Journal of Theoretical and Applied Information Technology
31st January 2021. Vol.99. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FOG COMPUTING ARCHITECTURE, BENEFITS, SECURITY, AND PRIVACY, FOR THE INTERNET OF THING APPLICATIONS: AN OVERVIEW

YEHIA IBRAHIM ALZOUBI[1], AHMAD AL-AHMAD [2], ASHRAF JARADAT[3], AND VALMIRA H. OSMANAJ [4]

[1,2,3] and [4] Management Information Systems Department, College of Business Administration, American University of the Middle East, Kuwait

E-mail: [1]yehia.alzoubi@aum.edu.kw,[2]ahmad.alahmad@aum.edu.kw, [3] ashraf.jaradat@aum.edu.kw, [4]valmira.osmanaj@aum.edu.kw

ABSTRACT

To overcome the problem related to cloud computing such as high latency and to increase the efficiency of data processing, Fog computing was proposed and implemented close to IoT devices. This structure helps these devices to meet the requirements of location awareness and low latency, which can not be met by cloud computing. Many benefits, applications, and security and privacy issues were discussed in the literature for Fog computing. This paper provides an overview of all these aspects to provide the reader with a holistic understanding of Fog computing. More focus is given to the security and privacy issues in our discussion since these issues may hinder organizations from implementing Fog computing. The findings of this paper show that a few studies that discussed empirical findings of using Fog computing and many questions related to security and privacy issues are ye to be answered in future research.

Keywords: *Fog computing, IoT, Benefit, Application, Security*

1. INTRODUCTION

IoT devices and applications are dominant, currently, in different industries, homes, and smart cities[1, 2]. Due to the large number, the amount of data produced from these devices is huge and heterogeneous which needs a high-speed internet, massive storage, powerful computing resources [3, 4]. Cisco, in 2012, proposed the concept of Fog computing (FC) [5, 6]. The idea behind FC was to enhance the computing processes for the resources-constrained IoT devices and storing the data sent by these devices [2, 7]. Furthermore, Fog also supposed to mitigate the problems of Cloud computing in shortening the response time, complexity of the distributed nature of the IoT devices, mobility, and location awareness of IoT applications [8-11].

FC can be defined as "an end-to-end horizontal architecture that distributes computing, storage, control, and networking functions closer to users along the Cloud-to-thing continuum" [12]. FC acts as a bridge between IoT devices and Cloud computing. FC is an extension to the Cloud towards the end-users' devices (edge of the network) [13, 14]. Fog node conducts control, communication, and computation on behalf of the Cloud. It also provides storage close to the end-users [15, 16]. Since Fog nodes are geographically distributed and close to user's devices, the communication time with the Cloud and bandwidth is greatly reduced [13, 14]. Therefore, Fog may achieve real-time applications reqyuirements and network bandwidth bottlenecks [17, 18]. However, due to limited storage capacity and computation power, FC cannot replace Cloud computing. Moreover, the probability of facing attacks will be higher in the Fog comparing to the Cloud with super computation and well-established security measures [19, 20].

Since Fog has its own nature and characteristics, solutions applied for security and privacy-preserving in the Cloud can not be applied with the same effectiveness, or they may not be doable in the Fog [11, 15]. As a result, FC should have its own tools and techniques to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

maintain the privacy and security of IoT devices connected to it [1, 21, 22]. The main aim of this paper is to answer the following research question.

What are the benifts of Fog Computing?

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

The contribution of this paper is by providing an overview of the benefits, architecture, and security and privacy issues of FC. Moreover, this paper provides an overview of proposed techniques and tools to be used to enhance Fog security and privacy. Many papers have been published during the last 4 years discussing the issues of privacy and security in the FC environment. Recently, the focus was on using blockchain technology in order to address many of these issues (e.g., authentication, Trust, and privacy) [2, 4].

The rest of this paper is organized as follows. Section 2 discusses the research methodology. Section 3 presents the FC architecture. Section 4 presents an overview of the benefits and applications of FC. Section 5 discusses the state-of-the-art of privacy and security challenges due to the use of FC. Section 6 discusses the future research direstions and the limitation of the paper. Section 7 concludes this paper.

2. RESEARCH METHODOLOGY

This paper reviewed the available literature that describes the architecture, benefits, and security and privacy issues of FC. We did not consider any database or journal. The search was done using the Google Scholar engine. We used the combination of the key search words; fog computing, benefits, architecture, security, privacy. We used the Boolean "AND" and "OR" between these words such as "fog computing" AND "benefits" OR "architecture" OR "security" OR "privacy". This procedure resulted in 100 papers. After going manually, through each selected paper, 30 papers were excluded from further analysis due to abstracts or contents that did not meet our paper aim. Table 1 summarizes the paper selected papers for this review.

Table 1. Selected Studies

Focus	Study
Fog security and privacy	[1, 2, 5, 6, 9, 13, 14, 18-52]
Fog benefits	[3, 7, 8, 12, 15, 18, 50, 53-57]
Fog architecture	[8, 17, 18, 53, 58-64]

3. FOG COMPUTING ARCHITECTURE

The reviewed literature identified five types of Fog nodes with their configurations as listed below [26]:

- Servers: Their capabilities are high and they are deployed in common places such as shopping centers and parks.
- Networking devices: The function of these devices includes routing, packet forwarding, and analog-to-digital signal conversions. Some examples of these devices are gateways, routers, and switches as they can be a potential infrastructure of FC.
- Cloudlets: They are considered as micro-Cloud that are located in the Fog layer (i.e., Fog nodes) and designed to extend Cloud services towards IoT devices.
- Base stations: They can be used as Fog nodes if they are equipped with required storage and computing power.
- Vehicles: Parked or moving vehicles can serve as Fog nodes if they are equipped with some computation capabilities.

Fog architecture, in general, compromises three layers; device layer, Fog layer, and Cloud layer. These layers are connected with public authorities such as key generation center and certificate authority [17]. The three layers are defined as follows.

Device layer: This is the closest layer to the end-users. This layer includes all IoT devices (mobile or static) such as mobile phones, smart vehicles, card readers, sensors, and so on. In general, these devices are geographically distributed and have low computation capabilities and limited storage resources [27].

Fog layer: It is the middle layer between the device layer and the Cloud layer, but it is located close to the device layer. It is composed

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of a large distributed number of Fog nodes [25]. The layer extends the Cloud layer by providing many services such as real-time analysis to IoT devices data, temporarily storing, and transmitting a summary of the IoT devices data to the Cloud [27]. These services help in reducing the processing load of IoT devices [25]. Fog nodes play an intermediate role between the cloud and IoT devices.

Cloud layer: The Cloud layer involves the high-performance servers and permanent storage of data. Many services are provided by the Cloud layer such as transportation and power distribution applications [19]. This layer also provides a complex analysis that can be done remotely and at any time. Moreover, the cloud provides the Fog with control strategies and policies that help in enhancing the quality of latency-sensitive services offered by Fog nodes [26].

4. FOG COMPUTING BENEFITS AND APPLICATIONS

Many applications, specifically the latency-sensitive ones, can gain several benefits by distributing FC close to IoT devices. Some of these benefits, which were reported in the literature, are summarized as follows [28, 53].

- Reduces latency: Fog enables real-time analysis and data processing, and support time-sensitive control local cyber-physical systems.
- Supports cognition: Being close to IoT devices, FC can provide better awareness of user's requirements. It will be better to determine where to carry out computing, control, and storage processes.
- Enhances agility: Fog helps in conducting faster innovation (e.g., experiment and create) and affordable scaling (e.g., develop and use new services) as it deals with IoT devices directly without the need to wait for the large network Cloud vendors.
- Enhances efficiency: Since Fog is distributed with location and resources (i.e. computing, control, and storage), it can take full advantage of the available resources along with the distribution. It also helps applications leveraging from resources available on network and IoT devices such as routers and databases. The closer is Fog to the IoT devices, the better integration with IoT systems, which enhances the overall system performance and efficiency.
- Improves security: Although Fog creates new security challenges, it enhances the overall security. That is less chances of eavesdropping as the information traverse less distance.
- Saves bandwidth: Since FC extends processing computation (e.g., data pre-processing and cleaning) and storage that will be done locally in Fog, less data will be transmitted to the Cloud. This will save internet bandwidth.
- Supports mobility: The distributed nature of Fog will support mobile devices such as smartphones and vehicles which change their places very often. Fog nodes (e.g., using routing and addressing protocol) can interact directly with IoT devices. Also, various mobile devices can directly communicate with each other without the need to be sent to Cloud or even base station. This enables IoT devices to process the data generated from other IoT devices.
- Enables geographical distribution and decentralized data analytic: The distributed nature of the Fog nodes between the IoT and the Cloud enables IoT location tracking without the need for the Cloud.
- Promotes Heterogeneity: Fog nodes involve a wide range of devices such as servers, routers, gateways, base stations, and access points. These devices provide wide services with different levels of applications, storage, and processing capabilities. Moreover, Fog is a virtualized platform, so some virtual nodes can be used as Fog nodes, which indicates the heterogeneity nature of Fog nodes.
- Supports Interoperability: The devices used in Fog node may come from different providers and deployment in various environments, FC should provide the cababilty of working with different provides and different network requirements.
- Enhances low energy consumption: Fog nodes will not generate a lot of heat due to

its distributed nature. Moreover, deploying some optimal energy policy in IoT devices, in this short-range communication, will reduce communication energy consumption. As a result, power consumption and cost will be reduced.

In general, FC is suitable for applications that need instant response and feedback. Therefore, FC would be helpful in any application that is latency-sensitive, such as smart environment, smart transportations, intelligent surveillance, water pressure at the dams, self-maintaining trains, smart traffic signals, wireless sensors and actuator networks (WSAN), 5G mobile networks, brain-machines, energy grids, disaster support applications, urgent services, health systems, video streaming, gaming, and augmented reality [29].

5. SECURITY AND PRIVACY ISSUES OF FOG COMPUTING

Due to the unique nature of the FC, it has its own security and privacy issues as well as the issues that inherited from cloud computing. Therefore, the solutions that usually used in the cloud will not be applicable in the FC [31]. These challenges as well as the proposed and recommended solutions are discussed as follows. Table 2 summarize the future recommendations and solutions.

Table 2. Fog Computing Security and Privacy Recommendations and Future Opportunities

Challenge	Recommendations/ Practices	Future Opportunities
Authentication	• Deploy cooperative authentication and other collaborative authentication approaches of Fog nodes to achieve the latency requirement for real time services and support the users' mobility [26]. • Consider a trusted third party node distributed next to each Fog node [30]. • A lightweight end-to-end authentication [21]. • Deploy advanced cryptographic mechanisms that does not depend on central authority and, possibly, in the presence of untrustworthy entities [32]. • Blockchain technique [33]. • Consider the functions of anonymity, integrity, traceability, and batch authentication, while implementing lightweight authentication [34]. • Deploy a key agreement protocols among Fog network [21].	• Design a distributed authentication mechanisms [35]. • Consider an identification and authentication of world-wide infrastructure members of interconnected Fog data centers owned by different companies and individuals [35]. • Design new authentication and trust mechanisms that address heterogeneity of Fog nodes and IoT nodes [53]. • Explore authentication enforcement approaches [34]. • Design cross-domain authentication and handover authentication techniques between the same entities in different trust domain [34]. • Design identification and mutual authentication mechanisms of different entities in the same trust domain [34]. • How to achieve a scalable authentication in Fog computing-based radio access network? [21].
Access Control	• Use Fog servers to support multi-layer access control technique [65, 66]. • Use fine-grained access control in each trusted domain [28]. • Deploy authorization infrastructure in every trust domain [35]. • Consider the inter group and hierarchical fine-grained access control system which support the extension from a single domain to multi domains [34]. • Deploy Policy-driven security management framework including policy analysis [38].	• Design robust access control techniques that support secure collaboration and interoperability between heterogeneous resources in Fog environment [60]. • Address a sophisticated way to detect policy conflicts and resolve the detected conflicts [38]. • Design a distributed access control mechanism [26]. • Cross-domain access control such as access conflict, unauthorized access, policy management, user-level management, and attribute management need to be addressed in future research [21].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Lightweight Protocol Design		• Design authentication protocols of different vendors/operators [53]. • Design lightweight protocols to support real-time services for Fog-assisted IoT applications [26].
Detection Systems	• Tools like CLOUDWATCHER for partial network monitoring by selecting specific devices and PAYLESS for scanning SDN communication with minimal computing resources [66]. • Ensure the balance between local and global defense mechanisms [26]. • All defense mechanisms should be able to exchange information with each other [35]. • The defense mechanisms should behave autonomously to reduce the maintenance overhead and improve the usability of the security infrastructure [35].	• Design Fog systems that consider the potential of underlying operating system [66]. • Design detection systems that coordinate different detection components [21]. • Design global monitoring infrastructure that involves multiple layers and/or trust domains [35]. • Build high-security and low-cost collusion attack detection systems [39].
Trust Management	• Deploy Blockchain technique [5, 32]. • Deploy Fog-based middleware, such that a trust agent estimates the interpersonal trust between a Fog node and the Cloud [39].	• How to achieve decentralized, situation-aware, scalable and consistent trust management mechanisms? [26]. • How to achieve persistent, unique, and distinct identity? How to treat intentional and accidental misbehaviour? How to conduct punishment and redemption of reputation [40].
Packet Forwarding		• How to prevent the privacy leakage against intermediate Fog nodes during packet forwarding? [26].
Malicious Fog Node	• Deploy strong access-control policies for Fog nodes [53].	• Design new methods to detect the rogue and corrupted Fog nodes [26]. • Design physical secure Fog nodes [53]. • Design secure hardware, safe against physical damage, jamming, etc. [53].
Virtualization	• Prevent honest-but-curious service providers to access to or modify the results of the virtualized services [32]. • Consider geographical location and the resource ownership policies, such as migrating virtual machines might be allowed to use additional resources from the virtualization infrastructure if they hold certain privileges [35]. • Apply network isolation among tenants in the virtualization infrastructure [35]. • Ensure that virtualized services can access only the data they are entitled to [32].	• Develop and provide a set of security mechanisms to validate the correct deployment, operation and migration of virtualized services [32].
Fault Tolerance	• Consider using hybrid failure handling method [61]. • Developers should incorporate redundant replications and user-transparent, fault-tolerant deployment, and execution techniques in orchestration design [67].	• Design novel methods for avoiding the unnecessary resource consumption and offer sufficient caching capabilities [39]. • More research is needed [41].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Data identification, Aggregation and Integrity	• Identify and protect sensitive data mechanisms to prevent information leakage for users [26]. • Deploy multi-Key homomorphic signature for data aggregation [26]. • Deploy integrity verification, minimum overhead, public auditing, and dynamics support mechanisms [28]. • Consider backup and recovery mechanisms [66].	• Design secure and private offloading and load balancing schemes [53]. • Design secure and efficient provable data possession protocols to guarantee the data integrity [26]. • The research of data integrity should focus on batch auditing, dynamic auditing, privacy preserving, and Low complexity [34].
Data Distribution	• Enable users to make decisions on data sharing [32]. • Deploy the social network for service sharing in the Fog [39].	• How to achieve fine-grained data sharing scheme to realize fine-grained data access in Fog computing? Without such a scheme, many real-time applications may be blocked [26]. • Provide a mechanism to securely exchange information across the Fog [32].
Content Distribution	• Deploy Blockchain technique [42].	• Investigate approaches to achieve secure service discovery and anonymous broadcast encryption simultaneously [26].
Data Protection and Search	• Provide dynamics support and refined result [28].	• How to build a secure keyword search scheme in Fog environment with distributed nature? [34]. • How to build efficient security index that is suitable for resource-constrained devices? [34]. • How to design a distributed searchable encryption algorithm? [34].
Big Data Analysis		• How to design decentralized big data analysis with differential privacy in Fog computing? [26].
Verifiable Computation	• Confidentiality of inputs, outputs and computing tasks, and the verifiability of outputs [28].	• Design a mechanism for receivers to verify the correctness and integrity of the offloaded task [53]. • How to build a secure verifiable computing among different trust domain? [39]. • How to design practical publicly verifiable computation schemes suitable for IoT applications in Fog computing? [26].
Aided Computation		• How can Fog nodes assist IoT devices to perform aided computation tasks to satisfy different features and goals in IoT applications? [26] • How to build a scalable, efficient and decentralized secure infrastructure is challenging but important for the healthy development of Fog computing [26].
Forensics		• How to design a management of evidence system with the existence of multiple actors, infrastructures, technologies, and scenarios? [35]. • More research is needed [41]. • More effective solutions should be provided [68].
Data privacy	• Deploy anonymity system between different Fog nodes layers (mix-based protocol) [30].	• Design a solution that ensures the usage of distributed resources minimizes the disclosing of private information [40].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

	• Enable the users to determine the most suitable mechanism to protect, query, and process their data [32, 35]. • Fog should offer contextual information to the IoT devices to facilitate the application of some privacy techniques, like k-anonymity [32]. • Utilize the collaboration between Fog data centers and Cloud data centers to decrease the complexity of the cryptographic algorithm [34].	• Preserving data privacy issue needs more research [26]. • Design lightweight, dynamic, and distributed secure data storage system based on several functional encryption methods [34].
Identity privacy	• Deploy anonymous and stateless process like STAMP which keep user's location and identity private, even from the Fog network [66]. • Define some levels of privacy protection in data combination [26].	• Design new effective privacy-preservation methods [33]. • Develop mechanisms that allow IoT users to identify their own privacy requirements as well as enforcement mechanism [32]. • Develop mechanisms to identify the misbehaved users [35]. • Design dynamic fine-grained identity privacy-preservation scheme [34].
Location privacy	• Deploy a mobility management service that handle changes of users and Fog devices' locations [44]. • Use anonymity system between the Fog nodes layer and upper layers of the Fog architecture [30].	• Design dynamic fine-grained location privacy-preserving scheme [34]. • Global and local location privacy need more research [69].
Usage privacy	• Use anonymity systems [33].	• Design a smart way of partitioning the application that ensures the offloaded resource usages do not disclose privacy information [40].

5.1. Authentication

Authentication is considered as the main security issue of FC. This is because the Fog offers different services to a huge number of IoT devices. Authentication should be applied at different levels during communication between Fog nodes and IoT devices [35]. Traditional authentication techniques such as public key infrastructure (PKI) and certificates will not be effective due to the resource-constrained IoT devices (e.g., power, storage, and processing) [35]. Hence, new authentication techniques have been proposed like identity, Decoy, anonymous, and cooperative, single-domain, cross-domain, and handover authentication [26].

5.2. Access Control

To ensure security and achieve IoT device privacy, access control is used. Cryptographically implemented traditional access control techniques such as symmetric key-based techniques are not suitable for Fog environment [53]. Hence, new solutions were proposed to suit the nature of the Fog. For example, attribute-based encryption (ABE) access control was suggested [35]. Fine-grained access control was suggested by many authors [46]. A policy-driven management framework in order to achieve effective access control in the Fog environment was also suggested [6]. Also, leakage-resilient functional encryption schemes, device management, and key management are proposed [26, 53].

5.3. Light-Weight Protocol Design

Lightweight protocols are designed to improve the real-time service performance by decreasing the communication between the IoT devices and Fog nodes. Various lightweight cryptographic schemes and techniques were proposed to address this issue; including the elliptic curve cryptosystem [26], masking techniques,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

encryption algorithms, hash functions, and stream chippers for secure end-to-end communication [5].

5.4. Detection Systems

Various techniques are used to detect intrusion in the Cloud system and lessen the impact of insider attacks, flooding attacks, port scanning, and attacks on the VM and hypervisor [25]. Authors have proposed Fog IDS which are signature-based, artificial intelligence (AI) based, neural network-based, association rule-based, fuzzy logic and support vector machine-based, lightweight countermeasure utilizing bloom filters and host-based, network, and distributed detection systems [26, 41, 53].

5.5. Trust Management

Trust is managed differently in FC, compared to Cloud computing, where Cloud is considered semi-trusted and the underlying protocol is faithfully executed. In the case of FC, the Fog nodes may become effortlessly fraudulent; therefore they may initiate an active attack at any moment [28]. The proposed trust management solution in the Fog environment includes Trusted Execution Environment (TEE), Region-Based Trust-Aware (RBTA), self-managed trust management system, quantitative trust management component, and Bayesian network-based trust model, evidence-based trust model, monitoring-based trust model, and reputation management, and trusted distributed platform over the edge devices [26, 35].

5.6. Packet Forwarding

To maintain the privacy of the packet sent between two Fog nodes themselves or between Fog and IoT devices, it should be ensured that the features of the sent packet are maintained. However, due to the limited resources of Fog, this may represent a challenge [35]. End-to-end connectivity requires the cooperation of other nodes to enable message delivery and privacy-preserving packet forwarding should be used [26].

5.7. Malicious Fog Node

One of the main challenges of FC is the existence of fake Fog nodes, which will be a big threat to data security and privacy. In order to avoid this, it was proposed to deploy fake node detection systems and trust-based routing mechanisms [5]. Moreover, creating and deleting virtual machine instances in a dynamic way complicates the process of maintaining a blacklist of rogue nodes [47]. Additional issues like scalability, message overhead, and slow convergence might appear [5].

5.8. Virtualization

Virtualization is a key feature of FC. It creates isolated environments in FC to guarantee the smooth functioning of the Fog system and affects the Fog node performance [39]. For the purpose of launching attacks, a lack of security measures will enable VM to manipulate the services of the Fog, take control of the underlying hardware and operating system. Several solutions have been proposed like implementing policies for isolation, virtual machine monitoring, network abstraction, hardening the hypervisor, multi-factor authentication, installation of detection systems at host and network, user-based permissions model, and private networks and process [35, 41, 66].

5.9. Fault Tolerance

Like any other paradigm, Fog may not be implemented to be completely secure and exempt from all the threats. Malicious adversaries may disable or take control over some of the Fog nodes or the entire infrastructure, due to outdated software, vulnerabilities, misconfigurations, and other faults. Therefore, integrating different strategies and mechanisms as well as the deployment of a proactive fault-tolerance method is essential [35, 61]. Moreover, sometimes, the replacement will not be possible as the services are delivered at a local context [35]. The proactive fault tolerance technique can be used as a solution in the Fog environment to offer a high failure prediction accuracy [61].

5.10. Data Identification, Aggregation and Integrity

In FC, the IoT device user should be able to verify the correctness and integrity of the stored data in the Cloud. To achieve this, an agreement should exist between the end-user and the Cloud. The validity and integrity of data should be checked by the Cloud as data come from different Fog nodes. Otherwise, if the received data are not accurate, any security and auditing measures deployed on the data storage system would not be successful [28]. Authors have proposed various mechanisms to ensure data integrity such as Trusted Platform Module (TPM), homomorphic encryption, one-way entrance permutation, key distribution, and a combination of homomorphic,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

searchable, symmetric, and asymmetric encryption [5, 26].

5.11. Data Distribution

In the Cloud, the creator of the data can share them with other users. Some techniques were proposed in the literature to ensure secure sharing of the data over the Cloud like attribute-based encryption. Through such a technique, the creator of the data can encrypt the data before sharing them over the Cloud. The case; however, is different for the Fog. This is because the ciphertexts will not stay the same after received by the Fog nodes. Unlike Cloud Computing, the shared data in FC is not the same as created originally data; rather it is processed data the Fog nodes [26]. Some solutions were provided in the literature like fine-grained access control, authorization revocation, proxy re-encryption, and attribute-based and key-aggregate encryptions [28].

5.12. Data Protection and Search

End-users should be able to retrieve part of the data being stored in the Cloud by using particular keywords. Since the encrypted data may not be searchable due to the applied encryption scheme, other mechanisms like searchable encryption need to be used that enables Cloud to search the encrypted data without illuminating the underlying keywords [35]. Unfortunately, these techniques will not work in FC since the data stored in the Cloud are retrieved from the Fog nodes after being processed. Consequently, they are not the same as the original data from the end-user. Guan, et al. [28] suggest that any searchable storage mechanism in FC should be able to maintain the confidentiality of the queried data and the underlying keywords, comply with the dynamics of FC, and protect data privacy, especially for the end-users sensitive data.

Some of the recommended data protection and search techniques include a combination of homomorphic encryption and searchable encryption, symmetric and asymmetric searchable encryption, secure ranked keyword search scheme, attribute-based keyword search scheme, dynamic search method, proxy re-encryption with keyword search approach, hybrid key and data encryption schema used for single keyword search [35].

5.13. Content Distribution

In order to safeguard the content distribution service from information leakage, cutting-edge mechanisms are proposed. One of the solutions proposed is a secure discovery scheme to identify authorized users prior to content discovery [5]. Furthermore, a broadcast encryption scheme was proposed by delivering encrypted information at the broadcast channel [28]. A decentralized computing mechanism should be deployed to protect the privacy of the data at the Fog node level and secure the data from malicious attacks was also proposed [5]. A verifiable computational scheme that utilizes a content-based encryption mechanism. Another solution proposed is a model designed for dynamic computation in the Fog environment [28].

5.14. Big Data Analysis

Fog nodes collect an enormous amount of data from different sources in order to store and analyze them using advanced analysis techniques [3]. As a result, the IoT users may be subject to privacy infringements, while their personal data are being used for analysis, and the applied tools may extract sensitive information [5]. Thus it is crucial to implement advanced security systems in order to secure users' data privacy and analyzed data instantaneously. Fully homomorphic encryption and Cloud-aided privacy-preserving frequent itemset mining scheme were proposed for vertically divided databases [26]. As it utilizes randomized and re-encrypted keys to restrict control on privacy settings and on trust while sharing the data in the Cloud. To protect the privacy and query process of the outsourced databases, Hilbert curve-based cryptographic transformation technique is suggested [5]. The privacy-aware query authentication process is applied to ensure data confidentiality along with query result integrity.

5.15. Aided Computation

Through the data computation service, the data owner is able to outsource the computing tasks and the corresponding input data to the Cloud. The Cloud will process the data and return the results to the data owner. A successful and efficient deployment of this service should guarantee the confidentiality of computing tasks, input data and output data, and the data owner should be able to verify the validity of the received output. Some of the proposed solutions to attain secure data computation service in Cloud computing include server aided exponentiation, verification, encryption, function evaluation, and key exchange [26].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5.16. Verifiable Computation

The concept of verifiable computation was formally introduced by Gennaro, et al. [48]. In their work, they reported that the ability of computing devices to offload the computation of a function to other servers (e.g., Fog nodes) to analyze and return some correct computation. In order to encourage the offload of the computation to the Fog node, the end-user should be able to verify the accuracy of the computation. To address this issue, Gennaro, et al. [48] suggested using a protocol for verification. This protocol allows the server to return a non-interactive proof that can be verified by the client. This solution can provide input and output privacy for the client, at no additional cost. Another solution is the 'Pinocchio' system. This sytem enables the user to verify the computations done by a server using cryptographic assumptions [35]. So, using this system, the client can creat an evaluation key that describes the computation and the server. Then, it evaluates the computation and uses the evaluation key to produce a proof of accuracy. A Combination of homomorphic encryption and searchable encryption can be used in Fog for verifiable computation purposes [40].

5.17. Forensics

Various challenges can face digital forensics based on the environment where they are applied (i.e., Cloud or Fog). In the Fog environment, there are more log records which make it harder to acquire the log data from Fog nodes [68]. In order to address this issue in the Fog, some authors recommend keeping tracking of changes in data location among regions using Mobility Service (MS) and Location Register Database (LRD) [35]. Fog forensics are subject to some limitations like the need for international legislation, jurisdictions, and application-level logging [21, 23]. Moreover, storing trusted evidence in a distributed ecosystem with multiple trust domains is required, which requires more resources and computational processing power [24, 35].

5.18. Data Privacy

The privacy-preserving algorithms usually are executed among the Fog and the Cloud, excluding the end-user devices. Since the IoT devices share sensitive data collected by sensors and local devices, homomorphic encryption is used to enable the privacy-preserving aggregation of the encrypted data at the local gateways. In the case of the statistical queries, the differential privacy technique is employed to protect the privacy of any single data entry in the data set [40, 70]. Comparing to Cloud computing, Fog networks are more vulnerable in terms of data privacy risks. The vulnerability is observed due to two main reasons. First, Fog nodes are closer to the customer, which allows gathering more sensitive information from them. Secondly, computing the customer data is outsourced to the Fog node, which might collect data from IoT services and relate them to the real identities of the clients [30]. Several solutions have been suggested in the literature to reserve the privacy of data in Fog environment like masking technique or lightweight encryption algorithms, Home-Area Network (HAN), identity obstruction techniques, differential and homomorphic techniques, identity-based and attribute-based encryptions, and proxy re-encryption [40, 71].

5.19. Identity Privacy

The transitional Fog nodes forward packets received from IoT devices or other Fog nodes to the other Fog nodes or to the Cloud. So, Fog node must not know about the personal information of the users. To protect users' information, anonymity and encryption techniques are required to hide the identities of the users. Various solutions have been proposed to preserve identity privacy. One of these solutions is the pseudonym technique which was recommended by Tariq, et al. [5]. Another solution proposed by Prakash et al. [71] is by using the HAN encryption methods.

5.20. Location Privacy

One of the most important models for privacy is location privacy. Location, trajectory, and even mobility habits should not be discovered by the adversaries, especially due to the fact that the users send their tasks to the nearest Fog nodes. Mukherjee, et al. [21] explored how an adversary can disclose the user's behaviors by analyzing his/her usage of Fog services. For example, smart meters' readings may disclose information on the time that there is no one in the house or the favorite TV shows of the user. One of the solutions to preserve the privacy of the IoT device location is identity obfuscation [40]; a technique that prevents the Fog node from learning the Fog client identity, regardless of their vicinity. Identity obfuscation may be deployed using different methods, such as using a third party to generate a fake ID for every end-user. Another alternative solution to the location privacy threats is the

secure homomorphic protocol for fast data encryption and decryption [53].

5.21. Usage Privacy

Based on the location of the sender and receiver, the Fog nodes may realize the existed relationship between them, identify the senders, and analyze the users' mobility patterns. Therefore, it can guess the occupations, workplace, address, and intimacy, for example. Accordingly, it's fundamental to prevent privacy leakage against intermediate Fog nodes during packet forwarding [26]. Kumar, et al. [49] claim that identity obstruction techniques may be used to prevail in the privacy issue usage. Another possible solution to tackle usage privacy threats, caused by smart metering, is having the Fog client creating dummy tasks and offloads them to multiple Fog nodes to hide the real tasks among the dummy ones [40].

6. DISCUSSION

6.1. Open Research Issues

Unlike Cloud computing that is protected by Cloud providers, security and privacy solutions applied to Cloud computing cannot be easily extended to FC [21]. Furthermore, the solutions provided by literature to protect the Fog environment have oversimplified the real ecosystem nature of FC which consider the Fog environment as a single Cloud provider) [26]. Fog environment involves multiple interacting service providers, services, and infrastructures that belong to different trust domains [32]. Therefore, innovative solutions are required to meet the security and privacy-preserving requirements for the Fog environment. The following are the open research challenges related to FC security and privacy issues that require further future research.

1) Authentication: Authentication is one of the significant uncertainties in Fog computing since Fog node acts as controller and data accumulation points. user-level key supervision and update mechanisms in a Fog storage framework is a very critical task to aid fine-grained access control [53].
2) Trust management: Trust should be created between the IoT devices and the Fog nodes as well as between different Fog nodes in the FC environment. This makes building such trust an important task [72].
3) Detection Systems: It is critical to implement edge detection systems that integrate the different detection components [35].
4) Fog Forensic: It is essential to deploy cross-border legislation issues in the FC environment [73].
5) Dynamic Join and Leave Fog Node: There is a critical need to create an authentication scheme whenever an IoT device leaves one fog node and join another or when a Fog node leaves the Fog layer. This scheme should be of low complexity. Moreover, the system should be able to identify the misbehaved IoT device [37, 74].
6) Privacy Preservation: IoT device identity, location, data, and the resources shared with other IoT devices should be preserved [20].
7) Data Storage: After processing by the Fog node process, data will be unrecognized by the data owner. Therefore, integrity verification, public auditing, and dynamic support are essential to overcome this issue [26].
8) Data distribution: Access control will be changed after processing the data by the Fog Node. Therefore, authorization revocation, access efficiency, and fine-grained access control are all required to deal with this challenge when sharing the data [37].
9) Data search: The keywords of searching the data after processing by the Fog node. Therefore, secure searchability, refined result, and dynamics support are all required to enable data search of the processed data [31].
10) Computation: The data association and computation functions will be changed after processing by the Fog node. Therefore, verifiability of outputs, the privacy of inputs, outputs, and computing tasks are all required to enable secure computation [31].

5.2. Limitations

Like other review studies, this paper has some limitations. One of the limitations was access to the paper published. This paper was extracted data from papers that were published in a common database and written in English. So, the none-English written papers were not included in this review. Moreover, several recently published papers were not accessible in the related database. This may result in not including other security and privacy factors related to security and privacy issues of FC. Another point that may represent a limitation of this paper is that FC is a new research theme. That is, many papers are published in this field every week. This also may impact the findings of this paper as many papers would be published in the period between writing this paper and publish it.

7. CONCLUSIONS AND FUTURE DIRECTIONS

In this paper, we provide an overview of the benefits and applications of FC. It also provides an overview of Fog security and privacy issues as well as the proposed solutions. This paper identified 21 security and privacy issues of FC. Most of these issues have not solved yet. This is due to the fact that most of these solutions were exported from Cloud computing literature. The problem here is that FC extends the Cloud, but it has its own characteristics that make it different from the Cloud like the distribution nature, the limited resources, and the mobility of the IoT devices it serves.

Therefore, more research is yet to be conducted in this field. Moreover, future research may study the security and privacy issues of using Fog among different applications to establish a clearer understanding of these issues and their solutions. FC is stil in its early stage. Yet, many questions are yet to be answered about security and privacy of FC. The findings of this paper guide researchers and practitioners to shed more light on studying and designing new solutions to enhance the security and privacy of FC.

REFERENCES

[1] X. Shen, L. Zhu, C. Xu, K. Sharif, and R. Lu, "A privacy-preserving data aggregation scheme for dynamic groups in fog computing," *Information Sciences,* vol. 514, pp. 118-130, 2020.

[2] X. Huang, D. Ye, R. Yu, and L. Shu, "Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design," *IEEE/CAA Journal of Automatica Sinica,* vol. 7, pp. 426-441, 2020.

[3] A. Yassine, S. Singh, M. S. Hossain, and G. Muhammad, "IoT big data analytics for smart homes with fog and cloud computing," *Future Generation Computer Systems,* vol. 91, pp. 563-573, 2019.

[4] S. Iqbal, A. W. Malik, A. U. Rahman, and R. M. Noor, "Blockchain-Based Reputation Management for Task Offloading in Micro-Level Vehicular Fog Network," *IEEE Access,* vol. 8, pp. 52968-52980, 2020.

[5] N. Tariq, M. Asim, F. Al-Obeidat, M. Zubair Farooqi, T. Baker, M. Hammoudeh, *et al.*, "The security of big data in fog-enabled IoT applications including blockchain: A survey," *Sensors,* vol. 19, p. 1788, 2019.

[6] R. Guo, C. Zhuang, H. Shi, Y. Zhang, and D. Zheng, "A lightweight verifiable outsourced decryption of attribute-based encryption scheme for blockchain-enabled wireless body area network in fog computing," *International Journal of Distributed Sensor Networks,* vol. 16, p. 1550147720906796, 2020.

[7] M. Achouri, "Smart fog computing for efficient situations management in smart health environments," *Journal of Information and Communication Technology,* vol. 17, pp. 537-567, 2020.

[8] H. Elazhary, "Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions," *Journal of network and computer applications,* vol. 128, pp. 105-140, 2019.

[9] S. Nadeem, M. Rizwan, F. Ahmad, and J. Manzoor, "Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture," *International Journal of Advanced Computer Science and Applications,* vol. 10, pp. 288-295, 2019.

[10] A. S. Al-Ahmad, S. A. Aljunid, and N. K. Ismail, "Mobile Cloud Computing Applications Penetration Testing Model Design," *International Journal of Information and Computer Security,* 2019.

[11] A. S. Al-Ahmad and H. Kahtan, "Cloud Computing Review: Features And Issues,"

in *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, 2018, pp. 1-5.

[12] M. Chiang, S. Ha, I. Chih-Lin, F. Risso, and T. Zhang, "Clarifying fog computing and networking: 10 questions and answers," *IEEE Communications Magazine,* vol. 55, pp. 18-20, 2017.

[13] Z. Ashi, M. Al-Fawa'reh, and M. Al-Fayoumi, "Fog Computing: Security Challenges and Countermeasures," *International Journal of Computer Applications,* vol. 175, pp. 30-36, 2020.

[14] A. Ali, M. Ahmed, M. Imran, and H. A. Khattak, "Security and Privacy Issues in Fog Computing," in *Fog Computing: Theory and Practice*, A. Zomaya, A. Abbas, and S. Khan, Eds., ed United States: Wiley, 2020, pp. 105-137.

[15] P. Bellavista, J. Berrocal, A. Corradi, S. K. Das, L. Foschini, and A. Zanni, "A survey on fog computing for the Internet of Things," *Pervasive and mobile computing,* vol. 52, pp. 71-99, 2019.

[16] A. S. Al-Ahmad, S. A. Aljunid, and N. K. Ismail, "Mobile cloud computing applications penetration testing model design," *International Journal of Information and Computer Security,* vol. 13, pp. 210-226, 2020.

[17] A. V. Dastjerdi, H. Gupta, R. N. Calheiros, S. K. Ghosh, and R. Buyya, "Fog computing: Principles, architectures, and applications," in *Internet of Things*, ed Netherlands: Elsevier Science & Technology, 2016, pp. 61-75.

[18] R. Neware and U. Shrawankar, "Fog Computing Architecture, Applications and Security Issues," *International Journal of Fog Computing (IJFC),* vol. 3, pp. 75-105, 2020.

[19] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, "Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things," *IEEE Internet of Things Journal,* vol. 4, pp. 1143-1155, 2017.

[20] C. Rupa, R. Patan, F. Al-Turjman, and L. Mostarda, "Enhancing the Access Privacy of IDaaS System Using SAML Protocol in Fog Computing," *IEEE Access,* vol. 8, pp. 168793-168801, 2020.

[21] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, *et al.*, "Security and privacy in fog computing: Challenges," *IEEE Access,* vol. 5, pp. 19293-19304, 2017.

[22] C. Li, Z. Qin, E. Novak, and Q. Li, "Securing SDN infrastructure of IoT–fog networks from MitM attacks," *IEEE Internet of Things Journal,* vol. 4, pp. 1156-1164, 2017.

[23] M. Qatawneh, W. Almobaideen, M. Khanafesh, and I. Alqatawneh, "DFIM: A new digital forensics investigation model for internet of things," *Journal of Theoretical and Applied Information Technology,* vol. 97, pp. 3850-3867 2019.

[24] A. K. Alhwaitat, S. Manaseer, M. Alsyyed, A. Almaiah, and O. Almomani, "An investigation of digital forensics for shamoon attack behaviour in fog computing and threat intelligence for incident response," *Journal of Theoretical and Applied Information Technology,* vol. 98, pp. 977-990 2020.

[25] T. Khalid, M. A. K. Abbasi, M. Zuraiz, A. N. Khan, M. Ali, R. W. Ahmad*, et al.*, "A survey on privacy and access control schemes in fog computing," *International Journal of Communication Systems,* vol. 34, pp. 1-39, 2019.

[26] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Securing fog computing for internet of things applications: Challenges and solutions," *IEEE Communications Surveys & Tutorials,* vol. 20, pp. 601-628, 2017.

[27] D. Puthal, S. P. Mohanty, S. A. Bhavake, G. Morgan, and R. Ranjan, "Fog computing security challenges and future directions [energy and security]," *IEEE Consumer Electronics Magazine,* vol. 8, pp. 92-96, 2019.

[28] Y. Guan, J. Shao, G. Wei, and M. Xie, "Data security and privacy in fog computing," *IEEE Network,* vol. 32, pp. 106-111, 2018.

[29] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications,* vol. 88, pp. 10-28, 2017.

[30] N. Abubaker, L. Dervishi, and E. Ayday, "Privacy-preserving fog computing paradigm," in *2017 IEEE Conference on Communications and Network Security (CNS)*, 2017, pp. 502-509.

[31] Y. I. Alzoubi, V. H. Osmanaj, A. Jaradat, and A. Al-Ahmad, "Fog Computing

Security and Privacy for the Internet of Thing Applications: State-of-the-Art," *Security and Privacy,* vol. In Press, 2020.

[32] R. Rios, R. Roman, J. A. Onieva, and J. Lopez, "From SMOG to Fog: a security perspective," in *Second International Conference on Fog and Mobile Edge Computing (FMEC)*, 2017, pp. 56-61.

[33] S. Yu, G. Wang, X. Liu, and J. Niu, "Security and privacy in the age of the smart internet of things: an overview from a networking perspective," *IEEE Communications Magazine,* vol. 56, pp. 14-18, 2018.

[34] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access,* vol. 6, pp. 18209-18237, 2018.

[35] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems,* vol. 78, pp. 680-698, 2018.

[36] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet of Things Journal,* vol. 6, pp. 7992-8004, 2019.

[37] N. S. Khan and M. A. Chishti, "Security Challenges in Fog and IoT, Blockchain Technology and Cell Tree Solutions: A Review," *Scalable Computing: Practice and Experience,* vol. 21, pp. 515-542, 2020.

[38] C. Dsouza, G.-J. Ahn, and M. Taguinod, "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 (IEEE IRI 2014)*, 2014, pp. 16-23.

[39] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in Fog computing: A survey," *Future Generation Computer Systems,* vol. 88, pp. 16-27, 2018.

[40] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in *International conference on wireless algorithms, systems, and applications*, 2015, pp. 685-695.

[41] B. Z. Abbasi and M. A. Shah, "Fog computing: Security issues, solutions and robust practices," in *23rd International Conference on Automation and Computing (ICAC)*, 2017, pp. 1-6.

[42] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks,* vol. 141, pp. 199-221, 2018.

[43] X. Wang, L. Wang, Y. Li, and K. Gai, "Privacy-aware efficient fine-grained data access control in Internet of medical things based fog computing," *IEEE Access,* vol. 6, pp. 47657-47665, 2018.

[44] T. D. Dang and D. Hoang, "A data protection model for fog computing," in *2017 Second International Conference on Fog and Mobile Edge Computing (FMEC)*, 2017, pp. 32-38.

[45] H. F. Atlam, R. J. Walters, and G. B. Wills, "Fog computing and the internet of things: a review," *big data and cognitive computing,* vol. 2, pp. 1-18, 2018.

[46] A. Muthanna, A. A Ateya, A. Khakimov, I. Gudkova, A. Abuarqoub, K. Samouylov, *et al.*, "Secure and reliable IoT networks using fog computing with software-defined networking and blockchain," *Journal of Sensor and Actuator Networks,* vol. 8, p. 15, 2019.

[47] H. Tian, F. Nan, C.-C. Chang, Y. Huang, J. Lu, and Y. Du, "Privacy-preserving public auditing for secure data storage in fog-to-cloud computing," *Journal of Network and Computer Applications,* vol. 127, pp. 59-69, 2019.

[48] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in *Annual Cryptology Conference*, 2010, pp. 465-482.

[49] P. Kumar, N. Zaidi, and T. Choudhury, "Fog computing: Common security issues and proposed countermeasures," in *2016 International Conference System Modeling & Advancement in Research Trends (SMART)*, 2016, pp. 311-315.

[50] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A comprehensive survey on fog computing: State-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials,* vol. 20, pp. 416-464, 2017.

[51] A. Aljumah and T. A. Ahanger, "Fog computing and security issues: A review," in *2018 7th International Conference on*

Computers Communications and Control (ICCCC), 2018, pp. 237-239.

[52] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," *IEEE Internet Computing,* vol. 21, pp. 34-42, 2017.

[53] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji*, et al.*, "All one needs to know about fog computing and related edge computing paradigms: A complete survey," *Journal of Systems Architecture,* vol. 98, pp. 289-330, 2019.

[54] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," *Future Generation Computer Systems,* vol. 97, pp. 219-235, 2019.

[55] M. A. Khan, "A survey of security issues for cloud computing," *Journal of network and computer applications,* vol. 71, pp. 11-29, 2016.

[56] G. Simpson and K. Quist-Aphetsi, "A Centralized Data Validation Approach for Distributed Healthcare Systems in Dew-Fog Computing Environment Using Blockchain," in *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*, 2019, pp. 1-4.

[57] A. A. Mutlag, M. K. Abd Ghani, N. a. Arunkumar, M. A. Mohammed, and O. Mohd, "Enabling technologies for fog computing in healthcare IoT systems," *Future Generation Computer Systems,* vol. 90, pp. 62-78, 2019.

[58] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet of Things Journal,* vol. 3, pp. 854-864, 2016.

[59] M. H. Ashik, M. M. S. Maswood, and A. G. Alharbi, "Designing a Fog-Cloud Architecture using Blockchain and Analyzing Security Improvements," in *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, 2020, pp. 1-6.

[60] P. Hu, S. Dhelim, H. Ning, and T. Qiu, "Survey on fog computing: architecture, key technologies, applications and open issues," *Journal of network and computer applications,* vol. 98, pp. 27-42, 2017.

[61] R. K. Naha, S. Garg, D. Georgakopoulos, P. P. Jayaraman, L. Gao, Y. Xiang*, et al.*, "Fog Computing: Survey of trends, architectures, requirements, and research directions," *IEEE access,* vol. 6, pp. 47980-48009, 2018.

[62] Z. Hao, E. Novak, S. Yi, and Q. Li, "Challenges and software architecture for fog computing," *IEEE Internet Computing,* vol. 21, pp. 44-53, 2017.

[63] P. Varshney and Y. Simmhan, "Demystifying fog computing: Characterizing architectures, applications and abstractions," in *2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC)*, 2017, pp. 115-124.

[64] M. Aazam, S. Zeadally, and K. A. Harras, "Fog computing architecture, evaluation, and future research directions," *IEEE Communications Magazine,* vol. 56, pp. 46-52, 2018.

[65] K. Gai, M. Qiu, and M. Liu, "Privacy-Preserving Access Control Using Dynamic Programming in Fog Computing," in *2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing,(HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)*, 2018, pp. 126-132.

[66] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions," *Journal of Cloud Computing,* vol. 6, p. 19, 2017.

[67] Z. Wen, R. Yang, P. Garraghan, T. Lin, J. Xu, and M. Rovatsos, "Fog orchestration for internet of things services," *IEEE Internet Computing,* vol. 21, pp. 16-24, 2017.

[68] Y. Wang, T. Uehara, and R. Sasaki, "Fog computing: Issues and challenges in security and forensics," in *2015 IEEE 39th Annual Computer Software and Applications Conference*, 2015, pp. 53-59.

[69] H. F. Atlam, R. J. Walters, and G. B. Wills, "Fog computing and the internet of things: a review," *big data and cognitive computing,* vol. 2, p. 10, 2018.

[70] O. Abualghanam, M. Qatawneh, and W. Almobaideen, "A survey of key distribution in the context of internet of things," *Journal of Theoretical and Applied Information Technology,* vol. 97, pp. 3217-3241 2019.

[71] P. Prakash, K. Darshaun, P. Yaazhlene, M. V. Ganesh, and B. Vasudha, "Fog

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Computing: Issues, Challenges and Future Directions," *International Journal of Electrical and Computer Engineering,* vol. 7, p. 3669, 2017.

[72] U. Jayasinghe, G. M. Lee, Á. MacDermott, and W. S. Rhee, "TrustChain: a privacy preserving blockchain with edge computing," *Wireless Communications and Mobile Computing,* vol. 2019, 2019.

[73] M. Losavio, "Fog Computing, Edge Computing and a return to privacy and personal autonomy," *Procedia Computer Science,* vol. 171, pp. 1750-1759, 2020.

[74] A. K. Alhwaitat, S. Manaseer, and M. Alsyyed, "A survey of digital forensic methods under advanced persistent threat in fog computing environment," *Journal of Theoretical and Applied Information Technology,* vol. 97, 2019.