Middle
NFC	Near Field Communication	NIST	National Institute of Standards and Technology
OOA	On Off Attack	OSA	Opportunistic Service Attack
P2P	Peer to Peer	PaaS	Platform as a Service
PCI	Payment Card Industry	PIN	Personal Identification Number
PKI	Public Key Infrastructure	PoS	Proof of Stake
PoW	Proof of Work	QoS	Quality of Service
RAS	Reliability Availability, Serviceability	RBAC	Role Based Access Control
SaaS	Software as a Service	SANS	SysAdmin, Audit, Network and Security
SCADA	Supervisor and numerous and data acquisition	SCTP	Stream Control Transmission Protocol
SDN	Softwae Defined Network	SE	Secure Element
SHA	Secure Hash Algorithm	SLA	Service Level Agreement
SPA	Self Promotion Attack	SOC	Service Organization Control
STLS	Smart Traffic Light System	TEE	Trusted Execution Environment

Table 1. *Cont.*

Abbreviation	Explanation	Abbreviation	Explanation
TPA	Third Party Auditor	TPM	Trusted Platform Module
TTP	Trusted Third Party	UR	User Revocation
VHD	Virtual Honeypot Device		

2. Methodology and Evaluation

2.1. Research Questions

To fulfill the objectives of this study, this work is going to answer the following research questions:

Q1. What are the different security issues in Fog which need further investigation?
Q2. What are all the security aspects of Fog and how should they be categorized?
Q3. How did current research works address Fog security concerns? What are the other possible solutions and what security concerns need attention from the research community?

2.2. Paper Selection Approaches

To exploit the coverage of the searched literature in this work, we began by identifying the most used alternative words and synonyms in the research questionnaire. Therefore, we conducted our selection strategy based on our proposed taxonomy and Table 2 searching criteria. We first categorized the current research security issues and challenges for Fog computing into six categories: 1. Trust, 2. Privacy, 3. Authentication, 4. Access-Control, 5. Threats and Attacks, 6. Security Audit. We also looked into the security issues and solutions of other areas such as cloud computing, edge computing, and Blockchain which could suit the Fog computing environment. In order to focus on the most relevant articles based on the aims of our research, we also constructed different search strings using Boolean AND and OR operators. Then, we conducted a manual search (Fog computing security issue or privacy and security issue in Fog computing), using different search engines such as Google, Bing, and Baidu in the area of cloud computing, Fog computing security based on the search criteria in Table 2. The same approach was applied in renowned scientific research databases such as Google Scholar, ACM Digital Library, IEEE Xplore, Springer, Science Direct, and ResearchGate. Figure 2 presents our paper selection approach. We applied the Mendeley tool as well as the Google Scholar to manage citations from all extracted articles. We conducted our papers selection and evaluation based on the various criteria as shown in Table 2.

Table 2. Paper selection criteria.

Sl. No.	Criteria
01	Relevant to study of the cloud or Fog computing
02	Directly or indirectly related to cloud and Fog computing security
03	Fog computing security issues
04	Security and privacy issues in Fog computing
05	Security and trust issues in Fog computing
06	Authentication and authorization in Fog Computing
07	Authentication and access Control in Fog Computing
08	Privacy preservation in Fog computing
09	Threats and attacks issues in Fog computing
10	Security auditing standards in Fog computing

2.3. Evaluation of Results

After the initial exploration using several search strings from the sources above, we found 220 relevant papers and articles. After searching, filtering, inclusion and exclusion reviews, 127 articles were matched from the first filtration. With respect to our taxonomy, we have separated all these papers into various partitions.

Sections 3–5 are answering our first two research questions. The third research question is answered by Sections 5–7.

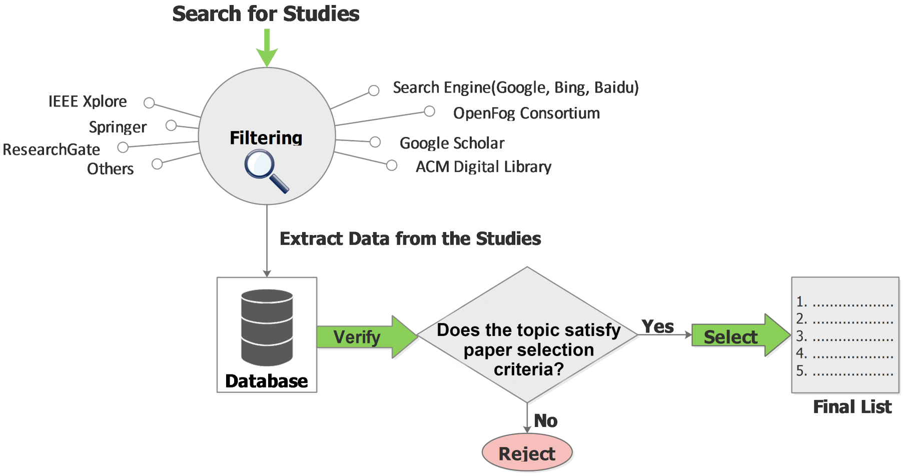

Figure 2. Paper selection process.

3. An Overview of Fog Computing

Fog computing ideally demonstrates the concept of a distributed network environment that connects two different environments and is closely linked with cloud computing and IoT. This new computing paradigm was initially and formally introduced by Cisco to extend the cloud network to the edge of the enterprise network [5]. The architecture of a Fog environment has three layers—the IoT layer, the Fog layer and the Cloud layer, as shown in Figure 3. The IoT layer consists of a massive amount of sensors and end devices. These devices include any mobile devices such as tablets or smart phones, single-board computers and micro controller units. This layer is liable for collecting and sending the data generated from devices to the Fog devices in the Fog layer. The Fog layer is the intermediary level which provides a link between the cloud and the IoT layer. The Fog devices in this layer process the received data and send the results to the cloud to store for future use. Individuals or organizations are providing Fog devices to process the applications in a Fog environment by contributing their idle resources. The providers should compensate for their offered resources based on the usage in a way that both providers and users will benefit [27]. The Cloud layer provides more available storage with no extra servers allowing the access of data anywhere, anytime.

In literature, similar Fog like technologies such as Edge Computing, Mobile Cloud Computing (MCC), Cloud Computing, Mobile Edge Computing (MEC), Cloudlet, Fog Dew Computing, Dew Computing and Micro Data Centres exist [6,12]. Ai et al. [28] provided a detail tutorial on three traditional edge related computing technologies, such as Fog, MEC and cloudlets. They also summarised standardisation, architectures, applications and principles of these technologies. However, the key difference is that it creates an enormously virtualized platform that offers diversified computation, storage and network services to its clients via unused end-device resources. With the features and characteristics of the Fog computing continuing to improve, the performances of a wide range of domains across different real-time IoT specific applications such as City: smart office, smart home, smart waste management; Electricity: smart grid; smart metering, Health: smart health care system, Transportation: smart vehicle accident prevention; traffic flow maintenance;

Smart Traffic Light System (STLS); Traffic control system, Entertainment: real-time video streaming and gaming systems are shown in Table 3.

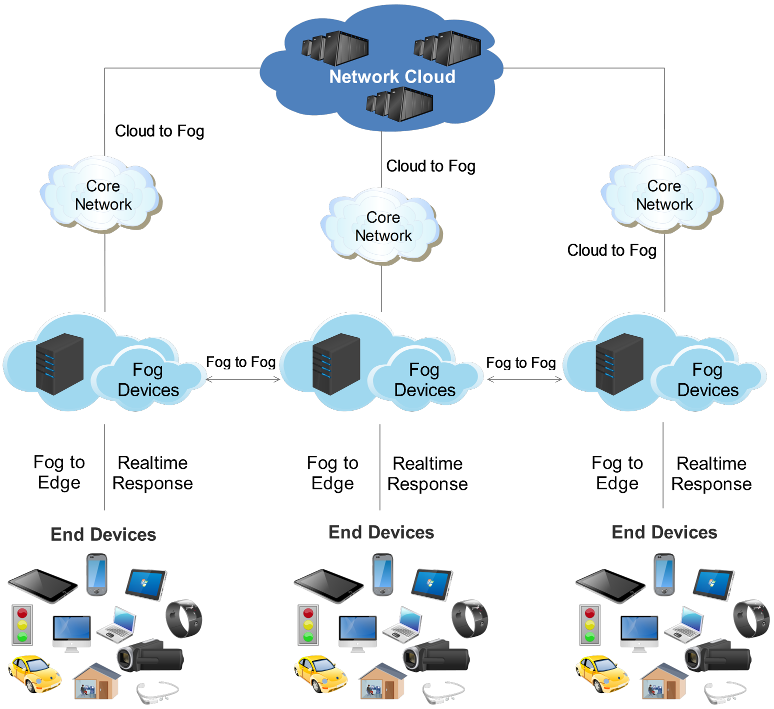

Figure 3. The architecture of Fog computing.

Table 3. Examples of Fog applications.

Application Domain	Application Service	Description
Smart city [29,30]	Smart home and Smart office	Provides automation control in home to control the electrical appliances and security and alarm systems
Electricity [31,32]	Smart grid and Smart metering	Provides monitoring and tracking service of energy hourly or day wise, etc.
Healthcare [33]	Smart health monitoring	Provides continuous monitoring of glucose, blood pressure, pulse rate, etc.
Entertainment [34]	Augment Reality	Provides the best user experience in Augmented Reality
	Real-time video streaming and gaming system Entertainment	Provides the best user experience in video streaming and gaming systems
Transportation [35,36]	Smart vehicle	Driverless vehicles
	Smart navigation	Suggests best routes and dynamic rerouting
	Road condition detection	Auto detects the condition of roads and adjusts the parameters to drive according to it
	Smart traffic lights	Reduce the traffic jams across the junctions

The features and characteristics of Fog computing are as follows [5]:

- Support Geographic Distribution
- Location Awareness
- Low Latency
- Heterogeneity
- Decentralization
- Large Scale QoS-aware IoT Application Support
- Mobility Support
- Interplay with Cloud
- Context Awareness

- Online Analytics
- Predominance of Wireless Access
- Close to the End Users
- Save Storage Space
- Higher Scalability
- Save Bandwidth
- Real-Time Interaction
- Data Security and Privacy Protection
- Low Energy Consumption

However, Fog computing has provided numerous other issues and challenges such as security and privacy. The technical distinctions between Fog and cloud computing from a security aspect are exhibited in Table 4. The OpenFog Consortium, technology giants, researchers and developers are strongly trying to mitigate these issues. Therefore, if they were able to attenuate all these issues, then it would be deemed capable to deal with the constantly increasing number of networked computational devices. This would then make the Fog platform the future of computing.

In accordance with the study of Fog computing characteristics, we have illustrated a differential table based on cloud and Fog features—Table 4. Finally, we have pointed out a few challenges that exist for the current cloud technology. Therefore, we have also illustrated a table and highlighted how Fog eliminates these challenges—Table 5.

Table 4. Technical difference between Fog and cloud in a security perspective.

Attributes	Cloud Computing	Fog Computing
Security management	Centralized	Distributed
Security concerns	General servers	Heterogeneous devices
Attack and threat level	Low	High
Security domain	Within the Internet	At the edge of the local network
Security pattern	No user defined security	User defined security
Security Audit and Analysis	Static or manual approach	Software based automated dynamic and real-time approach

Table 5. Security challenges at Fog.

Challenges	Role of Fog
Security of computing and access control	With Fog, the computation, process, storage and control of sensitive tasks are done as near as possible to the end user's device. In this distributed environment, all threats and attacks first need to be faced as Fog nodes, where Fog nodes are able to identify all illegitimate activity and can prevent any incidents before they are passed through to the system.
Security of data storage and users privacy	In Fog environments, data are originated from, or to sent to the end-user devices which are managed and preserved via secure Fog nodes. Hence, the data would be better preserved than stored in the user's device and more available than if it was maintained in remote data centers.
Security of communication and networking system	A Fog network is connected by an immense collection of Fog nodes, and it can provide uninterrupted secure communication and networking services by residing near the end user's device. Fog reduces the chances of various network and communication attacks.
Security of the resource-constrained IoT devices	A lot of IoT devices or end devices has limited resources. Hence, due to these limited resources, the IoT devices have little or no capability to defend themselves from sophisticated cyber-attacks. Fog nodes and cloud servers together can provide multi-level protection, i.e., "defense-in-depth".

Table 5. *Cont.*

Challenges	**Role of Fog**
Real-time incident response services	In Fog networks, the Fog nodes are able to provide real-time incident response services that notify the IoT system without disruption of any services.
Security challenges in the edge network	Because of the lack of available resources to end devices, Fog can manage and update security mechanisms such as authentication, access control, and trust management. Therefore, it can also protect devices that cannot protect themselves adequately.
Security credentials and software up to date	It is impractical to require that all the devices are connected several times a day to cloud for the security credentials and software to be updated. However, Fog nodes are able to manage security credentials and software updates on a large number of devices simultaneously, based on their criteria without downtime.
Monitor the security status	In the IoT environment, it is crucial to be able to notice trustworthy processes, whether the devices and systems are operating safely and securely. Many of today's hackers send false status messages that make operations appear normal. Fog provides a scheme to monitor security status in a trustworthy manner and can detect these types of attacks.

As Fog devices are much more distributed and belong to different users, security auditing is very important. In order to audit the security of Fog devices, there is a need to explore the network and data security issues related to Fog.

4. Fog Network and Data Security

Ensuring security for both network and data in Fog is a challenging task due to the vastly distributed nature of Fog computing. Most of the Fog devices are wireless, and data are processing in the user's devices. This section discussed the network and data security of Fog in detail.

4.1. Network Security

Due to the massive deployment of wireless networks in the Fog environment, ensuring security in these networks is a mandatory concern. Wireless networks are prone to attacks such as jamming, sniffers, spoofing and Man-in-the-middle (MITM). These attacks can affect the wireless network security of Fog computing, which can take place between the cloud to things continuum. In general, the users trust the network configurations and data generated by the network traffic, which is usually managed manually by a network administrator [37–39]. As Fog nodes placed at the edge of the network, therefore, would be an unmanageable task for the network administrator. In such a scenario, the Software Defined Network (SDN) will increase the scalability of the network and decrease the cost. Hence, SDN would be a preferable solution in Fog computing [10]. In Fog computing, SDN can provide features for network security, such as monitoring networks and Intrusion Detection System (IDS), as well as watching the traffic routes, which is referred to as CloudWatcher [40] and OpenFlow [41]. It also helps to isolate the traffic and manage prioritization to prevent attacks from network resource access controls and congested networks. However, CloudWatcher is unable to generate routing path and, if there many new flows in the network path, it is less efficient and performance degrades [42]. Klaedtke et al. [43] proposed a method for access control that was based on OpenFlow and for a network resource sharing system. The limitation of the proposed method is that it does not support multiple different abstractions. The authors [44], proposed an OpenWifi, which gave authentication to the guest users by letting them have access to the Fog node router in context with the security issues.

4.2. Data Security

In Fog computing, data generated by IoT or edge devices are gradually increasing with the number of IoT devices. Due to the lack of adequate resources for IoT devices, it is hard to process all the data on IoT devices [13]. IoT devices send the generated data to the nearby Fog node. After that, this node divides the generated data into several segments and forwards them to multiple Fog nodes for further processing. During this division and distribution time, the data could be altered or manipulated by attackers. Therefore, the integrity of the data must be ensured. Hence, the encryption and decryption process is not easy to implement due to associated resource constraints. In this case, light-weight encryption and decryption techniques would be a compatible solution [45]. However, user data are being outsourced as well as the user's data control, which is handed over to the Fog node. This still brings about the same security threats associated with cloud computing. In this circumstance, there might be a chance to lose or modify the outsourced data. In addition, illegitimate third parties with malicious interests might misuse the stored data. To mitigate these threats, a proposed solution is to present auditable data storage services, which are applicable for cloud computing data protection. In the context of a cloud storage system, a well-known technique is a homomorphic encryption and searchable encryption, which could be used to accumulate and ensure integrity, confidentiality, and verifiable to permit a client to investigate the data which are stored on untrusted servers [46]. Yang et al. [47] surveyed the existing research work related to auditing data storage services in the context of cloud computing. Eventually, from the circumstances above, there is still no proposed method that can meet the criteria based on a three-tier architecture for Fog computing [48]. Nonetheless, it is a challenging task to design a secure storage system, which will satisfy all requirements (dynamic processing, low-latency and high-scalability) and support smooth communication between the Fog and cloud environments. To detect network and data attacks in Fog, it is required to employ an Intrusion Detection System (IDS) across various layers.

Intrusion Detection System (IDS) is extensively used in cloud systems to identify and help protect from attacks, such as Denial of Service (DoS) attacks, insider attacks, port scanning attacks, flooding attacks on the VM (Virtual Machine), man-in-the-middle (MITM) attacks, hypervisors, as well as numerous systems [49]. It can be deployed under supervisory control and data acquisition (SCADA) [50], cloud [49] and the smart grid system [51,52]. It can also monitor and detect intrusive behavior of possible attackers, as well as analyze log files, access control (AC) policies and user access credentials. However, the above proposed methods are efficient in reducing false alarm rates, and it has less accuracy. In three-tier architecture of Fog computing, IDS must be deployed in the area of cloud, Fog, edge for monitoring, analysis of traffic, and intrusive activities of cloud servers, Fog nodes and edge devices. However, establishing security alone is not enough to provide the necessary protection against the propagation of viruses or malware from vulnerable nodes to other parts of the system. With regard to this situation, there may arise challenges such as corrective responses, alarm parallelization, false alarm controls and real-time notification [53]. A probable solution could be to deploy a perimeter IDS that coordinates different IDS in the Fog system [54]. On the contrary, while ensuring security in the Fog computing environment through IDS, several challenges may arise in terms of providing low-latency requirements [10].

4.3. Security Standards in Fog

Security standards form a vital part in maintaining protection for information systems. These standards are responsible to define the scope and security functions and features needed, as well as policies, in order to manage the information and human assets. Standards also help to evaluate the effectiveness of security measures and maintain the criteria for ongoing assessments of security. It is a necessity to consider proper security standards and commonly used security practices in the Fog computing environment in order to develop a feasible choice for the enterprise community.

IEEE 1934 [55] is a standard reference architecture for Fog to satisfy data-intensive application requirements. This architecture was proposed based on eight key attributes of the system, for example, RAS (reliability, availability, and serviceability), scalability, autonomy, openness, security, agility, hierarchy and programmability. For auditing purposes, we need to figure out the taxonomy of Fog security issues—by which, we can then identify what to audit and how to perform auditing in Fog by following recommended standards.

5. Taxonomy of Security Issues in Fog Computing

Fog is an augmentation of cloud computing that has many security issues. Naha et al. [6,56] comprehensively studied Fog computing architecture without paying much attention to Fog security. In this study, we have proposed a taxonomy, which is based on various security issues such as trust management, privacy assurance, authentication, access control, threats, attacks and vulnerabilities adhering to the Fog computing environment for auditing purposes. In the trust management section, we have discussed trust, the scope of trust, trust model and the potential attack on the trust computation area. In the privacy assurance section, we have discussed different privacy issues and privacy preservation techniques. In authentication, our observation relates to authentication domains, methods and potential attacks on the authentication processes. In the access control section, we identified the controlling area, requirements and access control methods. Finally, we summarized several threats, attacks and vulnerabilities. This taxonomy offers a better understanding of Fog security issues to the research community and enterprises. Figure 4, represents the proposed taxonomy and concise derivation of each section in the taxonomy, which will be described in the following subsections.

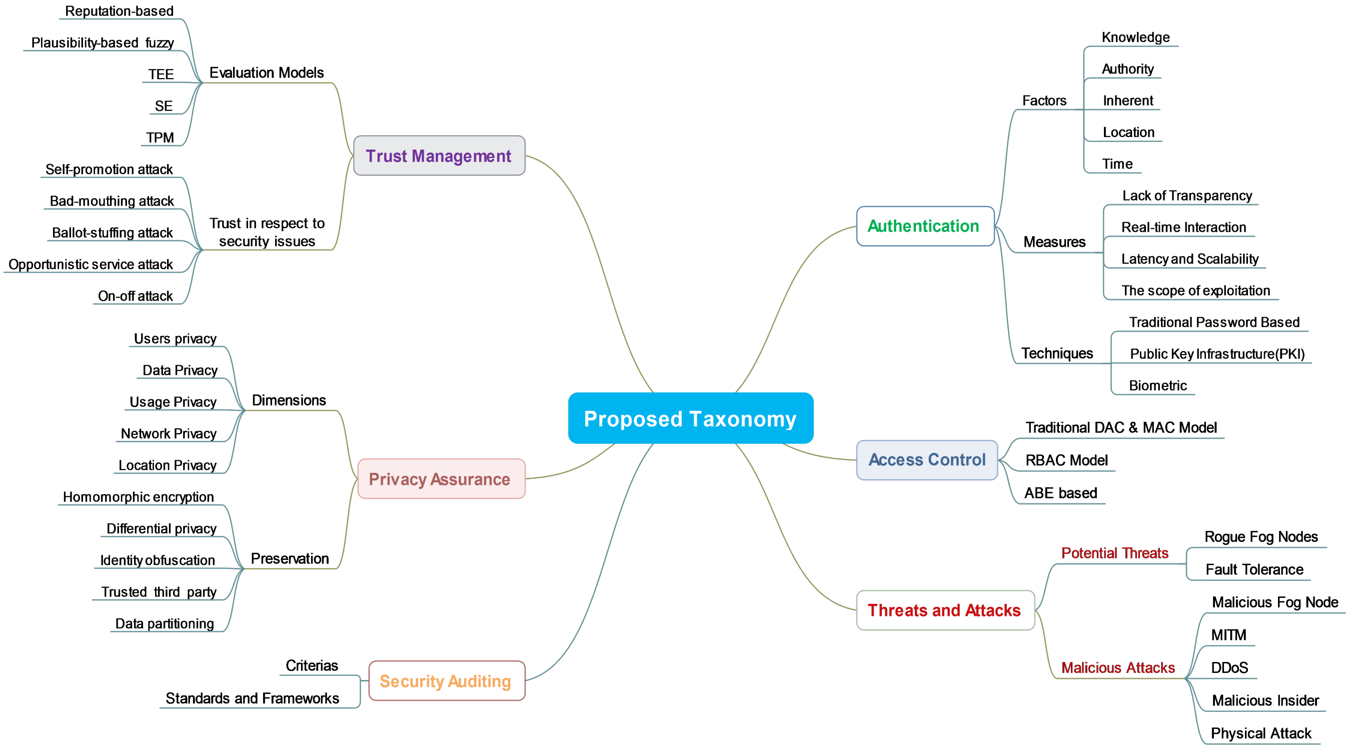

Figure 4. A taxonomy of security issues of fog computing.

5.1. Trust and Trust Management in Fog Computing

The definition of trust does vary across different fields. Trust is the level of undertaking that an entity will treat in an appeasing way [57]. Although this definition does not represent the proper trust definition according to the field of computing, it can be characterized as an “expectation that a device or system will faithfully behave in a particular manner to fulfill its intended purpose” [58]. Therefore, trust can support the devices that failed to communicate with each other and desire to establish a new connection. A Fog node might be considered safe or unsafe by relying on their trust level.

Trust management is considered in order to establish trust between entities. It is a system or mechanism that takes place between two nodes in a network to establish trust. It was first introduced by Blaze et al. [59]. They defined the problem of trust management as *"the problem of figuring based on formulated security policies and security credentials if a set of security credentials of an entity satisfies the security policies"*. Trust management examines the way of collecting and storing information to ensure the trustworthiness of an entity. It can be measured with creation, updating or revoking the trust [60].

In Fog computing, the devices are responsible for providing reliable and secured services for end-users. In this case, there must be a definite level of trust between all the devices in the Fog network. Authentication plays an important part in forming a primary set of relations between the end user's device and Fog devices in the system. As devices can always breakdown or become vulnerable to malicious attacks, authentication alone is not adequate to fix these problems. Fog computing has an aim to elevate the trustworthiness of the overall network. In the cloud computing platform, the data centers are typically owned and maintained by cloud service providers. However, in the Fog computing platform, dissimilar parties may act as service providers as diverse deployment options exist in such systems [10] such as Internet service providers, Cloud services providers and End-users. This flexibility makes obscure the required trust for Fog computing. Therefore, based on these circumstances, numerous problems arise in the Fog computing environment as follows:

- In the Fog environment, client is a node that can apply the required services as presented by the Fog device. Hence, Fog devices are retained and upheld autonomously and operated by various organizations or parties. In such a case, Fog clients are required to be more vigilant in the time of communication with Fog nodes. Generally, different possessors preserve security in different ways, and the security amongst Fog devices positioned in the same organization may also be dissimilar in context. Therefore, from a Fog client's observation, Fog nodes indicate a potentially great threat.
- From a Fog node's perspective, the client is also considered as a potential threat. These services can be comprised of various scripts or harmful ciphers with destructive consequences to the Fog node's software or hardware.
- Data are collected from the Fog clients through the Fog network, and it can be used for further work. However, after the data are collected from Fog clients, it might be corrupted or lost during the propagation process.
- Fog nodes can be deployed by anyone or any organization. Therefore, setting up a Fog node that may become a threat to the whole network may be complicated [15]. A rouge Fog device also known as a malicious Fog device can send illegal data and run over the entire network, which can have undesirable influences on the entire network performance and amplify the packet loss. This compromises Fog nodes or rouge nodes which can hamper the legitimate nodes in the Fog network.
- Usually, Fog nodes can be installed or deployed near the end-users, so that Fog nodes are easily accessible and can be tampered with spontaneously. If node hardware or software is tampered with, it will become a potential threat for the entire network. Therefore, data that are shared with the tampered Fog device can be exposed or revealed to unauthorized entities.
- Any Fog device which is compromised can be a source from which malicious objects originate that can impact the reliability of the whole Fog network.

In such scenarios, trust helps to maintain the relations built upon preceding interactions of devices or entities. Trust must play a two-way responsibility in the Fog environment [61]. First, the nodes that provide services to edge devices must be competent to authenticate the service requests to comprehend if the request is fake or genuine. Second, the edge devices that send or request data must be competent to authenticate the intentions of the node to guarantee its security. Therefore, applying the trust mechanism in the Fog environment permits Fog nodes, resource-limited IoT devices, and other Fog clients to identify the future behavior of one another. When identification of future behavior becomes probable, then Fog clients can easily choose a trusted Fog node that will provide the best services. As a sign of the problems presented in the solution of trust management, for a Fog system, there is a need to identify and detect all accidental or intentional behavior which can enable authorities to take the necessary action and rebuild the trust formation instantaneously [10]. The key factors that influence Fog computing are trust scope, trust characteristics and trust evaluation models.

Trust Scope: Guo et al. [62] demonstrated current methods of trust computation in the IoT system. They categorized the trust computing scheme into five scopes: aggregating, formation, update, propagation and trust composition. We can consider this scope of trust for the Fog computing environment as well. This segment will demonstrate each of these scopes in detail as below:

- Trust Aggregation: collect all the recommendations from others and combine them with one's own experiences in the trust computation which might be essential. Trust Aggregation elects how this is accomplished.
- Trust Formation: this defines the way to enable a combination of trust properties by trust composition. Some methods just study one property, and others reflect a mixture of some properties.
- Trust Update: it shows how often the trust values are updated. Periodical updates and Event-driven are two key methods.
- Trust Propagation: it decides on how to select a distributed or centralized process to compute and store the trust.
- Trust Composition: it defines a group of trust properties. It chooses what components have been used in the trust computation process. Social trust and service quality are the two key elements.

Characteristics of Trust in Fog Computing: This section describes the characteristics of trust in Fog computing in addition to various characteristics of trust that help to develop trust relationships related to the understanding of Fog computing much further. The authors [63] defined a few characteristics, which can be retained for the Fog environment.

- Is trust dynamic? Trust is required to be dynamic due to two reasons. First, the Fog system network topology is changing continuously as new devices join or leave concurrently on the Fog network. Then, devices in the network may deflect their behavior successively. Therefore, trust should be monitored uninterruptedly. For example, for the past year, entity A had a high trust towards entity B. However, recently, entity A found that entity B lied to entity A. Consequently, there is no trust between these two entities anymore.
- Is trust subjective? Although Fog networks are formed with a wide range of objects or devices, its security requirements vary from object to object or device to device. Thus, their trust properties are different, which is carried out more importantly over other properties. Having different types of trust policies for different objects, the trust will be subjective.
- Is trust transitive within a context? Following subjective issues, each device has a distinct security policy of its own. That is, if device A trusts device C, then device A may trust any device that device C trusts in the same context. However, this concludes that the trust might be explicit and difficult to be measured.
- Is trust asymmetric? Trust is an asymmetric relationship in nature. Being asymmetric in nature, trust is contrary to non-mutual relationships. It means that if device A trusts device B, we must not suggest that device B trusts device A.
- Is trust context-dependent? Context is significant in terms of Fog computing [64] and, at the same time, it is significant in terms of trust computing as well. Suppose, we might trust a friend to keep a secret, but not to keep our money with him. The same scenario can be applied in the Fog environment. One Fog device can be trusted to

accomplish a particular task for a client in the Fog environment, but for another task, it may not trust the same Fog device. Therefore, in this situation, trust needs to be context-dependent.

5.1.1. Trust Evaluation Models

Although Fog computing is vulnerable to any sort of illegitimate entity, it is important to ensure an effective and secure trust model that is compatible with trust computation in Fog computing.

While trust is classified amongst the imperative security requirements in Fog, there is quite a limited range of studies in the field. Most of the studies have just concentrated on the field of cloud computing.

Until now, there has been no strongly recommended trust model for Fog computing, but we can enumerate already existing trust models from IoT and cloud computing. In this section, we are going to discuss a few renowned trust models that are competent for Fog computing.

- Reputation-based: The reputation-based trust model [65] is broadly applied in peer-to-peer (P2P), e-commerce services, social media and user reviews. Occasionally, the fame of a service provider is beneficial to select amongst diverse service providers. Damiani et al. [66] demonstrated a reputation system model for P2P networks by applying a distributed polling algorithm to evaluate the consistency of the model. As this model sturdily relies on a general view, it is not appropriate in Fog computing as the nature of the end devices is dynamic. Moreover, Abhijit et al. [67] introduced a trust-based model to provide application layer security that can deal with the issues of user privacy, integrity and authentication. Hence, it will function as a trust-related safeguard in the Fog ecosystem for IoT related applications.
- Plausibility-based: Soleymani et al. [68] proposed an experienced and plausibility-based fuzzy trust model to secure a vehicular network. In a vehicular network application, it is significant to establish a trust to keep integrity and reliability. Hence, in vehicular environments, a secure trust model can handle the uncertainty and risks originating from defective information. Eventually, there are also several trusted models [10] regarding special hardware.
- Trusted execution environment (TEE): TEE is an isolated environment, which guarantees the confidentiality and integrity of code and data by executing in the secure area inside a processor.
- Secure element (SE): SE stores sensitive information securely and run the apps in a microprocessor chip to protect the data and application from malware attacks.
- Trusted platform module (TPM): TPM stores the host identification key pairs, which are used for hardware authentication inside a specialized chip. The data inside this chip cannot be accessed by software.

5.1.2. Attacks on Trust Computation Environment

In Fog computing, while Fog nodes and clients are communicating with each other, they must establish a connection with greater trust value in the Fog network. For Fog nodes and clients, the highly trusted nodes and clients will be selected and accepted frequently rather than Fog nodes and clients with lower trust. It helps to speed up the overall performance of the Fog network [62]. Malicious intruders will impersonate their nodes as highly trusted nodes, so that they can gain the possibility of compromising a network. In this segment, we are going to define several types of attacks that might occur in the Fog network:

- Self-promotion attack (SPA): in the SPA attack, the malicious Fog nodes increase their trust values to impersonate themselves as the highest trusted nodes.
- Bad-mouthing attack (BMA): this attack works by spreading fictitious information. Several malicious Fog nodes work together to provide depraved suggestions about a decent Fog node, which will damage the fame of those nodes. This is a form of a

collision attack, and it happens when numerous malicious nodes come together to spread false information.

- Ballot-stuffing attack (BSA): this attack is similar to the collusion attack, where a malicious node transfers decent suggestions regarding another wicked node to raise the fame of the malicious nodes.
- Opportunistic service attacks (OSA): after assuming that the fame has been lowered down by the Fog node, it can achieve a great service to retrieve its reputation.
- On-off attack (OOA): A malicious Fog node can provide bad and good services simultaneously to avoid being rated as a low trusted node. The OOA attacker can also behave differently with different neighbors to achieve an inconsistent trust opinion of the same node.

In accordance with the study above and based on different issues, we have illustrated a summary table on the existing related research works related to trust issues, which are shown in Table 6.

Table 6. The summary of Trust Issues in Fog environments from major survey papers.

Reference Paper	Highlights/Objectives	Achievements and Limitations
Rauf et al. [14]	• Propose a risk-based trust model for the IoT environment. • Dynamic domain adaptive security solution. • Parameters such as availability, reliability, response time, etc. used. • Direct and indirect observation also used for trust computation.	• The system can compute trust as well as compute risk levels of the system. • Layer-wise various attacks discussed. • The system will provide trustworthy information forwarding decision on the basis of trust and risk values.
Wang et al. [69]	• Performed a Fog-based hierarchical trust mechanism. • Solve resource consumption problems. • Able to monitor the trust state of the whole network. • Detect and recover data attacks and misjudgment nodes respectively.	• Reduce consumption of the energy by the network. • Ensure the state of trust for network and edge nodes. • Detect some attacks of hidden data. • Recover misjudgment nodes.
Rahman et al. [58]	• A broker based trust mechanism approach in Fog. • Deliberate the trustworthy Fog service. • Request matching algorithm has been used.	• Applies fuzzy logic for trust evaluation. • Able to perform dynamic trust operation. • Simultaneously maintained a trust relationship.
Soleymani et al. [68]	• Secure trust establishment among vehicles. • Fuzzy trust scheme based on plausibility and experience. • Demonstrated a series of security checks.	• Can deal with uncertainties and risks. • Detects faulty nodes and malicious attackers.
Yuan et al. [70]	• Reliable and lightweight trust evaluation mechanism. • More feasible against bad-mouthing attacks. • Employ fusion of Multi-source feedback information. • Used objective information entropy theory.	• Suitable for IoT edge computing on a large scale. • Facilitates low-overhead trust computing algorithms. • Trust factors are weighted manually or subjectively. • Gained computational efficiency and reliability.
Dang et al. [71]	• A data protection scheme has been used for Fog computing. • Dynamic and can handle mobility management service. • Introducing Fog-based region verification and privacy-aware role-based access control techniques.	• Able to deliberate up-to-date location services. • Efficient and feasible scheme.

5.2. Privacy in Fog Computing

Privacy is a key issue in any distributed environment. Across available literature, there are many mechanisms, which have been proposed to ensure the privacy of the data, such as encryption and hashing. However, these techniques are not suitable in the Fog because it affects the latency and time to process the application. The remaining part of the section discusses in detail the privacy assurance issues.

Privacy Assurance: Privacy assurance helps to preserve any private information, such as data, user, usage, locations, devices and network from unauthorized access [72–74]. In Fog Computing, all of the data used come from various sources like IoT devices, wireless networks as well as cloud networks. These data might be meaningful or meaningless, but we need to preserve it. Thus, appropriate privacy assurance can be treated as a substantial security issue in the Fog environment. There are also a few encounters ascends for privacy preservation, as the nodes are located adjacent to the end-users, and they can gather sensitive information [10].

5.2.1. Privacy Dimensions

Fog computing is used to work with sensitive information which is generated from several sources. For securing these types of sensitive information, privacy is one of the most significant concerns in Fog computing. There are lots of privacy issues that arise in the Fog environment. In the following section, we are going to describe Fog computing privacy issues from a different perspective:

- Users Privacy: usually, Fog computing consists of a large collection of IoT enabled devices which are connected through sensors or wireless networks. Therefore, IoT devices are used to generate sensitive data at the user level and upload it to Fog nodes for further processing. For sensitive data such as personal data, home-automated data, business data and health data, by analyzing all this sensitive information, an intruder can reveal a lot about a user's personal data and gain adequate knowledge.
- Data Privacy: as we already know, a Fog node works at the edge plane of the network, and it generally collects sensitive data that are generated by various sensing and end-user devices. Hence, Fog nodes are managed by third parties. Thus, when all the unprocessed data are being aggregated in the Fog layer, there might be a chance to compromise, alter, and miss-match the data. Under such circumstances, we need to indemnify the privacy of these data. Usually, Fog nodes send requests to the end-users to send their private data to them, in order to further process it, store it temporarily, and, finally, send data to the cloud for permanent storage [75]. Therefore, users will not have control over the data where all the access and control will be transferred to the Fog or cloud service providers. Under such circumstances, service providers or malicious insiders can manipulate the stored data. This signifies a privacy issue to the user's data.
- Usage Privacy: this privacy issue arises when a Fog client can avail of the required Fog services. For example, in a smart grid system, the reading of the smart meter reveals masses of information of a smart-house such as at the TV on and off time or when the home is vacant, which certainly brings privacy breaches for users [76].
- Network Privacy: wireless connectivity is comprehensive under the control of IoT as well as other edge devices in a Fog computing environment. It is a big matter of concern, as wireless connectivity is prone to network privacy attacks. The maintenance cost is correlated with the Fog nodes as it is positioned at the edge of the Internet, where network configurations are established manually [10]. The breach of private data is an important issue while using Fog networks. The end-users share resources which contribute to Fog processing. Due to this, information that is more sensitive is collected by the Fog network as compared to a remote cloud. To overcome these issues, an encryption scheme like HAN (Home-Area Network) might be useful.
- Location Privacy: in the Fog environment, the location privacy denotes to the protective techniques for breaches related to the client's location. While the client uploads

its responsibilities to the closest node, the uploaded node can assume that the client is contiguous and far away from other Fog processing devices. Therefore, if a client in the Fog environment uses multiple Fog application services from multiple locations, it may reveal its track directly to the Fog nodes, in order to avoid collision amongst the Fog nodes. As Fog nodes are vulnerable to potential attacks, It is easy to compromise the privacy by having the location credentials of the Fog clients. If the Fog clients are attached to an object or a person, then the location privacy is at risk. Whenever a Fog client frequently selects its closest Fog node, the node can certainly identify if the client is using the resources residing nearby.

5.2.2. Privacy Preservation

In Fog computing, it is used to collect and process user personal data, which is desirable. Thus, it is evident that a proper privacy-preserving and security mechanism is required to cope with the Fog computing environment. As we know, Fog computing consists of various devices that are connected to IoT as well as Cloud. Thus, we should apply privacy-preserving techniques between cloud and Fog to maintain data privacy because both Fog and cloud devices are resourceful and have adequate storage and power. On the contrary, IoT devices have limited resources. Thus, it's a difficult task to implement privacy-preserving techniques between the Fog and IoT devices. However, it is significant because the users of IoT devices may be concerned about their data which is sensitive [77]. Different privacy preservation techniques, methods, and schemes are proposed across many scenarios, including cloud [78], wireless network [79], smart grid [80], health-care systems [81], and online social networks [82].

- Homomorphic encryption: There is a method for privacy-preservation, which is homomorphic encryption (it is a method for operating encrypted data without decrypting it) that can be implemented to retain the privacy of transmitted data without decryption across local gateways [46].
- Differential privacy [83]: is to assure the privacy of random individual entries in the statistical data set. Although its computational overhead for such function is a big issue in Fog computing, it needs to be assiduous about the efficiency of the method.
- Identity obfuscation: There is a renowned technique called identity obfuscation technique [84], where the Fog node is able to recognize the Fog client is close by, but it cannot recognize the Fog client. As such, identity obfuscation is a technique for preserving location privacy, as it has many methods inwardly. There is an elementary method to preserve the location privacy of the Fog client, whereby this client is allowed to upload the data between diversified Fog nodes. This method is not efficient because it would waste Fog resources and enhance the latency. As we already know, the Fog client can choose its nearby Fog node to upload its data, so the Fog node is able to identify that the Fog client is residing nearby, which helps to get the Fog client's location credentials.
- Trusted third party: Wei et al. [84] demonstrated a method, where a trusted third party (TTP) generated a fraudulent ID for each Fog client. As a matter of fact, it is not necessary that the Fog client has to choose a node which is nearby, in spite of the fact that it can choose any nodes on the basis of a stipulated set of criteria such that the reputation, latency, or load balancing is not affected [85]. In this scenario, the Fog node can recognize the Fog client's rough location but cannot detect it exactly. In addition, there could be a scenario whereby a Fog client uses resources from multiple Fog nodes or the location of the client can be squeezed into a small region. As such, the location of the client must be within the coverage of several Fog nodes. According to the described scenario, the authors [86] used a method to preserve location privacy.
- Data partitioning: Another probable method could be effective for preserving user privacy by partitioning the data into multiple Fog nodes. The usage pattern is another privacy concern when clients are using Fog services. In this scenario, privacy-preservation techniques have been suggested in smart metering [80,87], but we cannot

apply these mechanisms in Fog computing directly because there is no TTP (i.e., smart meters in the smart grid) or no backup device. The Fogging device can accumulate the list of tasks for user usage. The creation of bogus tasks by the clients and uploading them to multiple nodes is one possible solution while hiding actual tasks from the bogus ones. However, this solution may not be operational as it raises the client's expense and wastes resources.

According to the discussion above and based on different criteria for privacy-preservation, it has summarized into Table 7.

Table 7. The summary of privacy issues in the Fog environment from major survey papers.

Reference Paper	Privacy Issues	Highlights/Objectives	Performances and Achievements
Wang et al. [88]	Data Privacy, Identity Privacy	• Fog based public cloud computing. • The idea of anonymity and secure aggregation techniques used. • Provide identity and data privacy. • Performed pseudonyms and homomorphic encryption techniques.	• Performed computation and communication effectively and efficiently. • Can save the communication bandwidth.
Yang et al. [89]	Location privacy, Location verification	• Introduced secure positioning protocols by preserving the location privacy. • Position based advanced cryptographic protocols have been introduced, which preserve the location privacy.	• Privacy is gained without utilizing additional computational overhead. • The system is as efficient and quite practical in practice.
Kumar et al. [90]	Location Privacy, Data Privacy	• Data confidentiality and location privacy are focused on. • Discussed how to access user data. • The misconceptions about the rights of users were discussed. • The concept of a decoy method with some incorporation for data and location privacy.	• The concept of decoy method for data and location privacy has been discussed. • Different attackers and their interest in a user's private data were also discussed.
Liu et al. [91]	Location privacy, Identity privacy	• Fog based vehicular ad-hoc network (VANET) • Secure and intelligent traffic light control system using Fog. • Location Based Encryption (LBE) and Cryptographic computational Diffie–Hellman puzzle has been used.	• Reduce the computation and communication overhead. • Traffic light may efficiently verify the authenticity of the vehicles. • Fog device friendly and is able to defend the Denial-of-Service (DoS) attack.
Lu et al. [92]	Device Privacy, Data Privacy	• Employing lightweight privacy-preserving data aggregation method, for Fog and IoT systems. • The homomorphic Paillier encryption, Chinese Remainder Theorem, and one-way hash chain techniques have been applied.	• Performed efficiently and aggregated hybrid IoT devices data into one. • Supported fault-tolerance (FT). • Prevents a false data injection attack by filtering injected false data at the network edge level. • Computation and communication costs are very low.
Qin et al. [79]	User's privacy, Network Privacy, Data Privacy	• Preservation of the privacy of the end user's over a radio network. • Techniques used include commitment schemes along with zero-knowledge proof and random-checking monitoring to preserve the privacy of the end user and to protect the data flow over the radio network.	• Provides user's privacy, data security, and network privacy in the Fog computing environment • Efficiency and accuracy is unpredictable in the Fog computing environment.

5.3. *Authentication in Fog Computing*

Authentication helps to verify a user's identity by verifying if a user's credentials match with the information in a database via the authentication server. In the context of Fog computing, authentication ensures and confirms an end user's identity. This helps ensure that only legitimate end users can have access to the Fog nodes who have met all the requirements to be authenticated as an end-user. Authentication is one of the five pillars of Information Assurance (IA) [93]. In Fog computing, authentication of the end user's devices permitted to Fog services is a significant requirement in the Fog network. In order to obtain the Fog services from the Fog infrastructure, an end user's device must be authenticated to be a part of the Fog processing infrastructure by authenticating itself. Authentication is also essential to defend against the access of unauthorized entities. Figure 5 shows the authentication issues in Fog computing. As can be seen, six major issues exist for authentication in Fog computing. If a user faces any of the issues depicted in the figure, his/her privacy could be endangered.

With the higher number of internet-enabled devices, authentication is getting more and more vital to permit secure communication for IoT applications and home automation [94,95]. Almost any object (entity) may be addressable and be capable of exchanging information over the network. Thus, it is significant to comprehend that each device or application can be potentially an intrusion point in the environment. Thus, it is mandatory to ensure a strong authentication mechanism for each device or application in the Fog network system.

Although Fog computing eliminates many difficulties compared to primitive cloud computing, it also provides excellent services such as mobility, geo-distribution, heterogeneity, real-time processing, etc. Similar to Cloud computing, Fog computing also faces new security challenges. Due to heterogeneity and interaction of third party authorities in the Fog computing system, it leads to an increase in the scope of security breaches. In such a case, there might occur various renowned attacks (e.g., data loss, account traffic hijacking, man-in-the-middle attack, denial of service attack, malicious insider attack, etc). Therefore, it is a significant issue to think about secure Fog networks by ensuring the security mechanism in every stage. In that case, authentication plays a key role in protecting the Fog network. Therefore, ensuring proper authentication mechanisms would be a suitable solution to prevent such attacks. As Fog computing is used to provide various services with low latency and cooperate with the edge devices as well as cloud systems, by providing any authentication mechanism, there might be a chance to raise critical issues such as latency, scalability, and efficiency, which needs to be handled according to the demands of the Fog computing environment.

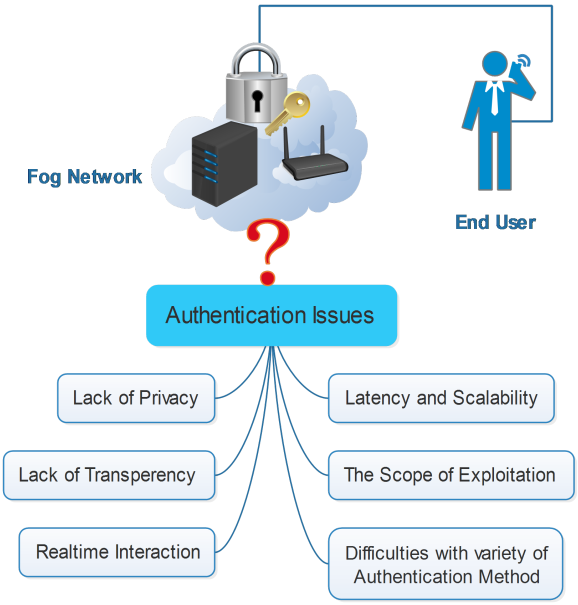

Figure 5. Authentication issues arise in Fog Computing.

5.3.1. Authentication Factors in Fog Computing

The authentication factor refers to attributes or data that can be considered to authenticate user access to a system. A legacy security system has a few authentication factors such as the knowledge factor, which is something users know, the possession factor which is something a user has and the inherent factor which is something the user is. In recent years, other authentication factors have been added—location factor and time factor, along with the old authentication factor, which is as follows:

- Knowledge Factor: is any credentials that consist of information that the user holds, such as Username, Password, Personal Identification Number (PIN) and answers to the secret questions [96].
- Authority Factor: would be any credentials that the user can own and carry with them, such as hardware devices like a mobile phone or a security token.
- Inherent Factor: is generally based on biometric identification (fingerprints, facial, retina).
- Location Factor: itself cannot usually refer to authentication, but it can be used with other factors. For example, a legitimate user normally can access a system from the home or office in any organization's home country. An attacker will try to access that system from a remote geographical location. With the help of a location factor, the system can prevent illegitimate user authentication into a system or network.
- Time factor: similar to the location factor, the time factor can be used as a supplement with other factors. It can be used together with the location factor. For example, an authorized user can have access to a system in a specific time period in an organization's home country. On the other hand, an illegitimate user tries to access that system from a remote geographical location of another country. Therefore, the authentication would be rejected based on the time and location factor.

5.3.2. Authentication Measures in Fog Computing

- Lack of Transparency: The existence of SLA between a Fog or cloud service and end-users is a vital issue in order to establish trust. Although many SLAs have clearly defined the privacy over the user's sensitive data, users are unable to trust them in how the data are being governed. Hence, the SLA verification gets limited when the service is being directly used in the Fog layer by the end users and a small organization, which should be monitored by a licensed third-party through SLA verification. There might be a lack of transparency that permits the users to monitor their own data in the Fog or cloud system.
- Real-time Interaction: Fog nodes and end-users interact with a huge number of devices simultaneously. Different services need different authentication mechanisms where, if the process takes a huge amount of time to authenticate, it would be a challenging task with respect to real-time interaction.
- Latency and Scalability: In accordance with the rapid growth of user devices and services, it is an ambitious task to guarantee the efficiency of the authentication mechanism. Whenever the latency of the authentication process is high and incompatible with the service, scalability is a big concern.
- The scope of Exploitation: In the context of Fog or cloud system, there is a diversified authentication mechanism for various services. These authentication methods can be compromised or exploited by the attacker and the attacker can appear to have gained administrative level access due to the deficiency in the authentication mechanism. There might be a chance to breach the security of data, devices as well as the Fog network system.

5.3.3. Authentication Techniques in the Fog Environment

Generally, users need to use various services simultaneously. Therefore, they need to use different authentication methods for different services where the performance of the authentication methods is different in the context of latency, efficiency and scalability. On the other hand, the user faces lots of difficulties to maintain access credentials for multiple services. Authentication is the most significant issue for the security and privacy of Fog computing. An authentication mechanism that is not secure might cause harm for the cloud, Fog and end user's devices, which is one of the main security concerns for Fog computing [97] as well. Therefore, different authentication techniques have been proposed for elevating security mechanisms in the Fog or cloud computing, but each authentication method has come up with its own dominance and limitations. In this subsection, a few traditional authentication techniques and their limitations as well as drawbacks according to the Fog environment have been described. We also described a few proposed solutions which meet with the Fog computing criteria.

- Password Based Authentication: In password authentication, the user must first give a password for every service, and the system administrator must keep track of all usernames and passwords on the server. Password Authentication is performed by accepting a key and password for allowing a user into local and remote systems. Password authentication can be categorized depending on its strength as weak authentication, stronger authentication and inconvenient authentication [98]. Therefore, password-based authentication has several applications, and it is deployed in cloud computing [99–101], but it will face numerous drawbacks and limitations when it is considered for Fog computing:
  - It takes an extensive computation to process. It is challenging due to the limited end device resources.
  - In the Fog network, end-users frequently communicate with various Fog nodes from different Fog environments. Therefore, it is inappropriate to keep a password for each Fog node. In addition, it is not a good concept to set the most used password for each Fog node.
  - Usually, a password does not provide high security because of numerous attacks [102], for example, vulnerability to offline dictionary attacks.
- PKI Based Authentication: public key infrastructure (PKI) based authentication creates and upholds a reliable networking environment by offering certificate and key management services that permit encryption and digital signature abilities between applications all in a way that is transparent and easy to use. PKI offers confidentiality, integrity, authenticity (CIA) and non-repudiation of the exchanged messages. In [15], the authors described security issues and focused on authentication issues at various levels of the Fog computing environment. Therefore, the traditional PKI-based authentication scheme is not effective in the context of Fog computing due to the poor scalability because, in a large environment like the Fog environment, the PKI-based technique can be troublesome, and it will work very slowly in terms of the distributed computing environment. The user of Fog (IoT device) is mostly resource-constrained, where they do not have much memory and computing power to accomplish the cryptographic operation [10]. In addition, the allocation of public keys can be weighty due to the enormous scale of Fog nodes and end-users. Another drawback is that, if the private keys cannot be well preserved, the security will be ruined.

On the other hand, the Diffie–Hellman [103] key exchange based authentication scheme is not compatible with the Fog environment due to its slow and extensive computations.

Balfanz et al. [104] demonstrated a user-friendly, cheap and secure method to resolve the authentication issue for wireless networks based on pre-authentication of the location-limited channel. Likewise, Nearfield communication (NFC) is used in Cloudlet to simplify the authentication process [105]. Ibrahim et el. [106] proposed a secure mutual authentication method for the Fog environment that allows authenticating any Fog user with the Fog nodes mutually in the Fog network. The authors [107] proposed a method based on the multi-Tier authentication scheme to Secure Login in Fog Computing. The authors [108] mentioned that the Advance Encryption Standard (AES) is a compatible encryption algorithm for the Fog computing environment as it needs low hardware resources and fewer computations. The authors [97] demonstrated that the end-user devices can initiate spoofing attacks and are prone to data tampering which can be preserved with the aid of PKI, Diffie–Hellman key exchange, monitoring by Intrusion detection techniques, and, finally, the authors' advice that the chances of such attacks can be prevented by deploying a secure authentication mechanism between the Fog platform and the end-users.

- Biometric Authentication: is a technique of user identity verification based on various biological inputs through scanning or analysis of some parts of the body. Biometric scanners scanning a user's physical biometric characteristics such as fingerprint, voice recognition, iris scan, face recognition, etc. Generally, biometric authentication takes place to manage access to digital or physical resources. Biometric authentication is an upcoming technology and is already rapidly deployed in mobile computing as well as cloud computing using fingerprint authentication, face authentication, keystroke-based authentication or touch-based authentication [10]. However, in the context of distributed Fog computing environments, biometric-based authentication techniques have a lot of limitations and drawbacks. Comparatively, it takes a huge amount of execution time, and its security level remains constrained when high-level security is very much required [106]. Therefore, considering biometric-based authentication for Fog computing is still a research issue [10].

In accordance with the study above, and based on different issues of authentication, this has been summarized in Table 8.

Table 8. The summary of Authentication issues in Fog environments from major survey papers.

Reference Paper	Highlights/Objectives	Performances and Achievements
Ibrahim et al. [106]	• An efficient and secure mutual authentication method for the cloud-Fog-edge system architecture. • Required to store one master secret key. • Does not need extra overheads such as re-initialization or the re-registration process.	• Required to perform fewer hash invocations and symmetric encryptions/decryptions. • In addition, simple countermeasures have been introduced. • Suitable and can be deployed efficiently to the Fog user's smart device/card.
Wazid et al. [109]	• Fog devices' security can be ensured through key management and authentication schemes. • Performed efficient and lightweight operations. • Bitwise exclusive-OR (XOR) and One-way cryptographic hash function techniques have been considered. • Demonstrated using formal security verification.	• Performed low computation and communication overheads. • Ensure high security compared to another existing method.
Dsouza et al. [110]	• Introduce a policy-based resources management in the Fog network. • Support interoperability and secure collaboration among various resources in the Fog system.	• Server authentication, device authentication, data migration authentication and instance authentication have been observed for the secured Fog computing environment.
Alharbi et al. [111]	• Ensure secure communications among the various IoT devices. • Performed challenge–response authentication technique.	• Performed effectively and efficiently. • It can achieve very low response latency. • Protects the IoT system from DDoS attacks.
Amor et al. [112]	• Introduces anonymous mutual-authentication amongst the Fog users and Fog servers. • Cryptographic and mathematical have been performed to establish the session key.	• Can accomplish effectively and efficiently and improve the security and privacy in the Fog network. • Can defend against various attacks such as man-in-the-middle attack, eavesdropping and reply attacks.
Hu et al. [113]	• Highlighted privacy-preservation and security methods for Fog based image processing applications. • Data encryption, the authentication and session key agreement, and data integrity checking such methods have been proposed.	• Can perform effectively and solve the issues of integrity, availability and confidentiality. • Increases little computation and communication overhead.
Ha et al. [114]	• An efficient and elliptic cryptographic based mutual-authentication technique for IoT based resource constrained devices. • Uses implicit certificate and key management for secure communication and mutual authentication.	• Achieved less execution time. • Suitable for resource constrained devices.
Gope et al. [115]	• Deliberated two-factor lightweight and privacy-preserving authentication method for resource constrained IoT devices. • Provide a resilient way of authentication.	• Very efficient computational capacity. • Can perform robustly against malicious attacks.

5.4. Access Control in Fog

Access control is a method of restrictive access to a system or to a physical or virtual resource. In computing, it is defined as a process by which users are granted privileges for retrieving information from the system, information or resources. In access control systems, individuals must have legitimate credentials before access can be granted to them. The process of access control is shown in Figure 6. As can be seen from the figure, if a user fails to comply with the enforced access control policy, his/her request accessing the resource database would be denied. Otherwise, the user would be granted access to use the resources in the environment.

By deploying Access Control in the Fog network system, it would be possible to conserve a user's privacy and assure that both the user and system security maintain trust between the Fog, cloud service providers and users. The authors in [116] highlighted a few Access Control (AC) problems in the area of Fog computing and classified these problems into the following types:

- The users should be authenticated by the Fog or cloud system if they wanted to use the services such as storage or computation, where several strategies must be used to control access for both services and data as well.
- Security management is difficult to control, given the number of requirements.
- The cloud and Fog system needs mutual access control.
- Access control mechanism helps to prevent attacks such as side-channel in Virtual machines (VMs).
- Resources are very limited to both the user and Fog devices, respectively.

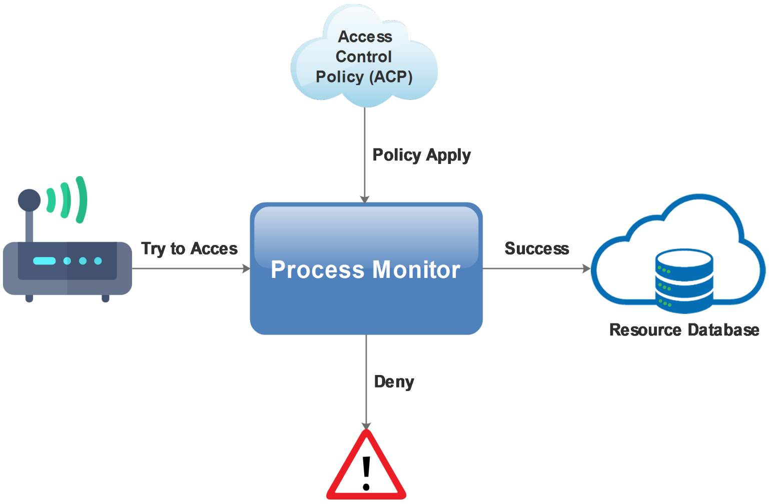

Figure 6. A process of access control (AC).

5.4.1. Access Control Models

Access control is the best method to achieve preservation within the networks, devices, and systems. While it helps user's admittance into the system, access control also supports efficient data protection from various kinds of adversaries. Conventionally, access control models (ACM) are categorized [117] into the following forms:

- Discretionary access control (DAC): the object's owner elects access permissions to others. These models are typically used in traditional applications of cloud and suffer from significant overhead costs in managing the multi-user environment. The second category abstract requires the need of resource-user mapping. Thus, compared to DAC models, this model is more flexible for distributed systems.
- Mandatory access control (MAC): The MAC models use multi-level security systems. Here, the administrator of the system decides who has access to the system. In a multi-level MAC model, both objects and subjects are recognized with a security

level classification (i.e., top secret, secret, classified and unclassified). The nature of Fog/cloud computing is outsourced, hence there is a need to focus on access control models which can be effectively applied in this computing environment.

- Role Based Model (RBAC): Designing a model for access control is a rudimentary challenge on a large scale to secure mobile distributed applications and database systems as there is a need to provide dynamic privileges for checking systems in the environment. RBAC is a fined grain model that offers more benefits compared to previous models [118], such as regulating the user's access to applications and resources by identifying the activities and the roles of users in the system [119]. RBAC authorizes the subject based on their responsibilities and roles of individual users within the Fog-cloud computing environment [116,117,120,121]. Roles may vary from the subject (user) to subject (user). That means, in this model, the responsibility of a subject is more vital than the subject itself [120,122].
  Limitations and Drawbacks of the RBAC Model:
  - The RBAC model had been developed for allocating user permissions statically.
  - It does not consider contextual information (e.g., location, time, device constraints) and dynamic/random behavior of users.
  - It cannot cope with dynamic segregation of duties.
  - It is coarse-grained. If you have a role called administrator, then you would assign the administrator role permission to "View employee record" (i.e., it has permissions to see all the records of employed) which denotes as an expansion of the role.
  - It ignores meta-data of resources e.g., employee owners' records.
  - It is hard to manage and maintain within a large administrative domain.
  - Access reviews are painful, error-prone and lengthy.
  - Permissions accompanying each role change or deletion is based on the change of the role.

  Therefore, RBAC in Fog should ensure quicker granting access permissions and minimize the above-mentioned limitations and drawbacks.
- Attribute-based Access Control (ABAC): This model is one of the latest methods of managing authorization. It is a talented alternative to conventional access control techniques and has attracted consideration from both academia and the industry. Comparatively, recent developments of ABAC still leave several unknown difficulties such as delegation, administration, auditability and scalability.
- Attribute Based Encryption (ABE): This model is an encryption-based Access Control model and best suits access control problems in the Fog-cloud environment. The Attribute-Based Encryption (ABE) [123] method categorized into two types. Firstly, the encryption is based on the key policy, which is known as key policy attribute-based encryption (KP-ABE) [124] and, secondly, the encryption is based on Cipher-text policy, which is known as Cipher-text policy Attribute-based Encryption (CP-ABE) [125].
  This model can preserve data privacy and enable data owners to define a desirable set of policies directly [116].
  - Key Policy Attribute-Based Encryption (KP-ABE): Goyal et al. [124] proposed KP-ABE in the year 2006, based on the classical ABE model and uses one of many communications. This technique achieves fine-grained access control with higher elasticity to control individuals compared to the traditional scheme [118].
  - Cipher-Text Policy Attribute-Based Encryption (CP-ABE): CP-ABE [125] was introduced as another alternative form of ABE. CP-ABE can provide fine-grained and reliable access control for cloud storage environments that is not trustworthy. Users can access data only if their attributes match the access policies associated with the data. CP-ABE works in a reverse compared to KP-ABE. In this, the key generated is attribute user set, where the ciphertext is fixed by access policy [118]. However, CP-ABE has two main drawbacks [126]: policies are not explained using standard languages, and it cannot support non-monotonic policies.

Architecture of ABE: The architecture of the ABE method is categorized as centralized and decentralized as well as hierarchical [121].

- Centralized: In a centralized architecture, the keys will be served by a central authority centre for the users.
- Decentralized: In a decentralized architecture, the information will be shared by multi-authorized authorities based on the policies of various organizations.
- Hierarchical: In hierarchical architecture, the scalability and flexibility are enhanced and assist the features of one-to-many encryption for the users.

Revocation Types of ABE: The revocation types are categorized into two types: attribute revocation and user revocation.

- Attribute Revocation (AR): by using the AR mechanism, the attribute from the user's attributes list will be removed by the revocation controller unit.
- User Revocation (UR): by using the UR mechanism, a user restricts data access via the revocation controller unit.

Revocation Method: There are various revocation methods to revoke a user and attributes using the ABE method. Proxy re-encryption, time re-keying, an update key, lazy revocation and Linear Secret Sharing Schemes (LSSS) matrix are the primary revocation methods.

Revocation Issue: Deploying the ABE method in cloud storage systems to control data access brings about forward and backward revocation issues.

Revocation Controller: The revocation controller is someone who is designated to execute the user or the attribute revocation method. In general, the owner of data revokes the attributes or the user, but the data owner can confer the revocation duties to the server or the authorized entity.

Limitations and Drawbacks of the ABE Based Model: As we mentioned before, Fog computing extends cloud and the functionalities as well as the requirements of Fog computing, which are unique. Thus, the access control structure of cloud computing is not able to directly meet the requirements of Fog computing. However, researchers [97,127] recommended that ABE techniques suit Fog computing, but still needs to improve and meet some criteria such as fine-grained, cryptographically enforces, latency and policy management problems, which need to be re-thought and considered for further research. Although the end device or user device in Fog computing are constrained resources, there is no need for deploying data encryption-decryption and access control mechanisms at the user level because the Fog devices are resourceful and used close to the end-user devices. Based on these circumstances, outsourcing access control methods would be the more appropriate solution for Fog computing. On the other hand, as we know already, Fog computing consists of a dynamic environment. Therefore, the ABE-based access control should support creating, updating and revoking the user attributes and access structures with the management of the access policies according to the dynamic behavior of Fog computing [116].

5.4.2. Issues and Requirements for Access Control in Fog Computing

To establish and ensure secure and efficient access control, policies must ensure confidentiality, accountability and integrity. However, due to the nature of the Fog computing environment, one should consider a few things to build a secure and strong Access Control (AC) [116,128], which are as follows:

- Computation and Communication Latency: it indicates how long it takes for a single packet to travel from one designated node to another node. The sender considers sometimes latency as the time for sending a packet and getting an acknowledgement from the sender, where the round-trip time is taken as latency. As Fog computing is renowned for its faster accessibility, we need to ensure low-latency for providing smooth services to the end users. We can indemnify the low-latency during processing time so that the access decision can transpire within a reasonable time.

- Efficiency: efficiency is also correlated to latency. In Fog computing, there are two types of devices e.g., resource rich (Smart Power Grid, Smart City, Smart Transportation System, E-Health, etc.) and resource constrained (mobile phone, smart-watch, smart-glass, etc.). The proper implementation of Access Control System in Fog computing is still a challenging issue because of its low efficiency. If the low efficiency occurs in a continuous manner, it can result in undesirable latency, which can affect the other parts of the network.
- Generality: with the distinction of hardware and software, we need to generalize all the systems and services of Fog computing.
- Data Aggregation: in Fog computing, users are geo-spatially distributed where Fog devices are used to collect data from user devices. Therefore, it is necessary to accumulate all Fog devices closer to the end users for reducing latency. The data generated from user devices will be meaningful or meaningless, but it should be handled intelligently and evenly [129]. During the whole aggregation process, authority changes are a critical issue for data access control.
- Privacy Desecration: as it is possible to exchange data from one domain to another domain, administration of the decentralized architecture of Fog computing leads us to protect the privacy of data through Fog access control. Thus, it becomes a critical requirement to protect the user's data privacy.
- Network Availability: in Fog computing, network availability must be defined in such a way that, when there is an issue of network unavailability, access control can also deliver the predefined level of functionality.
- Context Awareness: when multiple operations like capturing, transferring, processing and storing are running, access control decisions should be managed competently to support all the contextual information (e.g., health condition, weather condition, temperature, time, traffic condition, etc.) [81].
- Scalability: scalability is to facilitate the services according to the needs of the end users. In access control, scalability will provide the services that can grow or shrink according to the end user's level of capacity. For scalability, the CloudPolice [130] have proposed a distributed solution, in which hypervisors are responsible for the communication with each other to install access control states.
- Resource Restriction/Constraints: in Fog computing, the user or the edge resources are limited. Thus, it becomes tough to implement access control for Fog computing.
- Policy Management: it is an integral part of Fog computing architecture. Thus, the access control model needs to be capable to support creating, invoking, releasing, and deleting policy management. Dsouza et al. [110] developed a policy-driven security management framework, which is capable of supporting secure communication and resource sharing in the Fog environment.
- Accountability: in Fog computing, it is significant to keep track of the suspicious activities of intruders. This track keeping should be handled intuitively across the administrative domains.

5.4.3. Access Control Domains

In the Fog computing arena, for defining the access control system, the contextual domains are 1. Fog to Edge, 2. Fog to Fog, and 3. Fog to Cloud. Edge devices are communicating and sending data to Fog devices during the time that the Fog device uses to process all the data in such a way, so that, if the necessity arises, it can send all the processed data to the nearest Fog devices. When the issues for storing data arise permanently, Fog devices are able to send all the data to a data warehouse or cloud storage. Therefore, process/store identity and access data in the Fog/cloud computing by first ensuring secure Fog/cloud access control. Ensuring access control in the cloud/Fog environment is a crucial technique to enhance the user security—in this scenario, end-user/data privacy, faster communication and computation, network and communication security, etc. Such requirements shall be applied for the above-mentioned domains to enable the proper access control system. For this, all the primordial access control models are being advanced accordingly.

In accordance with the above study, and based on a different access control method, it has been summarized into Table 9.

Table 9. The summary of Access Control Issues in the Fog environment across major survey papers.

Reference Paper	Highlights/Objectives	Performances and Achievements
Zhang et al. [131]	• A promising CP-ABE based access control for a Fog computing environment. • Outsourcing and attribute update capability. • Encryption and decryption are outsourced.	• Perform heavy computation operations of encryption and decryption within a very small and constant time period. • Less computation cost and efficient attribute update. • Suitable for resource-constrained IoT devices.
Vohra et al. [118]	• Fog based decentralized Multi-Authority attribute based data access control. • Also based on the CP-ABE method. • Performs fast offline–online encryption and the partial decryption method.	• Secure and performs effectively and efficiently. • Ensures secure communication from untrusted devices on the Fog network. • Achieved authentication, access control, verifiability and confidentiality.
Popa et al. [130]	• A distributed multi-tenancy approach access control. • Access control only suits in infrastructure levels—as physical hosts and hypervisors.	• Simpler, scalable and robust techniques. • Requires extra processing power.
Fan et al. [132]	• CP-ABE based multi-authority data access control scheme in Fog-cloud computing systems. • Outsourced encryption and decryption computations.	• User and attribute revocation can be performed efficiently. • Secure and highly efficient scheme.
Xiao et al. [133]	• A hybrid and fine-grained access control solution. • Most of the decryption process can be outsourced. • Secure and suitable in the Fog computing environment. • Perfectly applicable for resource-constrained IoT devices and applications.	• Efficiency of data access is improved. • Key management cost is greatly reduced. • The limitation and drawbacks of this method are that they can be applied only in centralized architecture.
Yu et al. [134]	• Fine-grained access control and privacy is provided for Fog computing. • Can also guarantee security across side channel attacks. • leakage-resilient functional encryptions framework have been developed.	• Highly secured and fine-grained access control. • Fully secure leakage-resilient functional encryption schemes have been presented.
Zaghdoudi et al. [135]	• Access control mechanisms proposed for Fog computing and ad-hoc MCC. • Focused on measuring the system overhead with different metrics. • A different size of networks, different hash function, and a variable responsible nodes percentage such metrics considered.	• A generic access control solution with features that are robust and scalable. • Take overhead with the increase of nodes in the network.

5.5. Malicious Attacks and Threats in Fog Computing

Due to the isolated deployment of Fog nodes in some places, it fails to protect countermeasures and surveillances. As a result, it is very easy for intruders or malicious attackers to compromise the Fog networks through several malicious attacks [136]. For example, a malicious user can compromise a Fog node with its own generated trust values, smart meter, smart grid, traffic system or spoof IP addresses [15] to ruin sensitive information. In this segment, we will give an overview of these potential threats and attack issues.

5.5.1. Potential Threats

- Rogue Fog Node: Rouge Fog node is a one type of Fog device in the Fog computing environment that presents itself as a legitimate node and persuades end users to connect with it [137]. It may happen in such a scenario, when a Fog administrator instantiates an insider attack, to identify the rogue Fog node or a legitimate Fog node. Stojmenovic et al. [15] have proven that the data can be tampered by a man-in-the-middle attack, with updated or collected the data either in the Fog layer or cloud layer. There is also the possibility to launch additional attacks. Thus, in the context of privacy and security, the presence of a rogue Fog node will be a potential threat in the Fog environment. It is not easy to detect a rogue Fog node in Fog computing for various reasons. One of the main reasons is the diversified trust computing mechanism that brings about perplexed trust situations. On the other hand, we know that Fog computing is dynamic in nature and consists of numerous devices which leads to creating, deleting and revoking simultaneously. Therefore, for these various instances, it is difficult to manage the blacklisted nodes. The authors Han et al. [138,139] have demonstrated measurement-based models which permit a client to escape connecting to rouge access points (AP). Ma et al. [140] introduced a framework to identify the existence of rogue APs in wireless networks. Detecting a rogue Fog node in an IoT network is cumbersome because of the network complexity across different scenarios [13]. Nevertheless, by using trust measurement-based models in the IoT network, it helps to detect rogue nodes. Although this method is not adequate, it can be considered for limited security protection.

- Fault Tolerance: Fog computing is an emerging distributed computing platform that consists of a huge collection of numerous devices that is widely geo-distributed and heterogeneous. Therefore, there might be a high chance of failure of devices, as compared to cloud computing. Fog computing is dynamic in nature, whereby the Fog nodes or IoT devices connect or disconnect to a Fog layer over and over. Because of this behavior, there might be a chance to bring about unexpected faults and failures in the Fog environment. Therefore, in these circumstances, the Fog computing platform should provide all the necessary services without interruption if there is a failure occurring in individual Fog devices, networks, applications and services platforms [141]. Because Fog applications should be capable of instantly turning to other available nodes via some inbuilt mechanism if the services in an area become unusual. To mitigate these issues, standards should be applied. Stream Control Transmission Protocol (SCTP) is such example that can deal with such events and packet reliability in wireless sensor networks [142].

  In general, fault tolerance ensures the availability of devices or applications in the event of a failure to provide uninterrupted services. Nevertheless, on the basis of what service is being used, fault tolerance will change according to one's role and management privileges. In the cloud computing environment, fault tolerance is handled by applying three techniques—proactive, reactive and adaptive [143].

  Proactive fault tolerance policies refer to an escape rescue from faulty components by anticipating and replacing the failed components before it takes place.

  Reactive fault tolerance policies refer to the decrease in the influence of faulty components when the failure occurs in adaptive fault tolerance, where the procedure is carried out according to the situation automatically.

  There are numerous fault tolerance techniques which are often used in computing [144–146] such as Replication, Job Migration, checkpoint, self-healing, Rescue workflow, Safety-bag checks, Task Resubmission, Software Rejuvenation, Masking, Preemptive Migration and Resource Co-allocation. Nevertheless, in this paper, fault tolerance is mostly discussed based on the cloud computing environment as Fog computing is a new computing paradigm. In recent research works [147–151], the context of cloud computing in such a scenario was discussed. Therefore, fault tolerance in Fog computing is still a research task. In order to provide a reliable and robust Fog computing environment, failure handling of services should be effectively considered.

5.5.2. Malicious Attacks

Fog computing comprises various IoT or edge devices and collects the data from these devices by accomplishing latency conscious processes. Identifying malicious nodes is a complex task in the Fog environment [152]. As we know, Fog computing is a miniature of cloud computing, as such, almost all types of malicious attacks, which affected a cloud environment can also affect Fog computing. For example, DDoS (Distributed Denial of Service), MITM, sniffing, side channel attacks, DoS (Denial of Service), malware injection and authentication attacks are a few of them. Therefore, in these circumstances, without an appropriate prevention mechanism, it can severely damage the competency of the Fog system or network. In this portion, we are going to expose a few malicious attacks which might occur frequently and affect the Fog environment.

- Attacks from malicious Fog nodes and edge devices: As Fog nodes are compromised easily by any malicious attacker, it is a very serious and potential threat for the Fog network environment. The authors [45] mention various unique security threats in their research, which might occur in the IoT and Fog environments. For delivering services to the users, the received data from the IoT devices will be processed by Fog nodes. If some Fog nodes are compromised by any intruders, it is a problematic task to ensure the security of the data. One possible solution would be by establishing trust between Fog nodes themselves. In this case, an authentication mechanism is mandatory for ensuring secure, trusted communication. Therefore, Fog nodes cannot manage each other, so they need to trust only the cloud for authenticity. Sequentially, after being authenticated by the cloud, it should be placed in a Fog environment to process heavy data. However, they are not able to give a suitable solution for this attack. Li et al. [153] carried out research and presented a solution.

  It is vital to identify malicious Fog devices in Fog computing. Due to the lack of resource and edge devices, it is difficult to deploy proper authorization mechanisms between Fog nodes and edge devices. Thus, it is hard to prevent all attacks completely because of granting a few privileges and processing of the data. Sohal et al. [154] tried to solve the problem by using intrusion detection and virtual honeypot devices by introducing a Markov chain based framework.
- Man-in-the-Middle (MITM) Attack: All data traffic passing through is protected through secure transmission channels between Fog nodes and edge devices in Fog computing. During this communication process, a user's data will be snooped or impersonated by an external malicious attacker prior to performing a global concealing process in the Fog node. Such a scenario correlates with the MITM attack. In an MITM attack, a perpetrator secretly relays and manipulates the data during communication between two parties. Hence, MITM is a potential attack method which can be used as a typical attack in Fog computing. In Fog computing, an attacker can carry out sniffing or disrupt the packets between Fog devices. As mentioned earlier, in Fog computing, all devices are resource-constrained. By having this problem, it becomes a challenging task to deploy secure communication protocols and encryption–decryption methods amongst Fog nodes and IoT devices [97]. Stojmenovic et al. [97] proposed an authentication method that can possibly avoid MITM attack. To mitigate MITM attacks, the anomaly detection is hardly applicable in Fog computing because these methods were being used in traditional cloud computing. Therefore, to mitigate MITM attacks in Fog computing, a compatible solution still offers a challenge, which can be considered for further research.
- Reply Attack: Fog computing makes use of a distributed network of embedded sensors and actuators that communicate with the physical world. The replay attack technique is very straightforward. To inject an exogenous control input without being detected, the attacker takes over the sensors, observes and records their readings for a period of time, and then repeats the process when carrying out his attack. This is a very normal and natural assault for an attacker who is unaware of the system's complexities but is aware that the system will be in a steady state for the duration of the attack [155].
- False Data Injection: False data injection attacks are distinct from normal cyber attacks that attempt to compromise data availability because they concentrate on data integrity/manipulation. While the idea of a false data injection attack originated in smart grid applications [156], it can be applied to any other Internet-connected

environment, such as Fog computing. If the intruder can figure out what the current configuration is, he or she can insert malicious measurements that will deceive the state calculation process without being detected by any of the existing techniques for detecting bad measurements. False data injection attacks impose a great amount of challenges on the attackers. First, the attackers must understand the target's current configuration, especially the system's topology. Due to scheduled regular equipment maintenance and unplanned incidents such as unforeseen equipment outages, this system configuration changes frequently. Normally, only control centers have access to such knowledge. Given the sensitivity of control centers, physical access to them is strictly regulated and secured. As a result, obtaining such configuration information to perform these attacks is not trivial for attackers [157].

- Denial of Service Attack (DoS): In a Denial of Service (DoS) attack, the attacker prevents secondary networks from efficiently or accessing the spectrum band at all. DoS attacks can start with a single malicious node or multiple malicious nodes acting independently. DoS attack can effectively disrupt the usual operation of the Fog computing environment. The malicious nodes are dispersed around the available spectrum bands at random. Until acting, each malicious node observes its current spectrum band and sends a beacon to the malicious central entity. The malicious central agency returns to the malicious nodes a consolidated image of the secondary networks' spectrum occupancy. If the malicious nodes want to turn, they can explore other unknown spectrum bands in order to maximize the attack gain [158]. Further investigation is required to secure Fog computing environments from DoS attacks.
- Distributed Denial of Service Attack (DDoS): In the modern epoch, Distributed Denial of Service or (DDoS) is one of the most renowned and challenging threats for cyberspace and other online services. As Fog nodes are made up of limited resources, it is troublesome to manage a huge amount of requests simultaneously. When a malicious attacker or intruder initiates a bunch of inappropriate service requests towards the targeted device, or tries to spoof multiple devices concurrently using the IP addresses, the Fog node will be occupied for a longer span of time. Therefore, all the legitimate services of Fog devices will be inaccessible for legitimate users—as opposed to Fog nodes, which go on to compromise themselves and get used for generating DDoS attacks. A different plane of the Fog environment can be affected by this kind of attack. Recently, malicious attackers have been able to compromise online home-automated smart devices to execute a DDoS attack against popular online websites such as Twitter, Paypal and Reddit. After these attacks, all of these websites were severely affected. Hackers have been trying to use internet-connected home automated equipment, such as Closed Circuit Television (CCTV) cameras, printers, refrigerator, etc. to perform DDoS attacks on popular websites, such as Twitter, Spotify, PayPal, SoundCloud and Reddit [159,160]. In accordance with the Fog network system, all smart objects that are connected consist of more computational power, and they have the ability to perform various tasks concurrently. As compared to traditional DDoS attacks, in Fog computing, various Fog devices apply DDoS attacks which will become much more severe. Therefore, it is not possible to mitigate a DDoS attack completely in the Fog computing environment. At the present moment, we can only monitor them. Under these circumstances, current DDoS issues may need new thinking and further research which will classify DDoS issues much more precisely in the context of the Fog computing environment.
- Malicious Insider Data Theft Attack: According to the three-plane architecture of Fog computing, cloud computing is correlated to Fog computing. Hence, we should be conscious of all the malicious attacks which occur in cloud computing frequently. One severe attack in cloud computing could be a malicious insider attack for data theft purposes. On common terms, the end users will have to trust the cloud service provider despite being aware of this threat. It happens due to the deficiency of cloud service provider's authentication, authorization, and audit controls, which

allows attacks to spread out across the cloud system. In this regard, a few incidents have occurred which compromised corporate data, for example, Twitter's personal hacking [161,162] as well as the account hacking incident of U.S. President Barack Obama [163], which was exposed as a malicious intent to steal a user's credentials. The authors Rocha et al. [164] revealed that a malicious insider can gain access to the user's data easily in a cloud computing system. The attackers carry out their attacks which are generated from within cloud service providers. Therefore, the end user is not able to detect unauthorized access. There are diversified approaches which would be useful in order to secure data from faulty implementation, misconfigured service bugs in code by using encryption and access control to restrict them as well as to give protection from sophisticated attacks [165]. Another solution could be user behavior profiling, where the system keeps track of the amount of user data access and the duration of data use. Hence, the system can identify anomalous activities of end users, which can be used to detect malicious attacks. In this case, the authors Stolfo et al. [166] have proposed a new approach to assure the security of cloud computing by using user behavior profiling and decoy technology. There might still be a few issues [61] which arise on how to deploy the decoy in Fog networks and how to develop an on-demand decoy information to reduce the portion of stolen data from being lost.

- Physical Attacks: In traditional data centers, physical security is being provided by on site security staff. On the other hand, by applying complex measures e.g., card punch, thumb impression, and retina scanning, physical access control can be deployed much more convincingly. Thus, these issues are related to certification and audits to derive the necessary physical security measures which are required to meet the set standards. Basically, Fog nodes are widely distributed across various environments. Due to this point, it is impossible to implement traditional physical security measures in the Fog computing environment. For example, physical security measures can be applicable to place the edge box at the top of the streetlight's pole, which should be hidden from eye level as well as being surrounded with a fire-resistant coating to keep it safe from vandalism. There is a lower probability of physical attacks at the software level which enables the scope of theoretical attacks.

In accordance with the study above, and based on different issues regarding threats and attacks related to the Fog, it can be summarized in Table 10. The focus of this study is to address auditing issues to secure the Fog computing environment. The following section discusses security auditing issues in Fog.

Table 10. The summary of threats and attacks issues in Fog environments from major survey papers

Reference Paper	Highlights/Objectives	Achievements and Limitations
Stojmenovic et al. [97]	• Managed to conduct a MITM attack. • This attack is very stealthy and dangerous.	• An authentication scheme has been proposed to mitigate such attacks. • Encrypted communication method may not work always to protect from this kind of attacks. • On the other hand, complex encryption and decryption techniques are not always compatible due to resource limitation.
Wang et al. [167]	• Fog based storage technology to mitigate the cyber threat in the cloud. • Data stored separately in the Fog server as well as in the cloud storage.	• Ensure the integrity, confidentiality, and availability of data. • Attackers unable to get any information about data by using data fragments. • Can protect the confidentiality of the user's data better than traditional ways. • This approach is safe and feasible for cloud storage.
Homayoun et al. [168]	• Fully automated and Fog node ransomware detection techniques for the Fog layer. • Deep learning techniques can be applied.	• Detect and identify the ransomware within a very short time of execution of an application.

Table 10. *Cont.*

Reference Paper	Highlights/Objectives	Achievements and Limitations
Han et al. [138,139]	• The presence of fake Fog nodes or rogue Fog nodes is a serious threat to the Fog network.	• A practical, timing based method for the end users to avoid connecting to rogue Access Points.
Stolfo et al. [166]	• Decoy technology and user behavior profiling have been used for disguised detection.	• Mitigating insider data theft attacks. • Securing personal and business data.
Sandhu et al. [152]	• A framework which uses three technologies such as an IDS, a Markov model, and a virtual honeypot device (VHD). • Edge device classification depends on level of damage and frequency of attacks.	• Proposed system is able to identify malicious Fog nodes in Fog. • Successfully identify the malicious devices and also decreases IDS false alarm rates.
Hosseinpour et al. [169]	• Lightweight and distributed IDS system based on an Artificial Immune System (AIS). • Three-layered structure that includes the Fog, cloud and edge layers.	• Smart data approach has been used to build a lightweight and efficient IDS for the Fog platform. • Can detect silent attacks such as botnet attacks in IoT-based systems.
Alharbi et al. [170]	• Security system based on Fog that defends the IoT system from malware attacks. • Proposed challenge–response authentication to protect IoT systems further from DDoS attacks.	• Able to filter malicious attacks effectively while response latency is very low and network bandwidth consumption is low.

5.6. Security Auditing in Fog

In the traditional computing environment, it is often essential for technology experts to perform various security tasks such as examining security configurations, regulating potential vulnerabilities and constructing new security configurations with respect to every organization's own security policies [171]. On the other hand, it is getting much harder when new computing paradigms like Fog computing are considered. Traditionally, organizations can enforce their access control policies according to its employee's roles and responsibilities, which is actually a challenging task for most administrators. Therefore, this challenge will be much more difficult in a Fog computing environment where security policies can be deployed across a huge number of devices residing at the edges of the Fog network. Security administrators need adequate knowledge to accomplish multifarious administrative tasks. Therefore, in this section, we discuss the various issues of Fog computing security auditing.

Importance of auditing in Fog security

Fog computing is the latest computing paradigm in the modern computing world. The life cycle of security is shown in Figure 7. The very first step of the life-cycle is to identify. In this phase, it can be understood what needs to be protected. Next is the assessment phase. In the third stage, risk analysis indicates the existence of possible risks related to the potential issue. The audit determines the correctness of the analysed risks. At the last two stages, the protective actions and the resolution are placed in the cycle to remediate any possible security incident for the Fog user or the end device. The risk level from user to system is shown in Figure 8. As shown, the risk level can be considered from two sides, user-side and system side, respectively. Based on these two sides, Fog users may be exposed to different level of risks in an environment in which they can participate. In spite of its substantial growth of Fog, there still remains lots of barriers for much more widespread adopting of Fog computing services due to security issues. Lack of auditability is a primary security concern in the Fog computing environment.

In the following section, we discuss several key aspects of Fog security auditing.

Traditional auditing methods in Fog security

Fog computing has come up with numerous features and it is strongly dynamic in nature. All communication processes, data transmission, data analysis, user authentication and resource management can be automated and dynamic with real-time operation. According to the nature of Fog computing, its security auditing process would be dynamic and within a real-time process. However, the existing traditional security auditing standards and the manner of auditing are very manual, where a technology specialist team or group of individuals perform their auditing processes using their traditional auditing standards. The traditional approach is only applicable within a small environment or with limited resource. However, it is a problematic approach because this approach provides only limited support to make an evaluation and the quality of the audit heavily depends on auditor's knowledge and experience. In such cases, several difficulties can be anticipated.

1. Security auditing expert's knowledge can be inadequate or inappropriate.
2. To correctly configure out the Fog system's security, many organizations or users find it cumbersome because of the extensive expenditure to hire security professionals.

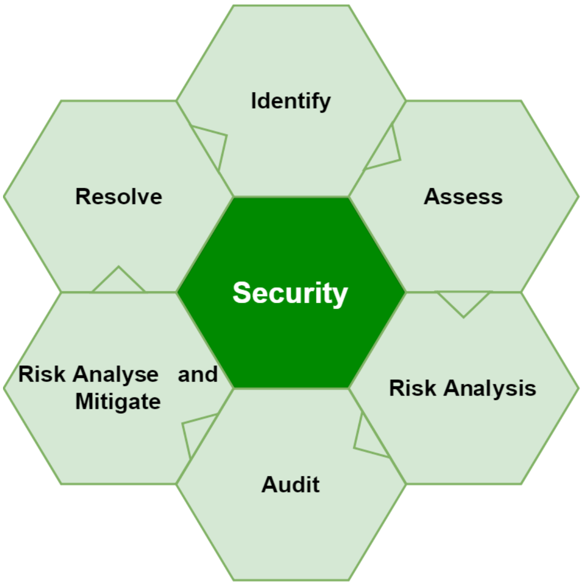

Figure 7. Life cycle of Security.

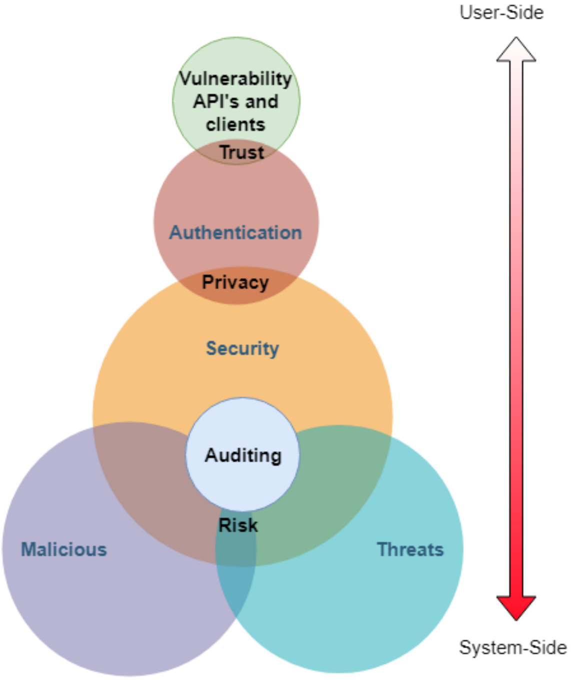

Figure 8. Risk level from user to system.

Therefore, a software-based automated auditing system, which can perform on a real-time basis, would be the best suited solution for the Fog computing environment.

Mitigating security breaches and privacy with auditing in Fog security

Fog computing provides several security and privacy concerns for the cloud and traditional computing as well as its own security flaws. In the Fog environment, there are extensive amounts of devices, applications and resources which exist simultaneously and communicate with each other within a geographically distributed environment. Therefore, there exists a big opportunity for rapid security and privacy vulnerabilities. There are many security demonstrations that exist for traditional or cloud computing, but these demonstrations are not predominantly well-suited with respect to Fog computing. With the help of Fog security configurations auditing, we can mitigate these security issues as well as privacy-related issues for Fog nodes or Fog computing devices. Auditing security measures are a way of examining for infringement which potentially exposes the vulnerability of a system.

Thus, when one focuses on Fog based auditing, there is a need to see these concerns as the core to the overall approach:

- To minimize or mitigate risks introduced by Fog;
- To identify new threats and defend them;
- To evaluate the efficiency of security controls related to Fog;
- To continuously improve policies, processes, procedures and tools;
- To perform knowledge based dynamic periodic auditing processes.

5.6.1. Criteria and Current Solutions

This section discusses current literature that presents various criteria and solutions for security auditing. Parkinson et al. [172] proposed a novel Graph-based Security Anomaly Detection (Graph- BAD) approach that translates the object-based security configurations into a graph model. They proposed a technique which was developed to identify vulnerabilities autonomously and perform security auditing of large systems without the need for expert knowledge. Similar work has been done by Kumar et al. [173] focusing on network risk evaluation. Bleikertz et al. [174] proposed an algorithm to audit the configuration network's security and the policies of the multi-tier cloud architecture using Amazon's EC2 public cloud.

Wang et al. [175] proposed an auditing system for data storage security by implementing a privacy-preserving auditing protocol using homomorphic authentication and random mask techniques for the preservation of privacy against Third Party Auditor (TPA). It can audit without requiring to have the knowledge of the user's data contents. A batch auditing protocol was also introduced in this study, which can be used to complete multiple auditing tasks across different users at the same time via TPA. A public auditing system contains four algorithms such as KeyGen, SigGen, GenProof, and VerifyProof. KeyGen is run by the user to set up the scheme, and to generate the required verification metadata, of which Siggen is used. GenProof is executed by the Cloud Server to provide proof of the data storage's correctness. VerifyProof is run by TPA to audit the proof from Cloud Server.

Wang et al. [176] recommended a set of characteristics for public auditing systems with the aim to focus on data storage security in the public cloud. Shah et al. [177] proposed several public auditing protocols which helped not only to check data integrity from the service provider, but also fraudulent customers. Privacy preservation is achieved through zero-knowledge, and by concealing data contents from the auditor. Yang et al. [47] reviewed several current works on data storage security auditing service in cloud computing. Mohammed et al. [178] proposed a secure protocol by a TPA that ensures the data integrity in Fog computing. The main drawback of this method is that the user has to depend on a third party. There should be trust between the TPA and user.

5.6.2. Existing Security Auditing Standards and Frameworks

Implementing security governance and auditing frameworks may support organizations to conduct and manage their own security risk levels. Various organizations or technology groups have created renowned frameworks and recommendations based on the traditional computing or cloud computing standards [179,180] which are globally used.

The most popular and renowned security audit standards and frameworks are presented in the following:

- Service Organization Control (SOC) 2: which is considered for auditing outsourced services sponsored by the American Institute of CPAs.
- ISO 27000 standards—ISO 27001:2005 and ISO 27002:2005 : Traditional security audits sponsored by ISO.
- CobiT (Control Objectives of Information and related Technology): sponsored and introduced by ISACA (Information System Audit and Control Association, www.isaca.org (accessed on 13 December 2020)) and ITGI (IT Governance Institute, www.itgi.org (accessed on 13 December 2020)). It is the most renowned and extensively accepted information technology governance framework.
- NIST (www.nist.org) 800-53 revision 4: Federal government audit sponsored by the National Institute of Standards and Technology (NIST)
- Cloud Security Alliance (CSA): Cloud-specific audit which is presented to cloud security auditing terms sponsored by CSA
- Payment Card Industry (PCI), Data Security Standard (DSS): PCI Qualified Security Assessor cloud supplement which is sponsored by PCI DSS.
- Basel II, ITIL, SANS(www.sans.org (accessed on 13 December 2020)), (ISC)^2 framework (www.isc2.org (accessed on 13 December 2020)), etc. organization which can audit and manage the levels of IT security risks.

To be effective, the above-mentioned security audit standards must confirm to a vast number of security concerns in the traditional computing or cloud computing paradigm. However, using these traditional auditing standards and frameworks in the Fog computing environment will not be well suited because all of these auditing standards and frameworks which are manual approaches. They can only provide limited support to make an evaluation and the audit's quality heavily depends on an auditor's experiences and knowledge which could be problematic, whereas the Fog environment is mostly dynamic and distributed across a large scale geographically. Therefore, software based automated auditing standards and frameworks which can perform real-time approaches would be best suited for the Fog computing environment.

The principal necessity to introduce cooperative context aware tools is extensively approved, and actions are being taken at the state level. Several studies have suggested how software tools can be used to extract meaningful knowledge to aid security configurations, auditing, and digital investigations [181]. Therefore, such tools are context-dependent, in that their functionality is conducted to identify threats that are expected. The only limitation of these tools is that each one requires different knowledge and skills to translate their output to obtain an understanding of why this extracted knowledge is significant [182]. Security auditing can be performed in an automated fashion by using Blockchain technology. The next section discusses Blockchain technology and what has been done so far in Fog using Blockchain technology.

5.6.3. Lightweight Cryptography Methods

Although the current cryptography methods like SHA-256 for hashing or advanced encryption standard (AES) for encryption on systems have a high processing power, they cannot be a suitable pick for IoT devices. To tackle this, the lightweight cryptography techniques proposed to diminish this gap where the above-mentioned methods cannot [183]. Several standard hashing methods such as SPONGENT [184], Lesamanta-LW [185] and PHOTON [186] were proposed while CLEFIA and PRESENT were proposed for block methods. Trivium and ENOCORO were also proposed as stream methods for lightweight cryptography. These functions and standards lead to overcoming the resource-limited devices. The flexibility around the key size, block size and rounds supports a range of design choices that enable the lightweight cryptography methods to tackle the gap that conventional cryptography algorithms such as AES struggles with. Hence, applying this method could be one of the best options to achieve encryption for resource limited devices.

As discussed, providing trust between Fog nodes is one of the important factors that should be taken into consideration as these end points may be vulnerable to several breaches and security attacks. To achieve a secure Fog environment, authentication plays a vital role in creating trust in a Fog environment while it cannot be a stand-alone solution. Apart from authentication, the behaviour of the nodes should be well understood. Behavioural analysis could help to provide a more trustable environment for the devices which interact with one another. There are various models to evaluate trust in Fog environments. Although these models can provide a level of trust in such environments, they have their own drawbacks that emerge from the need to have a comprehensive need for trust model in the Fog environment. Another measure to control the security of Fog devices is placing access control mechanisms. Providing appropriate access control to the users would prevent any privilege escalation for resource usage, which helps users increase their secrecy. Privacy is another factor that should come into consideration in a Fog environment. As there are various attacks on trusted computation environments, dimensions that affect the Fog privacy should be well analysed and appropriate privacy preservation techniques should be applied to remediate possible privacy breaches in such environments. Delivering these security mechanisms leads to a better protection and response in front of any potential threats that may threaten the Fog user.

As the traditional security techniques do not always fit into measuring security issue, a new distributed Blockchain technology is useful to handle security issues in Fog computing. In the next section, we discuss Blockchain and its utilization in Fog computing environments.

6. Blockchain Technology in Fog

The Blockchain is more than a database technology. Theoretically, a Blockchain is a ledger of the distributed database that can be programmed continuously to record a list of data. Blockchain is probably Bitcoin's major innovation foundation for a new decentralized and distributed system. Recently, Blockchain technology has been implemented across many real-time systems [187]. Blockchain is an evolving technology to build a secure, scalable and openly coordinated platform globally, which is not limited to currency or financial systems. Fog with Blockchain is shown in Figure 9.

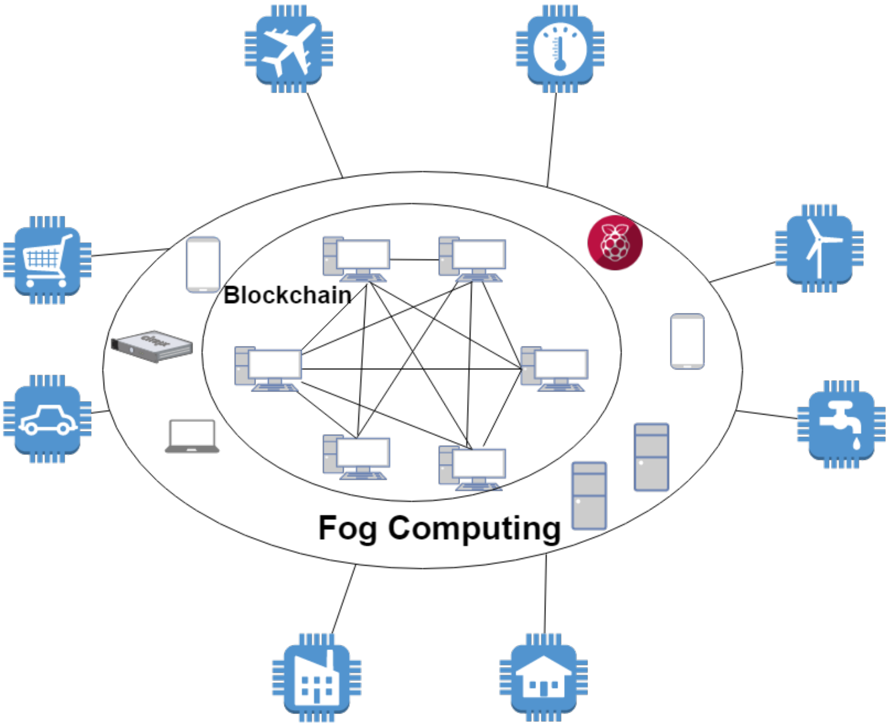

Figure 9. Fog with Blockchain.

6.1. Security Features of Blockchain Technology

Blockchain technology has its own strong security because there is no possibility of shutting down the system. A well-known cryptocurrency—Bitcoin [188]—was implemented using Blockchain technology. However, the financial system was still hacked, which it had never experienced before. The main strength of Bitcoin is its use of the Blockchain network as protection against attacks and threats by using multiple nodes which are committed to a single transaction by a consensus algorithm on this network. The transaction within Blockchain includes digital signatures. Currently, Blockchain uses the ECDSA public key algorithm to generate a digital signature. Blockchain prevents a single point of failure because it is a distributed system. It uses a hash function for block generation, of which currently it uses the SHA-256 hash function.

Some of the main features of Blockchain are as follows:

- Increased Capacity;
- Strong Security;
- Immutability;
- Faster Settlement;
- Decentralized System;
- Offers encryption and validation;
- Virtually impossible to hack;
- Can be private or public;
- Minting.

6.2. Role of Blockchain to Improve Security in Fog

The Blockchain technology was introduced for the secured cryptocurrency application such as Bitcoin. A realization soon dawned amongst many researchers that it possesses great security features that can be utilized in many real-world distributed applications (e.g., Cloud, and Fog computing). Security has become a key stumbling block toward the widespread adoption or implementation of Fog. Therefore, security concerns in Fog computing can be improved using Blockchain technology [189,190]. The following Blockchain features are useful in Fog context:

- Mitigate single point of failure;
- Highly encrypted network transactions;
- Node status tracking capabilities;
- Immutable Technology.

Blockchain can mitigate various threats and attacks in Fog such as the man-in-the-middle attack, DDoS attack and data tampering [191–194].

6.3. Blockchain between Fog and Edge Environments

Fog computing is a decentralized distribution system which aims to make cloud computing faster by creating data hubs or mini data processing centers which are hosted in smart devices. Basically, they accomplish a less demanding task and reduce the communication between the cloud and the end user. Fog allows for performing resource-constraints and short-term analytics close to the edge of the network, whereas the cloud accomplishes resource-intensive and longer-term analytics [195].

Fog computing faces enormous challenges, and there are constantly various issues that arise during its primary stages of its development. For example, in a distributed computing environment, it is a fact that how to protect its transactions and network resources with an evenly distributed security architecture is a challenge. It builds a kind of mesh network where every Fog node takes part based on their resource availability. Due to the distributed architecture of Fog computing, it is highly required when trust and security must be distributed. This is particularly significant where the Fog infrastructure, layers and Fog nodes are managed and owned by diversified entities.

However, a significant question arises in managing trust in a distributed and decentralized manner amongst participants that do not need mutual trust. Blockchain technology in reality is built for these kinds of challenges. Blockchain consensus algorithms have a suitability issue with regards to Fog applications. For instance, "Proof-of-Work" (PoW) consensus needs a huge computing capacity in order to solve a complex mathematical puzzle, so Fog devices are unable to host this mechanism. However, there are plenty of other protocols such as "Proof of Stake" (PoS) which is susceptible to running on Fog nodes with a similar capacity.

Blockchain uses a digital fingerprint for data, and the digital fingerprint is retained as long as the data remain. It thus provides an excellent way to securing data transferred from a distributing network between entities. When Blockchain is increasingly recognised when distinguishable from Bitcoin and any other cryptocurrencies, legal authorities and regulators will be required to develop a structure for recognising the protection it offers, and thereby theoretically extend the circumstances that can be used.

6.4. Recent Works that Used Blockchain for Fog

Several recent works used Blockchain for Fog computing environment. Tuli et al. [196] developed a framework that was based on Blockchain for the edge-Fog computing environment. This framework applied Blockchain, encryption techniques and authentication which can perform secure operations across sensitive data. Although this framework is a lightweight and based on a cross-platform, it has a few limitations and drawbacks because it takes comparatively higher computational overhead to carry out large scale deployments.

Sharma et al. [197] introduced a new and efficient distributed Blockchain cloud model based on three emerging technologies: Blockchain, Fog Computing and Software Defined Network (SDN). This model was presented to support high scalability, security, high availability, resiliency, real-time data delivery and low latency. Jeong et al. [198] proposed a Blockchain based secure Fog computing system. Their system can defend against various attacks such as IP spoofing, Sybil attacks and single points of failure. This system used the Blockchain method to guarantee secure authentication and non-repudiation. It can also perform operation when a Fog node is down.

Samaniego et al. [199] investigated the idea of virtual software-defined IoT components known as virtual resources in combination with the use of Blockchain technology. Dorri et al. [200] introduced a secure, private and lightweight Blockchain-based technology for the resource constraints related to IoT devices which can handle most security and privacy threats. It uses different kinds of Blockchains based on the network hierarchy and uses distributed trust methods to assure a decentralized topology.

6.5. Blockchain Oriented Startups in Fog and IoT Environments

OpenFog Consortium is one of the most well-known Blockchain oriented startups in the Fog environment. The OpenFog Consortium is in the process of building a composable and interoperable framework for Blockchain in the Fog distributed system. This implies that the various entities in the system that do not trust or are even known to each other still provide a meaningful consensus algorithm that is able to make decisions in a Fog oriented distributed system. The "autonomy," which is one of the eight pillars of OpenFog, is supported by the Consortium's work.

Recently, there have been multiple Blockchain oriented startups that have joined the OpenFog Consortium [190], and they are as follows:

- iExec: It Is the first Blockchain-Based Decentralized marketplace for Cloud Computing. It provides distributed applications that are secure, easily accessible and scalable to the services of computing resources for data-sets that are needed as well as the systems running on Blockchain (dApps).
- KeyChain: A new Global Blockchain-based data security infrastructure. It provides secure decentralized data authentication for the enterprise, finance environments, industries and IoT.

- Aetherworks: Brings original, high-quality technologies to the market and provides original software for distributed systems, including Fog computing and software-defined storages.
- Hyperchain: Provides an enterprise-level Blockchain network-based solution for government agencies, supply chain, data trading, fraud prevention and securities. It also supports enterprises to rapidly deploy, expand and configure Blockchain networks based on the Blockchain cloud platform.
- SONM: Provides infrastructure and can run any decentralized application (Fog application) or host Blockchain-based services. It also provides Fog computing distributed cloud computing services such as IaaS and PaaS, which are secured by Blockchain.
- Xage: The foremost Blockchain-protected security tool for the industrial IoT. Traditionally, more points of security vulnerability arise when there are more nodes and more connections. Moreover, the centralization technology prevents industrial systems working independently and in real time. Xage ensures that, with the combinations of Blockchain and encryption, more nodes mean more security, not less.

As described, Blockchain can significantly improve the security in a Fog environment. As creating the trust is one of the most important factors in Fog security, a consensus decision in a distributed system by Blockchain can ease this mechanism for Fog. Moreover, Blockchain can help to check the authentication and the integrity of data which transfer in a Fog environment.

7. Research Challenges and Future Research Directions

In this section, we are going to present and highlight a few significant and considerable issues which are challenging tasks for Fog computing to cope within cloud and edge environments. Finally, we provide a synopsis of probable research directions based on the existing research challenges.

7.1. Trust Management

Identification of trusted Fog nodes is a challenging task in the Fog platform. Usually, a Fog node that is trusted or untrusted can be identified by its malicious behavior. However, in this case, the malicious nature is not defined earlier on for a Fog node. Therefore, it is significant to define and categorize all malicious characteristics in the Fog system. The Fog system can be susceptible to regulate if a Fog node is trusted or untrusted. Hence, it is mandatory to enhance trust and, after all, an exalted trust management model is highly required.

Another challenging research issue is combining both distributed and centralised environments, which is important in the context of cloud-Fog-IoT environments. Therefore, a centralized trust management is required for the IoT environment, and it would be possible by using a Fog platform. Hence, it is still a challenging research issue.

Moreover, trust management in the Fog platform is entirely different compared to the cloud computing platform due to the distinctions of the cloud and Fog platform architecture and service offering mechanisms. As mentioned earlier, Fog is widely distributed; on the other hand, the cloud is centralized. In that case, it is easier to deploy trust management in the cloud environment because the cloud platform has its own in-place security infrastructure, whereas the Fog platform is more open, and the in-place security mechanism is absent. As a result, the Fog is vulnerable to malicious attacks. In addition, trust in the cloud environment is unidirectional, whereas trust in the Fog environment would be bidirectional in nature. The Fog node and the IoT devices must maintain a trusted relationship between one another before their interaction, as it is highly required in the Fog platform. Hence, designing a bidirectional trust model in the context of Fog and the IoT platform is a challenging task as well.

7.2. Privacy Assurance

The Fog nodes hold sensitive or private information of users, as the Fog nodes are placed in the proximity of the end users. Therefore, it is a challenging issue to assure trusted communication and make a secure computing environment between the Fog and IoT devices. In such a case, we can consider encrypting the user sensitive data before sending it to the Fog nodes. It is not viewed as a proper technique in the context of IoT devices, since conventional encryption and decryption mechanisms need a lot of computational power, whereas the IoT devices face challenges to encrypt and decrypt the user's sensitive data due to the resource constraints of IoT devices.

In another context, a single Fog node can manage sensitive data which come from different Fog users or across different applications. Therefore, there might be a chance to mix up different sources of data after the data aggregation step. In such a case, enforcing proper data encapsulation techniques at the Fog API or middleware level would be the solution. Hence, more research is needed.

Another challenging issue is to provide context-aware services in the Fog environment to the end user devices which are often involved in sharing sensitive resources such as location, as well as others' personal information amongst other geographically connected devices. Therefore, in such a scenario, it is highly required to ensure that data protection is present. Hence, providing the identity and location privacy in the Fog environment is a challenging task.

7.3. Authentication

It is an obvious fact that strong authentication and secure communication protocols in the Fog platform are missing. It is a rather alarming message for the research community. There has not been much research about the authentication mechanism in the area of Fog computing. However, several researchers have already proposed several solutions that we described earlier in the taxonomy section. However, these solutions are still not able to cope with the Fog platform. Therefore, to design and develop a new authentication method for Fog computing, one must consider the following criteria and how it can cope with the Fog platform smoothly.

- Authentication mechanisms must be compatible with the Fog user, end devices (IoT devices), application services and Fog Service providers on the cloud-Fog-IoT platform.
- Conventional authentication mechanisms are inefficient, and there is a necessity for a secure, environment-friendly, efficient, and scalable solution to cope up with an extensive amount of IoT devices that have limited resources to facilitate scalability and efficiency.
- Security and performance are both highly required in terms of different contextual devices and applications.
- Must meet with the dynamic behavior of the Fog environment, where Fog nodes dynamically leave and join frequently in the Fog network.
- Must ensure low complexity-based authentication in terms of scalability of the Fog network.
- Ensure smooth authentication and re-authentication methods in a dynamic manner.
- Design an efficient authentication method, where a cryptographic lightweight encryption algorithm should be considered between the Fog system and the IoT devices that can easily cope with the low processing power of IoT devices.
- Authentication should be less costly, as well as provide high usability and, in return, it should be user-friendly.

7.4. Access Control

In terms of the authentication mechanisms, there has not been much research work about access control methods in the Fog computing environment. However, plenty of work has been done in this field. Therefore, we still need to be able to accomplish an efficient design to draw the right kind of potential access and control model, with the intention to facilitate a secure platform within the heterogeneous devices in the Fog environment.

In the description section of access control, we mentioned a few access control models, describing their various features, characteristics, and, in the context of the Fog environment, we also highlighted numerous drawbacks and limitations. Many researchers have mentioned that Attribute Based Encryption (ABE) would be suitable as a method of owning access to control in the cloud, Fog and IoT environments. Because of the heterogeneous characteristics of the Fog system, the ABE method should be reconstructed in order to mitigate the major challenges (Latency, policy-management, fine-grained and enforced by the cryptographic method) amongst the cloud-Fog-IoT computing environment users.

On the other hand, in the Fog system, data originate and are encrypted and decrypted by miniaturized devices with low computational powers. In such a case, deploying access control mechanisms in those devices would be a burden and would need heavy computational power to process the access control mechanism. Meanwhile, Fog devices are being placed near end devices. In addition, Fog devices are much more computationally powerful than end user IoT devices. Therefore, to overcome the limitations of IoT devices, an outsource capability lightweight ABE based access control would be compatible with the Fog environment. As opposed to Fog computing, which is dynamic in nature, there are numerous devices which join and leave simultaneously in the Fog network. Thus, the access control policy and attributes of the users would be changed according to this dynamic characteristic. Therefore, it is highly required that ABE-based access control mechanisms must have the capability to assist in creating, updating, as well as revoking the attributes of the users. With ABE based access control, designing the revocation process would face new challenges, and how Fog collaborates with the cloud environment during the revocation process would need to be part of further research. Therefore, to design a new access control method for the Fog platform, one must consider a few characteristics which are as follows:

- As we have mentioned earlier, Fog is a fully virtualized platform by nature, and it provides diversified environments for the Fog network. In this case, there might be a chance in which a side-channeled-attack occurs due to the nature of sharing resources amongst untrusted tenants. Therefore, it is a significant concern in terms of designing an access control method which must be capable of synthesizing within the virtualized platform and multitenant environment efficiently and securely.
- Access control should be secure and efficient for the Fog environment computing on the basis of multi-authority, as well as be attribute-based, considering low computation with outsourcing capabilities as well as attributes that have the means to control user revocation capability.
- An access control method should be lightweight and fine-grained due to the resource constraints suffered amongst IoT devices.
- An access control method must be capable of performing in both centralized and distributed architectural environment accordingly.

7.5. Threats and Attacks

As we mentioned earlier, Fog computing faces various security and privacy issues. Due to the distributed nature and extensive amount of devices connected with it, often, there might be a chance for a threat or an attack to occur. In the description section, we have already highlighted several threats and attacks and their impact in the Fog environment. Detection, identification and mitigation of these threats and attacks would be a challenging task in terms of the dynamic Fog computing environment. However, in order to build a reliable and trustworthy Fog platform, there is a research gap and the lack of security solutions available to detect and identify these threats and attacks needs to be addressed. Based on our review across various threats and attacks, we have suggested the following issues which need to be addressed in the future to overcome these challenges:

- Complex trust situations and insecure authentication and authorization systems.

- Dynamic behavior such as creating, deleting, joining and leaving of Fog nodes, or servers in the Fog layer.
- Detection of malicious nodes or rogue nodes is a challenging task because of the dynamic nature of leaving and joining by the Fog nodes.
- Implementing IDS in large-scale, geo-distributed with low-latency requirement with highly mobile Fog computing systems is a complex task.
- Due to the distributed environment, hybrid detection techniques are required to identify malicious activities.
- Due to the resource constraints of the Fog devices, designing a high security and low cost threat and attack detection is the key problem in the Fog.
- Identifying and mitigating threats and attacks from both the Fog node and Fog user at the same time is challenging.

7.6. Security Auditing

Audit rights provide a crucial risk mitigation tool regarding security issues related to the Fog. Auditing security configurations in the Fog platform is a complex task, as it is a gateway to the cloud platform and heavily relies on expert knowledge, which is required for understanding the different security configurations. However, these systems can be imperfect, and not user friendly for the home users and small companies.

In this section, we explore various unique challenges that isolate Fog security auditing from the traditional security auditing or cloud security auditing protocols. These challenges represent the significance of special provisions for Fog security auditing in current or evolving security auditing standards.

Challenges:

- The Fog computing landscape is dynamic and consists of huge resources, where traditional data encryption or decryption need a heavy computational overhead.
- Without proper technological support, it is challenging to manage extensive amounts of different contextual data.
- To identify new security threats and defend against those threats is also a challenging task
- Fog computing brings easy accessibility to our work and personal lives, but with that accessibility comes new security risks and challenges
- Understanding the different contexts of the Fog computing environment is important. Different contexts with regards to the environment's security issues would bring different research challenges.

Questions:

- How to encrypt or decrypt data and how to access that data simultaneously?
- How to perform auditing processes across different environment data contexts?
- Do we need to use the same matrix for the edge environment or cloud environment?
- Can our current risk assessment capture the risks correctly?
- How to perform and manage real-time processing and auditing at the same time?

In order to overcome the above-mentioned challenges and questions, it is highly required to develop an automatic method, which can be capable to recognize and identify security infringements as well as mitigate those security risks in Fog computing. Further research needs to be carried out by utilizing Blockchain technology to mitigate security issues in Fog.

7.7. Secure 5G Enable Fog Network

In the near future, Fog devices will be connected through the 5G network. Connecting Fog devices with the 5G network, new security challenges emerge mainly in the authentication. The traditional one-way or mutual authentication process is not useful due to the authentication process between the user and services [201]. In this case, a new hybrid authentication model is required. Using 5G, Fog will be useful to talk with things and devices. For example, in a smart home and smart city environment, one citizen needs an ambulance which will direct him to a specialized hospital close to the location of the user where a remote surgery can perform. Here, a hybrid security mechanism is required to secure the whole application environment since many parties are involved in this processing. Any emergency environment similar to this requires a strong and reliable authentication process. User privacy is also important in such a 5G enabled Fog computing environment because user data may pass through the various untrusted, third-party devices, network equipment, and access networks. Hence, we need to explore more about hybrid authentication methods and privacy protection in a 5G enabled Fog network.

8. Conclusions

The main objective of this study is to review, investigate and analyze the issues of the Fog computing platform to recognize their probable security flaws. The obvious fact is that there are numerous security issues that do not exist in the traditional cloud computing environment, which need to be considered. In addition, significant developments in the Fog environment are required. We fill the gap of the current literature by aggregating all security aspects of Fog computing paradigm such as authentication, access control, privacy preservation, trust management, threats, attacks and security auditing. We have also investigated the main challenges, and tried to exhibit the motives as to why the security methods in the cloud platform cannot be employed directly in Fog computing when it comes to auditing. In this study, we have also introduced a taxonomy, by considering numerous security issues and protection according to the Fog environment, as well as briefly introduced and discussed these issues retrospectively. In addition, we also discussed how Blockchain could help to provide solutions to some of the data security concerns in the Fog environment. However, further research is required to see how much protection can be ensured against threats and attacks using Blockchain in Fog. At the end, we highlighted several threats and attacks which might occur frequently under the circumstances of the Fog computing network.

Interestingly, the Fog is a new paradigm, which therefore requires mitigation of the associated security issues that are still challenging tasks. With regards to the system architecture of Fog computing, researchers need to do further future work and figure out the challenges with respect to security within the three-tiered architecture of the cloud-Fog-IoT computing system. As Fog computing is an extension of cloud computing, in this paper, we only covered the security issues concepts related to Fog. We did not consider the security-related issues in the cloud.

In the future, we will be investigating secure SLA management in Fog through the Blockchain and integration of SDN and Blockchain in Fog to improve the efficiency of the system, compare security and privacy solutions of other similarly distributed environments such as Mobile computing and Edge computing with the Fog and present these security issues and suitable solutions for the Fog. Furthermore, we will investigate and classify the threat models and Blockchain technologies in Fog computing.

Author Contributions: Conceptualization, A.A.-N.P., R.K.N. and S.G.; Formal analysis, A.A.-N.P.; Investigation, A.A.-N.P., S.K.B. and E.A.; Methodology, A.A.-N.P. and R.K.N.; Project administration, R.K.N.; Supervision, R.K.N.; Validation, A.A.-N.P.; Visualization, A.A.-N.P.; Writing—original draft, A.A.-N.P.; Writing—review & editing, R.K.N., S.G., S.K.B., M.A.K.P., E.A., M.B.A., A.M. and M.G.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Säveros, F.; Gong, M.; Carlsson, N.; Mahanti, A. An energy-efficient handover algorithm for wireless sensor networks. In Proceedings of the 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC), Las Vegas, NV, USA, 9–11 December 2016; pp. 1–8, doi:10.1109/PCCC.2016.7820636.
2. Gartner. Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, up 31 Percent from 2016. 2017. Available online: https://thejournal.com/articles/2017/02/09/gartner-2017-will-see-8.4-billion-connected-things.aspx (accessed on 12 January 2021).
3. Symanovich, S. The Future of IoT: 10 Predictions about the Internet of Things. Cyber Security Blog, Norton by Symantec, Accessed. 2019. pp. 2–17. Available online: https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html (accessed on 12 January 2021).
4. Assunção, M.D.; Calheiros, R.N.; Bianchi, S.; Netto, M.A.; Buyya, R. Big Data computing and clouds: Trends and future directions. *J. Parallel Distrib. Comput.* **2015**, *79*, 3–15.
5. Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog computing and its role in the internet of things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 13–17 August 2012; pp. 13–16.
6. Naha, R.K.; Garg, S.; Georgakopoulos, D.; Jayaraman, P.P.; Gao, L.; Xiang, Y.; Ranjan, R. Fog Computing: survey of trends, architectures, requirements, and research directions. *IEEE Access* **2018**, *6*, 47980–48009.
7. Kapil, D.; Tyagi, P.; Kumar, S.; Tamta, V.P. Cloud computing: Overview and research issues. In Proceedings of the 2017 International Conference on Green Informatics (ICGI), Fuzhou, China, 15–17 August 2017; pp. 71–76.
8. CSO. *The 14 Biggest Data Breaches of the 21st Century*; CSO: Perth, Australia, 2020.
9. Zissis, D.; Lekkas, D. Addressing cloud computing security issues. *Future Gener. Comput. Syst.* **2012**, *28*, 583–592.
10. Yi, S.; Qin, Z.; Li, Q. Security and privacy issues of fog computing: A survey. In Proceedings of the International Conference on Wireless Algorithms, Systems, and Applications, Qufu, China, 10–12 August 2015; pp. 685–695.
11. Zhang, P.; Zhou, M.; Fortino, G. Security and trust issues in Fog computing: A survey. *Future Gener. Comput. Syst.* **2018**, *88*, 16–27.
12. Khan, S.; Parkinson, S.; Qin, Y. Fog computing security: A review of current applications and security solutions. *J. Cloud Comput.* **2017**, *6*, 19.
13. 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.
14. Rauf, A.; Shaikh, R.A.; Shah, A. Security and privacy for IoT and fog computing paradigm. In Proceedings of the 2018 15th Learning and Technology Conference (L&T), Jeddah, Saudi Arabia, 25–26 February 2018; pp. 96–101.
15. Stojmenovic, I.; Wen, S. The fog computing paradigm: Scenarios and security issues. In Proceedings of the 2014 Federated Computer Science and Information Systems (FedCSIS), Warsaw, Poland, 7–10 Septmber 2014; pp. 1–8.
16. Wang, Y.; Uehara, T.; Sasaki, R. Fog computing: Issues and challenges in security and forensics. In Proceedings of the 2015 IEEE 39th Annual Computer Software and Applications Conference (COMPSAC), Taichung, Taiwan, 1–5 July 2015; Volume 3, pp. 53–59.
17. 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.
18. Ud Din, I.; Guizani, M.; Kim, B.; Hassan, S.; Khurram Khan, M. Trust Management Techniques for the Internet of Things: A Survey. *IEEE Access* **2019**, *7*, 29763–29787.
19. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access* **2019**, *7*, 82721–82743.
20. Tariq, N.; Asim, M.; Al-Obeidat, F.; Zubair Farooqi, M.; Baker, T.; Hammoudeh, M.; Ghafir, I. The security of big data in fog-enabled IoT applications including blockchain: A survey. *Sensors* **2019**, *19*, 1788.
21. Yu, S.Y.; Brownlee, N.; Mahanti, A. Comparative analysis of big data transfer protocols in an international high-speed network. In Proceedings of the 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC), Nanjing, China, 14–16 December 2015; pp. 1–9.
22. Yu, S.Y.; Brownlee, N.; Mahanti, A. Characterizing performance and fairness of big data transfer protocols on long-haul networks. In Proceedings of the 2015 IEEE 40th Conference on Local Computer Networks (LCN), Clearwater Beach, FL, USA, 26–29 October 2015; pp. 213–216.
23. Yu, S.Y.; Brownlee, N.; Mahanti, A. Comparative performance analysis of high-speed transfer protocols for big data. In Proceedings of the 38th Annual IEEE Conference on Local Computer Networks, Sydney, NSW, Australia, 21–24 October 2013; pp. 292–295.
24. Yu, S.Y.; Brownlee, N.; Mahanti, A. Performance Evaluation of Protocols for Big Data Transfers. In *Big Data: Storage, Sharing, and Security*; Auerbach Publications: New York, NY, USA, 2016; p. 43.
25. Tange, K.; De Donno, M.; Fafoutis, X.; Dragoni, N. Towards a Systematic Survey of Industrial IoT Security Requirements: Research Method and Quantitative Analysis. In Proceedings of the 2019 Workshop on Fog Computing and the Iot (iot-fog'19), Montreal, QC, Canada, 15–18 April 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 56–63, doi:10.1145/3313150.3313228.
26. Takabi, H.; Joshi, J.B.; Ahn, G.J. Security and privacy challenges in cloud computing environments. *IEEE Secur. Priv.* **2010**, *8*, 24–31.

27. Battula, S.K.; Garg, S.; Naha, R.K.; Thulasiraman, P.; Thulasiram, R. A Micro-Level Compensation-Based Cost Model for Resource Allocation in a Fog Environment. *Sensors* **2019**, *19*, 2954.
28. Ai, Y.; Peng, M.; Zhang, K. Edge computing technologies for Internet of Things: A primer. *Digit. Commun. Netw.* **2018**, *4*, 77–86.
29. Soliman, M.; Abiodun, T.; Hamouda, T.; Zhou, J.; Lung, C.H. Smart home: Integrating internet of things with web services and cloud computing. In Proceedings of the 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, Bristol, UK, 2–5 December 2013; Volume 2, pp. 317–320.
30. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of things for smart cities. *IEEE Internet Things J.* **2014**, *1*, 22–32.
31. Sial, A.; Singh, A.; Mahanti, A. Detecting anomalous energy consumption using contextual analysis of smart meter data. *Wirel. Netw.* **2019**, 1–18, doi:10.1007/s11276-019-02074-8.
32. Sial, A.; Singh, A.; Mahanti, A.; Gong, M. Heuristics-Based Detection of Abnormal Energy Consumption. In Proceedings of the International Conference on Smart Grid Inspired Future Technologies, Auckland, New Zealand, 23–24 April 2018; pp. 21–31.
33. Yuehong, Y.; Zeng, Y.; Chen, X.; Fan, Y. The internet of things in healthcare: An overview. *J. Ind. Inf. Integr.* **2016**, *1*, 3–13.
34. Xu, J.; Andrepoulos, Y.; Xiao, Y.; van Der Schaar, M. Non-stationary resource allocation policies for delay-constrained video streaming: Application to video over Internet-of-Things-enabled networks. *IEEE J. Sel. Areas Commun.* **2014**, *32*, 782–794.
35. Tammishetty, S.; Ragunathan, T.; Battula, S.K.; Rani, B.V.; RaviBabu, P.; Nagireddy, R.; Jorika, V.; Reddy, V.M. IOT-based traffic signal control technique for helping emergency vehicles. In Proceedings of the First International Conference on Computational Intelligence and Informatics, Hyderabad, India, 28–30 May 2016; pp. 433–440.
36. Gerla, M.; Lee, E.K.; Pau, G.; Lee, U. Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. In Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, 6–8 March 2014; pp. 241–246.
37. Tsugawa, M.; Matsunaga, A.; Fortes, J.A. Cloud computing security: What changes with software-defined networking? In *Secure Cloud Computing*; Springer: New York, NY, USA, 2014; pp. 77–93.
38. Khatiwada, M.; Budhathoki, R.K.; Mahanti, A. Characterizing Mobile Web Traffic: A Case Study of an Academic Web Server. In Proceedings of the 2019 Twelfth International Conference on Mobile Computing and Ubiquitous Network (ICMU), Kathmandu, Nepal, 4–6 November 2019; pp. 1–6.
39. Song, Y.D.; Mahanti, A. Comparison of mobile and fixed device workloads in an academic web server. In Proceedings of the 2019 IEEE International Symposium on Measurements & Networking (M&N), Catania, Italy, 8–10 July 2019; pp. 1–6.
40. Shin, S.; Gu, G. CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?). In Proceedings of the 2012 20th IEEE International Conference on Network Protocols (ICNP), Austin, TX, USA, 30 October–2 November 2012; pp. 1–6.
41. McKeown, N.; Anderson, T.; Balakrishnan, H.; Parulkar, G.; Peterson, L.; Rexford, J.; Shenker, S.; Turner, J. OpenFlow: Enabling innovation in campus networks. *ACM SIGCOMM Comput. Commun. Rev.* **2008**, *38*, 69–74.
42. Sharma, V.K.; Verma, L.P.; Kumar, M.; Naha, R.K.; Mahanti, A. A-CAFDSP: An adaptive-congestion aware Fibonacci sequence based data scheduling policy. *Comput. Commun.* **2020**, *158*, 141–165.
43. Klaedtke, F.; Karame, G.O.; Bifulco, R.; Cui, H. Access control for SDN controllers. In Proceedings of the Third Workshop on Hot Topics in Software Defined Networking, Chicago, IL, USA, 22 August 2014; pp. 219–220.
44. Press, G. *Idc: Top 10 Technology Predictions for 2015*; Fobes: Jersey City, NJ, USA, 2014.
45. Lee, K.; Kim, D.; Ha, D.; Rajput, U.; Oh, H. On security and privacy issues of fog computing supported Internet of Things environment. In Proceedings of the 2015 6th International Conference on the Network of the Future (NOF), Montreal, QC, Canada, 30 September–2 October 2015; pp. 1–3.
46. Lu, R.; Liang, X.; Li, X.; Lin, X.; Shen, X. Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *23*, 1621–1631.
47. Yang, K.; Jia, X. Data storage auditing service in cloud computing: challenges, methods and opportunities. *World Wide Web* **2012**, *15*, 409–428.
48. Guan, Y.; Shao, J.; Wei, G.; Xie, M. Data security and privacy in fog computing. *IEEE Netw.* **2018**, *32*, 106–111.
49. Modi, C.; Patel, D.; Borisaniya, B.; Patel, H.; Patel, A.; Rajarajan, M. A survey of intrusion detection techniques in cloud. *J. Netw. Comput. Appl.* **2013**, *36*, 42–57.
50. Maglaras, L.A.; Jiang, J.; Cruz, T.J. Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems. *J. Inf. Secur. Appl.* **2016**, *30*, 15–26.
51. Valenzuela, J.; Wang, J.; Bissinger, N. Real-time intrusion detection in power system operations. *IEEE Trans. Power Syst.* **2013**, *28*, 1052–1062.
52. Qin, Z.; Li, Q.; Chuah, M.C. Defending against unidentifiable attacks in electric power grids. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *24*, 1961–1971.
53. Anwar, S.; Mohamad Zain, J.; Zolkipli, M.F.; Inayat, Z.; Khan, S.; Anthony, B.; Chang, V. From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. *Algorithms* **2017**, *10*, 39.
54. Cruz, T.; Rosa, L.; Proença, J.; Maglaras, L.; Aubigny, M.; Lev, L.; Jiang, J.; Simoes, P. A cybersecurity detection framework for supervisory control and data acquisition systems. *IEEE Trans. Ind. Inform.* **2016**, *12*, 2236–2246.
55. IEEE Std 1934-2018, IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing. 2018. Available online: https://sci-hub.se/10.1109/IEEESTD.2018.8423800 (accessed on 13 December 2020).

56. Bellavista, P.; Berrocal, J.; Corradi, A.; Das, S.K.; Foschini, L.; Zanni, A. A survey on fog computing for the Internet of Things. *Pervasive Mob. Comput.* **2019**, *52*, 71–99.
57. Li, H.; Singhal, M. Trust management in distributed systems. *Computer* **2007**, *40*, 45–53.
58. Rahman, F.H.; Au, T.W.; Newaz, S.S.; Suhaili, W.S.; Lee, G.M. Find my trustworthy fogs: A fuzzy-based trust evaluation framework. *Future Gener. Comput. Syst.* **2018**, *109*, 562–572.
59. Blaze, M.; Feigenbaum, J.; Lacy, J. Decentralized trust management. In Proceedings of the 1996 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 6–8 May 1996; pp. 164–173.
60. Cho, J.H.; Swami, A.; Chen, R. A survey on trust management for mobile ad hoc networks. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 562–583.
61. Mukherjee, M.; Matam, R.; Shu, L.; Maglaras, L.; Ferrag, M.A.; Choudhury, N.; Kumar, V. Security and privacy in fog computing: Challenges. *IEEE Access* **2017**, *5*, 19293–19304.
62. Guo, J.; Chen, R.; Tsai, J.J. A survey of trust computation models for service management in internet of things systems. *Comput. Commun.* **2017**, *97*, 1–14.
63. Pranata, I.; Skinner, G.; Athauda, R. A holistic review on trust and reputation management systems for digital environments. *Int. J. Comput. Inf. Technol.* **2012**, *1*, 44–53.
64. Kraemer, F.A.; Braten, A.E.; Tamkittikhun, N.; Palma, D. Fog computing in healthcare—A review and discussion. *IEEE Access* **2017**, *5*, 9206–9222.
65. Jøsang, A.; Ismail, R.; Boyd, C. A survey of trust and reputation systems for online service provision. *Decis. Support Syst.* **2007**, *43*, 618–644.
66. Damiani, E.; di Vimercati, D.C.; Paraboschi, S.; Samarati, P.; Violante, F. A reputation-based approach for choosing reliable resources in peer-to-peer networks. In Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, DC USA, 18–22 November 2002; pp. 207–216.
67. Abhijit, J.P.; Syam Prasad, G. Trust Based Security Model for IoT and Fog based Applications. *Int. J. Eng. Technol.* **2018**, *7*, 691. doi:10.14419/ijet.v7i2.7.10924.
68. Soleymani, S.A.; Abdullah, A.H.; Zareei, M.; Anisi, M.H.; Vargas-Rosales, C.; Khan, M.K.; Goudarzi, S. A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing. *IEEE Access* **2017**, *5*, 15619–15629.
69. Wang, T.; Zhang, G.; Bhuiyan, M.Z.A.; Liu, A.; Jia, W.; Xie, M. A novel trust mechanism based on fog computing in sensor–cloud system. *Future Gener. Comput. Syst.* **2018**, *109*, 573–582.
70. Yuan, J.; Li, X. A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion. *IEEE Access* **2018**, *6*, 23626–23638.
71. Dang, T.D.; Hoang, D. A data protection model for fog computing. In Proceedings of the 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC), Valencia, Spain, 8–11 May 2017; pp. 32–38, doi:10.1109/FMEC.2017.7946404.
72. Aghasian, E.; Garg, S.; Montgomery, J. User's Privacy in Recommendation Systems Applying Online Social Network Data, A Survey and Taxonomy. *arXiv* **2018**, arXiv:1806.07629.
73. Fu, A.; Song, J.; Li, S.; Zhang, G.; Zhang, Y. A privacy-preserving group authentication protocol for machine-type communication in LTE/LTE-A networks. *Secur. Commun. Netw.* **2016**, *9*, 2002–2014.
74. Aghasian, E.; Garg, S.; Montgomery, J. An automated model to score the privacy of unstructured information—Social media case. *Comput. Secur.* **2020**, *92*, 101778.
75. Talluri, L.S.R.K.; Thirumalaisamy, R.; Kota, R.; Sadi, R.P.R.; KC, U.; Naha, R.K.; Mahanti, A. Providing Consistent State to Distributed Storage System. *Computers* **2021**, *10*, 23.
76. Aghasian, E.; Garg, S.; Gao, L.; Yu, S.; Montgomery, J. Scoring users' privacy disclosure across multiple online social networks. *IEEE Access* **2017**, *5*, 13118–13130.
77. Koo, D.; Shin, Y.; Yun, J.; Hur, J. A Hybrid Deduplication for Secure and Efficient Data Outsourcing in Fog Computing. In Proceedings of the 2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Luxembourg, 12–15 December 2016; pp. 285–293.
78. Cao, N.; Wang, C.; Li, M.; Ren, K.; Lou, W. Privacy-preserving multi-keyword ranked search over encrypted cloud data. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 222–233.
79. Qin, Z.; Yi, S.; Li, Q.; Zamkov, D. Preserving secondary users' privacy in cognitive radio networks. In Proceedings of the IEEE INFOCOM 2014—IEEE Conference on Computer Communications, Toronto, ON, Canada, 27 April–2 May 2014; pp. 772–780.
80. Rial, A.; Danezis, G. Privacy-preserving smart metering. In Proceedings of the 10th annual ACM Workshop on Privacy in the Electronic Society, Chicago, IL, USA, 17 October 2011; pp. 49–60.
81. Al Hamid, H.A.; Rahman, S.M.M.; Hossain, M.S.; Almogren, A.; Alamri, A. A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. *IEEE Access* **2017**, *5*, 22313–22328.
82. Novak, E.; Li, Q. Near-pri: Private, proximity based location sharing. In Proceedings of the IEEE INFOCOM 2014—IEEE Conference on Computer Communications, Toronto, ON, Canada, 27 April–2 May 2014; pp. 37–45.
83. Dwork, C.; van Tilborg, H.; Jajodia, S. Differential Privacy. In *Encyclopedia of Cryptography and Security*; Springer: Boston, MA, USA, 2011.

84. Wei, W.; Xu, F.; Li, Q. Mobishare: Flexible privacy-preserving location sharing in mobile online social networks. In Proceedings of the 2012 Proceedings IEEE INFOCOM, Orlando, FL, USA, 25–30 March 2012; pp. 2616–2620.
85. Naha, R.K.; Othman, M. Optimized load balancing for efficient resource provisioning in the cloud. In Proceedings of the 2014 IEEE 2nd International Symposium on Telecommunication Technologies (ISTT), Langkawi, Malaysia, 24–26 November 2014; pp. 442–445.
86. Gao, Z.; Zhu, H.; Liu, Y.; Li, M.; Cao, Z. Location privacy in database-driven cognitive radio networks: Attacks and countermeasures. In Proceedings of the 2013 Proceedings IEEE INFOCOM, Turin, Italy, 14–19 April 2013; pp. 2751–2759.
87. McLaughlin, S.; McDaniel, P.; Aiello, W. Protecting consumer privacy from electric load monitoring. In Proceedings of the 18th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 17–21 October 2011; pp. 87–98.
88. Wang, H.; Wang, Z.; Domingo-Ferrer, J. Anonymous and secure aggregation scheme in fog-based public cloud computing. *Future Gener. Comput. Syst.* **2018**, *78*, 712–719.
89. Yang, R.; Xu, Q.; Au, M.H.; Yu, Z.; Wang, H.; Zhou, L. Position based cryptography with location privacy: A step for fog computing. *Future Gener. Comput. Syst.* **2018**, *78*, 799–806.
90. Kumar, P.; Zaidi, N.; Choudhury, T. Fog computing: Common security issues and proposed countermeasures. In Proceedings of the International Conference System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 25–27 November 2016; pp. 311–315.
91. Liu, J.; Li, J.; Zhang, L.; Dai, F.; Zhang, Y.; Meng, X.; Shen, J. Secure intelligent traffic light control using fog computing. *Future Gener. Comput. Syst.* **2018**, *78*, 817–824.
92. Lu, R.; Heung, K.; Lashkari, A.H.; Ghorbani, A.A. A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. *IEEE Access* **2017**, *5*, 3302–3312.
93. Ahmadizadeh, E.; Aghasian, E.; Taheri, H.P.; Nejad, R.F. An Automated Model to Detect Fake Profiles and botnets in Online Social Networks Using Steganography Technique. *IOSR J. Comput. Eng.* **2015**, *17*, 65–71.
94. Chegini, H.; Mahanti, A. A Framework of Automation on Context-Aware Internet of Things (IoT) Systems. In Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing Companion, Auckland, New Zealand, 2–5 December 2019; pp. 157–162.
95. Chegini, H.; Naha, R.K.; Mahanti, A.; Thulasiraman, P. Process Automation in an IoT–Fog–Cloud Ecosystem: A Survey and Taxonomy. *IoT* **2021**, *2*, 92–118.
96. Aghasian, E.; Garg, S.; Montgomery, J. A privacy-enhanced friending approach for users on multiple online social networks. *Computers* **2018**, *7*, 42.
97. Stojmenovic, I.; Wen, S.; Huang, X.; Luan, H. An overview of fog computing and its security issues. *Concurr. Comput. Pract. Exp.* **2016**, *28*, 2991–3005.
98. Mohammed, S.; Ramkumar, L.; Rajasekar, V. Password-based Authentication in Computer Security: Why is it still there? *SIJ Trans. Comput. Sci. Eng. Its Appl.* **2017**, *5*, 33–36.
99. Tsai, J.L. Efficient Nonce-based Authentication Scheme for Session Initiation Protocol. *IJ Netw. Secur.* **2009**, *9*, 12–16.
100. Lu, R.; Cao, Z.; Chai, Z.; Liang, X. A Simple User Authentication Scheme for Grid Computing. *IJ Netw. Secur.* **2008**, *7*, 202–206.
101. Kumar, M. An Enhanced Remote User Authentication Scheme with Smart Card. *IJ Netw. Secur.* **2010**, *10*, 175–184.
102. Lee, C.C.; Liu, C.H.; Hwang, M.S. Guessing Attacks on Strong-Password Authentication Protocol. *IJ Netw. Secur.* **2013**, *15*, 64–67.
103. Fadlullah, Z.M.; Fouda, M.M.; Kato, N.; Takeuchi, A.; Iwasaki, N.; Nozaki, Y. Toward intelligent machine-to-machine communications in smart grid. *IEEE Commun. Mag.* **2011**, *49*. 60–65.
104. Balfanz, D.; Smetters, D.K.; Stewart, P.; Wong, H.C. Talking to Strangers: Authentication in Ad-Hoc Wireless Networks. In Proceedings of Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 8–11 February 2002.
105. Bouzefrane, S.; Mostefa, A.F.B.; Houacine, F.; Cagnon, H. Cloudlets authentication in nfc-based mobile computing. In Proceedings of the 2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), Oxford, UK, 8–11 April 2014; pp. 267–272.
106. Ibrahim, M.H. Octopus: An Edge-fog Mutual Authentication Scheme. *IJ Netw. Secur.* **2016**, *18*, 1089–1101.
107. Manzoor, A.; Tahir, M.A.u.H.; Wahid, A.; Shah, M.A.; Akhunzada, A. Secure Login Using Multi-Tier Authentication Schemes in Fog Computing. *EAI Endorsed Trans. Internet Things* **2018**, *3*, 5.
108. Vishwanath, A.; Peruri, R.; He, J.S. *Security in Fog Computing through Encryption*; DigitalCommons@ Kennesaw State University: Hong Kong, China, 2016.
109. Wazid, M.; Das, A.K.; Kumar, N.; Vasilakos, A.V. Design of secure key management and user authentication scheme for fog computing services. *Future Gener. Comput. Syst.* **2019**, *91*, 475–492.
110. Dsouza, C.; Ahn, G.J.; Taguinod, M. Policy-driven security management for fog computing: Preliminary framework and a case study. In Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IRI), Redwood City, CA, USA, 13–15 August 2014; pp. 16–23.
111. Alharbi, S.; Rodriguez, P.; Maharaja, R.; Iyer, P.; Subaschandrabose, N.; Ye, Z. Secure the internet of things with challenge response authentication in fog computing. In Proceedings of the 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC), San Diego, CA, USA, 10–12 December 2017; pp. 1–2.

112. Amor, A.B.; Abid, M.; Meddeb, A. A Privacy-Preserving Authentication Scheme in an Edge-Fog Environment. In Proceedings of the 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), Hammamet, Tunisia, 30 October–3 November 2017; pp. 1225–1231.
113. 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.
114. Ha, D.A.; Nguyen, K.T.; Zao, J.K. Efficient authentication of resource-constrained IoT devices based on ECQV implicit certificates and datagram transport layer security protocol. In Proceedings of the Seventh Symposium on Information and Communication Technology, Ho Chi Minh, Vietnam, 8–9 December 2016; pp. 173–179.
115. Gope, P.; Sikdar, B. Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices. *IEEE Internet Things J.* **2018**, *6*, 580–589.
116. Zhang, P.; Liu, J.K.; Yu, F.R.; Sookhak, M.; Au, M.H.; Luo, X. A survey on access control in fog computing. *IEEE Commun. Mag.* **2018**, *56*, 144–149.
117. Meghanathan, N. Review of access control models for cloud computing. *Comput. Sci. Inf. Sci.* **2013**, *3*, 77–85.
118. Vohra, K.; Dave, M. Multi-Authority Attribute Based Data Access Control in Fog Computing. *Procedia Comput. Sci.* **2018**, *132*, 1449–1457.
119. Sandhu, R.S.; Coyne, E.J.; Feinstein, H.L.; Youman, C.E. Role-based access control models. *Computer* **1996**, *29*, 38–47.
120. Punithasurya, K.; Jeba Priya, S. Analysis of different access control mechanism in cloud. *Int. J. Appl. Inf. Syst. Found. Comput. Sci.* **2012**, *4*, 34–39.
121. Sookhak, M.; Yu, F.R.; Khan, M.K.; Xiang, Y.; Buyya, R. Attribute-based data access control in mobile cloud computing: Taxonomy and open issues. *Future Gener. Comput. Syst.* **2017**, *72*, 273–287.
122. Langaliya, C.; Aluvalu, R. Enhancing cloud security through access control models: A survey. *Int. J. Comput. Appl.* **2015**, *112*, doi:10.5120/19677-1400.
123. Sahai, A.; Waters, B. Fuzzy identity-based encryption. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 22–26 May 2005; pp. 457–473.
124. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 30 October–3 November 2006; pp. 89–98.
125. Bethencourt, J.; Sahai, A.; Waters, B. Ciphertext-policy attribute-based encryption. In Proceedings of the IEEE Symposium on Security and Privacy 2007 (SP'07), Berkeley, CA, USA, 20–23 May 2007; pp. 321–334.
126. Wang, Y.; Wei, L.; Tong, X.; Zhao, X.; Li, M. CP-ABE Based Access Control for Cloud Storage. In *Information Technology and Intelligent Transportation Systems*; Springer: Cham, Switzerland, 2017; pp. 463–472.
127. Li, F.; Rahulamathavan, Y.; Conti, M.; Rajarajan, M. Robust access control framework for mobile cloud computing network. *Comput. Commun.* **2015**, *68*, 61–72.
128. Salonikias, S.; Mavridis, I.; Gritzalis, D. Access control issues in utilizing fog computing for transport infrastructure. In Proceedings of the International Conference on Critical Information Infrastructures Security, Berlin, Germany, 5–7 October 2015; pp. 15–26.
129. Arlitt, M.; Carlsson, N.; Gill, P.; Mahanti, A.; Williamson, C. Characterizing intelligence gathering and control on an edge network. *ACM Trans. Internet Technol.* **2011**, *11*, 1–26.
130. Popa, L.; Yu, M.; Y. Ko, S.; Ratnasamy, S.; Stoica, I. CloudPolice: Taking access control out of the network. In Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks 2010, Monterey, CA, USA, 20–21 October 2010; p. 7, doi:10.1145/1868447.1868454.
131. Zhang, P.; Chen, Z.; Liu, J.K.; Liang, K.; Liu, H. An efficient access control scheme with outsourcing capability and attribute update for fog computing. *Future Gener. Comput. Syst.* **2018**, *78*, 753–762.
132. Fan, K.; Wang, J.; Wang, X.; Li, H.; Yang, Y. A secure and verifiable outsourced access control scheme in fog-cloud computing. *Sensors* **2017**, *17*, 1695.
133. 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.
134. Yu, Z.; Au, M.H.; Xu, Q.; Yang, R.; Han, J. Towards leakage-resilient fine-grained access control in fog computing. *Future Gener. Comput. Syst.* **2018**, *78*, 763–777.
135. Zaghdoudi, B.; Ayed, H.K.B.; Harizi, W. Generic Access Control System for Ad Hoc MCC and Fog Computing. In Proceedings of the International Conference on Cryptology and Network Security, Milan, Italy, 14–16 November 2016; pp. 400–415.
136. 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.
137. Patwary, A.A.N.; Hossain, N.; Sami, M.A. A Detection Approach for Finding Rogue Fog Node in Fog Computing Environments. *Am. J. Eng. Res.* **2019**, *8*, 2320–0847.
138. Han, H.; Sheng, B.; Tan, C.C.; Li, Q.; Lu, S. A measurement based rogue ap detection scheme. In Proceedings of the IEEE INFOCOM 2009, Rio de Janeiro, Brazil, 19–25 April 2009; pp. 1593–1601.
139. Han, H.; Sheng, B.; Tan, C.C.; Li, Q.; Lu, S. A timing-based scheme for rogue AP detection. *IEEE Trans. Parallel Distrib. Syst.* **2011**, *22*, 1912–1925.

140. Ma, L.; Teymorian, A.Y.; Cheng, X. A hybrid rogue access point protection framework for commodity Wi-Fi networks. In Proceedings of the IEEE INFOCOM 2008—The 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 1220–1228.
141. Dastjerdi, A.V.; Buyya, R. Fog computing: Helping the Internet of Things realize its potential. *Computer* **2016**, *49*, 112–116.
142. Madsen, H.; Burtschy, B.; Albeanu, G.; Popentiu-Vladicescu, F. Reliability in the utility computing era: Towards reliable fog computing. In Proceedings of the 2013 20th International Conference on Systems, Signals and Image Processing (IWSSIP), Bucharest, Romania, 7–9 July 2013; pp. 43–46.
143. Patra, P.K.; Singh, H.; Singh, G. Fault tolerance techniques and comparative implementation in cloud computing. *Int. J. Comput. Appl.* **2013**, *64*, 37–41.
144. Latchoumy, P.; Khader, P.S.A. Survey on fault tolerance in grid computing. *Int. J. Comput. Sci. Eng. Surv.* **2011**, *2*, 97.
145. Lussier, B.; Lampe, A.; Chatila, R.; Guiochet, J.; Ingrand, F.; Killijian, M.O.; Powell, D. Fault tolerance in autonomous systems: How and how much? In Proceedings of the 4th IARP-IEEE/RAS-EURON Joint Workshop on Technical Challenges for Dependable Robots in Human Environments (DRHE), Nagoya, Japan, 16–18 June 2005.
146. Bala, A.; Chana, I. Fault tolerance-challenges, techniques and implementation in cloud computing. *Int. J. Comput. Sci. Issues* **2012**, *9*, 288.
147. Wu, Y.; Song, H.; Xiong, Y.; Zheng, Z.; Zhang, Y.; Huang, G. Model defined fault tolerance in cloud. In Proceedings of the 6th Asia-Pacific Symposium on Internetware on Internetware, Hong Kong, China, 17 November 2014; pp. 116–119.
148. Latiff, M.S.A. A checkpointed league championship algorithm-based cloud scheduling scheme with secure fault tolerance responsiveness. *Appl. Soft Comput.* **2017**, *61*, 670–680.
149. Jiang, F.C.; Hsu, C.H. Fault-tolerant system design on cloud logistics by greener standbys deployment with Petri net model. *Neurocomputing* **2017**, *256*, 90–100.
150. Liu, Y.; Fieldsend, J.E.; Min, G. A framework of fog computing: Architecture, challenges, and optimization. *IEEE Access* **2017**, *5*, 25445–25454.
151. Sharma, Y.; Javadi, B.; Si, W.; Sun, D. Reliability and energy efficiency in cloud computing systems: Survey and taxonomy. *J. Netw. Comput. Appl.* **2016**, *74*, 66–85.
152. Sandhu, R.; Sohal, A.S.; Sood, S.K. Identification of malicious edge devices in fog computing environments. *Inf. Secur. J. Glob. Perspect.* **2017**, *26*, 213–228.
153. Li, Z.; Zhou, X.; Liu, Y.; Xu, H.; Miao, L. A non-cooperative differential game-based security model in fog computing. *China Commun.* **2017**, *14*, 180–189.
154. Sohal, A.S.; Sandhu, R.; Sood, S.K.; Chang, V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Comput. Secur.* **2018**, *74*, 340–354.
155. Hosseinzadeh, M.; Sinopoli, B.; Garone, E. Feasibility and detection of replay attack in networked constrained cyber-physical systems. In Proceedings of the 2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 24–27 September 2019; pp. 712–717.
156. Ahmed, M.; Pathan, A.S.K. False data injection attack (FDIA): An overview and new metrics for fair evaluation of its countermeasure. *Complex Adapt. Syst. Model.* **2020**, *8*, 1–14.
157. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.* **2011**, *14*, 1–33.
158. Tan, Y.; Sengupta, S.; Subbalakshmi, K. Analysis of coordinated denial-of-service attacks in IEEE 802.22 networks. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 890–902.
159. BBCNews. BBC, Cyber Attacks Briefly Knock out Top Sites. 2016. Available online: https://www.bbc.com/news/technology-37728015 (accessed on 13 December 2020).
160. BBC. BBC, Smart Home Devices Used as Weapons in Website Attack. 2016. Available online: https://www.bbc.com/news/av/technology-37741225 (accessed on 13 December 2020).
161. Arrington, M. In Our Inbox: Hundreds of Confidential Twitter Documents. July 2009. Available online: http://techcrunch.com/2009/07/14/in-our-inbox-hundreds-of-confidential-twitterdocuments (accessed on 15 December 2020).
162. Takahashi, D. French Hacker Who Leaked Twitter Documents to TechCrunch Is Busted. March 2010. Available online: http://venturebeat.com/2010/03/24/french-hackerwho-leaked-twitter-documents-to-techcrunch-isbusted (accessed on 15 December 2020).
163. Allen, P. Obama's Twitter Password Revealed after French Hacker Arrested for Breaking into US President's Account. March 2010. Available online: https://www.dailymail.co.uk/news/article-1260488/Barack-Obamas-Twitter-password-revealed-French-hacker-arrested.html (accessed on 16 December 2020).
164. Rocha, F.; Correia, M. Lucy in the sky without diamonds: Stealing confidential data in the cloud. In Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W), Hong Kong, China, 27–30 June 2011; pp. 129–134.
165. Pepitone, J. Dropbox's Password Nightmare Highlights Cloud Risks. June 2011 Available online: https://money.cnn.com/2011/06/22/technology/dropbox_passwords/index.htm (accessed on 16 December 2020).
166. Stolfo, S.J.; Salem, M.B.; Keromytis, A.D. Fog computing: Mitigating insider data theft attacks in the cloud. In Proceedings of the 2012 IEEE Symposium on Security and Privacy Workshops (SPW), San Francisco, CA, USA, 24–25 May 2012; pp. 125–128.

167. Wang, T.; Zhou, J.; Huang, M.; Bhuiyan, M.Z.A.; Liu, A.; Xu, W.; Xie, M. Fog-based storage technology to fight with cyber threat. *Future Gener. Comput. Syst.* **2018**, *83*, 208–218.
168. Homayoun, S.; Dehghantanha, A.; Ahmadzadeh, M.; Hashemi, S.; Khayami, R.; Choo, K.K.R.; Newton, D.E. DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer. *Future Gener. Comput. Syst.* **2019**, *90*, 94–104.
169. Hosseinpour, F.; Vahdani Amoli, P.; Plosila, J.; Hämäläinen, T.; Tenhunen, H. An Intrusion Detection System for Fog Computing and IoT based Logistic Systems using a Smart Data Approach. *Int. J. Digit. Content Technol. Its Appl.* **2016**, *10*, 34–46.
170. Alharbi, S.; Rodriguez, P.; Maharaja, R.; Iyer, P.; Bose, N.; Ye, Z. FOCUS: A fog computing-based security system for the Internet of Things. In Proceedings of the 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 12–15 January 2018; pp. 1–5.
171. Fu, A.; Yu, S.; Zhang, Y.; Wang, H.; Huang, C. NPP: A new privacy-aware public auditing scheme for cloud data sharing with group users. *IEEE Trans. Big Data* **2017**, doi:10.1109/TBDATA.2017.2701347.
172. Parkinson, S.; Qin, Y.; Khan, S.; Vallati, M. Security Auditing in the Fog. In Proceedings of the Second International Conference on Internet of Things, Data and Cloud Computing (ICC'17), Cambridge, UK, 22–23 March 2017; ACM: New York, NY, USA, 2017; pp. 191:1–191:9, doi:10.1145/3018896.3056808.
173. Kumar, S.; Negi, A.; Prasad, K.; Mahanti, A. Evaluation of network risk using attack graph based security metrics. In Proceedings of the 2016 IEEE 14th International Conference on Dependable, Autonomic and Secure Computing, 14th International Conference on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Auckland, New Zealand, 8–12 August 2016; pp. 91–93.
174. Bleikertz, S.; Schunter, M.; Probst, C.W.; Pendarakis, D.; Eriksson, K. Security audits of multi-tier virtual infrastructures in public infrastructure clouds. In Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop, Chicago, IL, USA, 4–8 October 2010; pp. 93–102.
175. Wang, C.; Chow, S.S.; Wang, Q.; Ren, K.; Lou, W. Privacy-preserving public auditing for secure cloud storage. *IEEE Trans. Comput.* **2013**, *62*, 362–375.
176. Wang, C.; Ren, K.; Lou, W.; Li, J. Toward publicly auditable secure cloud data storage services. *IEEE Netw.* **2010**, *24*, 19–24.
177. Shah, M.A.; Swaminathan, R.; Baker, M. Privacy-Preserving Audit and Extraction of Digital Contents. *IACR Cryptol. Eprint Arch.* **2008**, *2008*, 186.
178. Mohammed, L.A.; Munir, K. Secure Third Party Auditor (TPA) for Ensuring Data Integrity in Fog Computing. *Int. J. Netw. Secur. Its Appl.* **2018**, *10, 13–24* .
179. Spremic, M. Standards and frameworks for information system security auditing and assurance. In Proceedings of the World Congress on Engineering, London, UK, 6–8 July 2011; pp. 978–988.
180. Ryoo, J.; Rizvi, S.; Aiken, W.; Kissell, J. Cloud security auditing: Challenges and emerging approaches. *IEEE Secur. Priv.* **2014**, *12*, 68–74.
181. Franke, U.; Brynielsson, J. Cyber situational awareness—A systematic review of the literature. *Comput. Secur.* **2014**, *46*, 18–31.
182. Garfinkel, S.L. Digital forensics research: The next 10 years. *Digit. Investig.* **2010**, *7*, S64–S73.
183. Buchanan, W.J.; Li, S.; Asif, R. Lightweight cryptography methods. *J. Cyber Secur. Technol.* **2017**, *1*, 187–201.
184. Bogdanov, A.; Knezevic, M.; Leander, G.; Toz, D.; Varici, K.; Verbauwhede, I. Spongent: The design space of lightweight cryptographic hashing. *IEEE Trans. Comput.* **2012**, *62*, 2041–2053.
185. Hirose, S.; Ideguchi, K.; Kuwakado, H.; Owada, T.; Preneel, B.; Yoshida, H. A lightweight 256-bit hash function for hardware and low-end devices: lesamnta-LW. In Proceedings of the International Conference on Information Security and Cryptology, Shanghai, China, 20–24 October 2010; pp. 151–168.
186. Guo, J.; Peyrin, T.; Poschmann, A. The PHOTON family of lightweight hash functions. In Proceedings of the Annual Cryptology Conference, Barbara, CA, USA, 14–18 August 2011; pp. 222–239.
187. Zyskind, G.; Nathan, O. Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the 2015 IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, 21–22 May 2015; pp. 180–184.
188. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*; Technical Report; Manubot: 2019. Available online: https://git.dhimmel.com/bitcoin-whitepaper/ (accessed on 10 October 2019).
189. Botezatu, B. How Blockchain Can Improve Internet of Things Security. 2018. Available online: http://aiweb.techfak.uni-bielefeld.de/content/bworld-robot-control-software/ (accessed on 19 November 2019).
190. Antunes, H. Blockchain and Fog: Made for Each Other. 2018. Available online: https://blogs.cisco.com/innovation/blockchain-and-Fog-made-for-each-other (accessed on 25 November 2019).
191. Dickson, B. How Blockchain Can Improve Cybersecurity. 2017. Available online: https://bdtechtalks.com/2017/01/11/how-blockchain-can-improve-cybersecurity/ (accessed on 24 April 2020).
192. Momot, A. How Blockchain Can Be Used to Dramatically Improve Cybersecurity. 2018. Available online: https://cybersecurityventures.com/how-blockchain-can-be-used-to-improve-cybersecurity/ (accessed on 25 April 2020).
193. Parker, M. Four Ways to Improve the Security of Blockchain. 2017. Available online: https://securitycurrent.com/four-ways-improve-security-blockchain/ (accessed on 25 April 2020).
194. Rubens, P. Security Applications of Blockchain. 2017. Available online: https://www.esecurityplanet.com/network-security/blockchain-security.html (accessed on 25 April 2020).

195. Mehdipour, F.; Javadi, B.; Mahanti, A.; Ramirez-Prado, G.; Principles, E. Fog computing realization for big data analytics. In *Fog and Edge Computing: Principles and Paradigms*; Wiley: Hoboken, NJ, USA, 2019; pp. 259–290.
196. Tuli, S.; Mahmud, R.; Tuli, S.; Buyya, R. FogBus: A Blockchain-based Lightweight Framework for Edge and Fog Computing. *arXiv* **2018**, arXiv:1811.11978.
197. Sharma, P.K.; Chen, M.Y.; Park, J.H. A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE Access* **2018**, *6*, 115–124.
198. Jeong, J.W.; Kim, B.Y.; Jang, J.W. Security and Device Control Method for Fog Computer using Blockchain. In Proceedings of the 2018 International Conference on Information Science and System, Seville, Spain, 18–20 September 2018; pp. 234–238.
199. Samaniego, M.; Deters, R. Using blockchain to push software-defined IoT components onto edge hosts. In Proceedings of the International Conference on Big Data and Advanced Wireless Technologies, Blagoevgrad, Bulgaria, 10–11 November 2016; p. 58.
200. Dorri, A.; Kanhere, S.S.; Jurdak, R. Blockchain in internet of things: challenges and solutions. *arXiv* **2016**, arXiv:1608.05187.
201. *5G Security: Forward Thinking Huawei White Paper*; Huawei, China 2015; Available online: https://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf (accessed on 18 November 2020). .