Fog Computing: Security Challenges and Countermeasures

Zain Ashi
School of Computing Science
Princess Sumaya University for Technology
Amman-Jordan

Mohammad Al-Fawa'reh
School of Computing Science
Princess Sumaya University for Technology
Amman-Jordan

Mustafa Al-Fayoumi
School of Computing Science
Princess Sumaya University for Technology
Amman-Jordan

ABSTRACT
Innovative technologies such as cloud computing systems provide global cooperative services for end users and medium-large companies. Fog computing extends cloud computing storage networking and computing capabilities to edge and backbone servers on the cloud for Internet of Things (IoT) devices, to optimize efficiency with low latency, location awareness, and geographical distribution applications. One of the considerable difficulties facing fog computing systems is security and privacy challenges. This survey reviews current fog computing system architectures, their features, security challenges associated with IoT devices, and existing countermeasures, in order to guide researchers to find comprehensive solutions to reduce the security risks related to fog computing systems.

General Terms
IoT security challenges and Countermeasures

Keywords
IoT, Cloud, Edge Computing, Fog Computing, Security

1. INTRODUCTION
IoT combines various devices and communication methods to exchange information. Today the IoT is more than a descriptive term for the dream of connecting everything to the Internet, and it is an increasingly active concept transforming many industrial processes and everyday life, opening up opportunities for new technologies and developments. All devices will be connected and will be able to communicate with each other. This presents significant challenges to security. According to [1], the expected number of IoT devices will increase to 75.44 billion by 2025. IoT services are already available and in operation in a wide range of systems, such as smart manufacturing, healthcare, transport, and autopilot systems, and are increasingly common in every home in the form of smart meter systems. The challenge is how to run the computational intensive applications of these systems and how to handle the massive amount of collected data on low computational power and small battery IoT devices [2]. The best solution is to transfer the processing of IoT devices to high-capability cloud systems using a mechanism called offloading, which moves data processing from the edge of the IoT devices to a robust cloud-based system via gateways and embedded devices [3]. It seems that the centralized cloudbased system is the right solution, but the massive workload from the IoT services to the cloud systems, the unreliable longlatency Internet networks, and the delivered security issues increases the associated challenges rather than decreases them [2].

Fog computing is a new technology developed by the Cisco Group. It was implemented to bring services closer to IoT devices through its nodes by combining the available computing, storage, and networking resources at the edge of the network [4]. Decentralized fog architecture is well situated between IoT devices and cloud servers in order to provide users with more efficient services. Since fog nodes have more memory and more processing power, a large amount of data from IoT nodes can be processed immediately. Some data and computations that require more computing power are transmitted from the fog nodes to the back-end cloud via high speed communications [4]. The architecture used involves interaction between the three levels (cloud computing, fog computing, and edge computing), as shown in Figure 1.

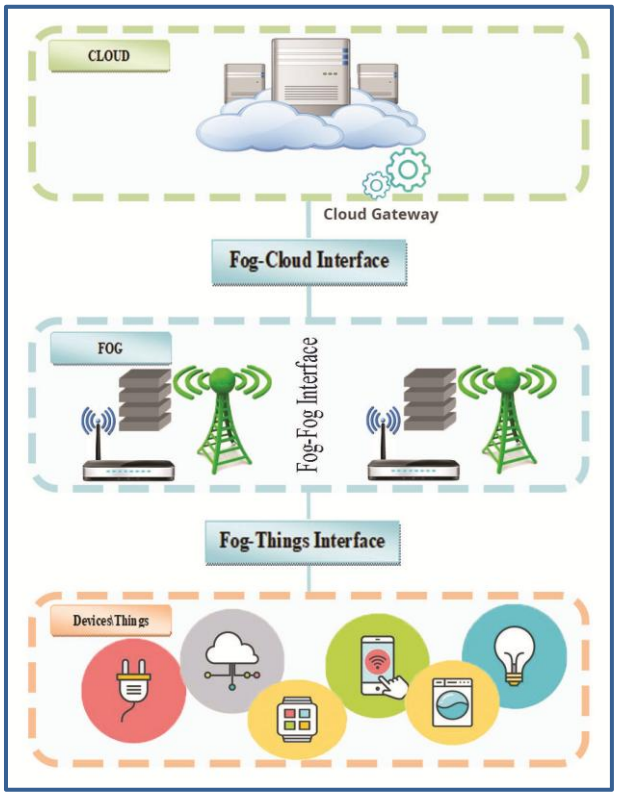

Figure 1: Three Tier Fog Computing Architecture.

Fog nodes (FNs) in the fog level reduce network congestion and latency in the network. FN functions are to process data directly rather than sending it to the cloud, and to collaborate with the nearest FNs to share data storage and computing tasks. FN determines whether to process the data in the fog level or send it to the cloud, where there are more ample resources for storage and computation. Cloud computing

systems provide a factual infrastructure that opens up new opportunities in a competitive market for digital business. Fog computing systems optimize these services by bringing them near to the edge of the network, closer to the IoT devices. Fog computing systems have several distributed nodes that are less capable of processing and storing than those in cloud systems.

Such circumstances lead the entire system through major security and privacy problems, which must be considered to protect the integrity and confidentiality of the transmitted and processed data. Data streaming from many IoT devices to the nearest fog nodes raises several security concerns about who is responsible for this data. An authority party has to interfere to guarantee the data protection of these users in order to establish trusted security relationships between the IoT user and fog computing systems. The Global Data Protection Regulation (GDPR) [5] was established in 2018, outlining the legal principles of the fog computing system. One of GDPR's key statements is anyone who manages the processing of the IoT data is responsible for that data protection, and financial penalties will be imposed for failures, but it is unclear what authority is responsible for implementing these regulations.

The architecture of fog computing is explored in details in section II, and several fog features are explored in section III. Some previous studies are described in section IV, and security challenges, open questions, and their countermeasures are in sections V and VI. Ultimately and our conclusion is in section VII.

2. THE ARCHITECTURE OF FOG COMPUTING

Fog architecture is illustrated as a three-tier architecture, comprising the edge, fog, and cloud levels, as shown in Figure 1 [6]. Lee et al. [7] described the fog architecture as a network of IoT back-end systems, and Hong et al. [2] considered the fog level to be an extension of the cloud level, to provide services closer to the edge-based position of the IoT applications. In ascending order, the edge, fog, and cloud levels have increasing processing and storage capacities. In short, the level of fog is a decentralized level imposed between the cloud and the edge levels, to reduce the overhead and latency of applications in the cloud. Services will be sent to the cloud level when there are computations and data requiring more computing power than that available or expedient in the fog level. The fog level is made up of several geographically distributed FNs represented by high computational devices (such as routers, bridges, gateways, switches, and local servers). These FNs are connected from one side to the IoT devices (such as mobile phones, sensors, cameras, and wearable devices), and from the other side to the cloud servers. All of them are linked via wireless connections (e.g. Bluetooth and Zigbee etc.), wired connections (optical fiber, Ethernet, etc.), or both connection types can be used in combination. The level of the cloud is "used to support services such as Infrastructure as a Service (IaaS), Software **as** a Service (SaaS) and Platform as a Service (PaaS)" [6].

However, FNs can now directly deliver these services to the edge-level IoT devices. FNs collect data from IoT devices in milliseconds to make decisions and monitor activities, to provide real-time services [8].

3. FOG COMPUTING FEATURES

Fog nodes spread close to IoT devices at the edge of the network, optimizing the services provided, and increasing the utilization of FN resources such as storage, networking, and data transmission. Fog computing systems have several features that have been explored in depth by various studies [4]. They can be understood in contrast with the features of cloud computing [9]:

3.1 Location Awareness and Low Latency

FN provides IoT devices with services based on their locations relative to the region of that FN. Each device sends data and gets services from the closest FN, and receives responses within milliseconds. Therefore fog nodes services improve the efficiency of the real-time and decision making services.

3.2 Geographic Distribution

FNs are distributed at consecutive locations to guarantee high-quality data transmission between themselves and IoT devices during their traverse of FNs' regions.

3.3 Decentralization

Multiple FNs can cooperate to perform any heavy computing services from IoT devices. When computing is distributed between FNs' resources, there is no need for centralized servers.

3.4 Real-Time Services

FNs have the ability to provide the users with real-time services, with great value to many systems that do not tolerate

3.5 Saving Utilization of Cloud Storage

The FNs collect a massive amount of user data, and onlyfiltered data is emigrated to be stored in the cloud.

3.6 Heterogeneity

Fog computing system consists of broad types of FNs that vary in the capabilities from one to another, due to different operating systems between high-capacity servers and limited-capacity sensors. Communication in the fog computing systems also varies in speed and nature, and may be wired or wirelesses, depending on the requirements of serviced systems.

3.7 Mobility Support

FNs allow direct communication with mobile devices, enabling user identity and location to be distinguished using protocols such as Cisco's locator/ID separation protocol.

4. LITERATURE REVIEW

Adapting the economy's IoT and cloud revolution adds value to businesses, as evidenced by many successful case studies on customers who adapted their companies to the IoT revolution, but in all cases an overriding consideration is the security and privacy of user data [1]. Hong et al. [2] explored maximizing Quality of Service (QoS) in multi-hop computation offloading to the cloud for industrial systems. They proposed a distributed game-theoretic mechanism with two QoS-aware distributed algorithms, by which they achieved great efficiency in computation offloading to the cloud. Flores et al. [3] added that the heterogeneity of the IoT devices and their large-scaled architecture presented real concerns in the offloading domain. Therefore, as an offloading interface between Android IoT devices and cloud resources, they created an AutoScaler mechanism to facilitate offloading workload in the heterogeneity and the large-scaled architecture of the IoT systems. The architectures addressed in [1], [2], and [3] were IoT-cloud computing systems in which processing is carried out in a centralized manner. Centralization raises the cloud system's processing burden, contributing to security and privacy concerns, location awareness, and latency of realtime services issues. With

regard to the use of fog computing systems as an extension of cloud computing systems and IoT devices, there is more secure architecture in decentralized fog computing systems, and implementation enhances real-time services [4]. Fog implementation has been explored in smart grid systems [10], and cloud real-time service latency can be halved using intermediary fog data [11]. Fog computing systems are seen in the digital market as a revolution of the development of the services in this domain and others, but system implementation has posed several new issues of security and privacy. Munir et al. [9] describe the fog computing system as "a cloud that is close to the ground", and fog has inherited some IoT-Cloud computing system security and privacy issues [7]. Moreover, the new architecture is threatened by new attacks [4], [6], [7]. Stojmenovic et al. [11] tested man-in-the-middle attack's stealthy features by checking its CPU and memory use on fog computers, finding that the man-in-the-middle attack is very stealthy, because it is easy to launch, but difficult to deal with. The researchers in [9] discriminate between the cloud computing system and the fog computing system, as shown in Table 1. Some researchers have considered environmental perspectives, reporting that the implementation of fog computing system reduces CO2 emissions from fog Data Centers (DCs) by half compared to emissions entailed by use of the conventional IoT-Cloud computing system [12]. This is significant as many companies are keen to embrace a more environmentally friendly philosophy with regard to their DCs, such as Apple using renewable energy [6]. The three-tiered architecture of the fog computing system has been explored by many studies with regard to real-life implementation, such as smart cities, vehicle networks, healthcare systems, and smart grid systems [4], [6], [13]. Security and privacy issues have also been extensively discussed [4], [6], [12], [13], as elaborated upon in this paper.

Motivated by the prior concerns of privacy and security, many scholars have been driven to find solutions to these issues from different specialized perspectives. Kulkarni et al. [14] believed that the smart TV remote control could reveal the privacy of the user, so they proposed a framework using the fog computing concept in the wireless networks to preserve the privacy of the user. The challenge they encountered with their framework was that TV remote control system has low processing capabilities, and these devices could not undertake encryption or any heavyweight processes. The same challenges were faced by Lu et al. [15], whose scheme, as they asserted, was characterized by lightweight processing, which they suggested for smart grid communications. Both of these studies eliminated potential user privacy threats as well as user authentication [14], [15]. Chen et al. [16] also addressed smart grid schemes, using Cipher Text Protocol Attribute-Based Encryption (CP-ABE) cryptographic solution. They reported that the CP-ABE scheme combines the safety goals with the efficiency of the system. The CP-ABE cryptographic solution was used by Fan et al. [17] to perform secure control of data access in vehicle network system. In the opinion of Hur et al. [18], the difficulty in applying that cryptographic solution is to select an efficient user attribute to control the users' access policies. They claimed that they had chosen an efficient user attribute for their proposed mechanism for effective and secure access to the data, which was distinct in that they executed two phases of encryption and distributed keys for each attribute set.

Table 1. Comparison between Fog and Cloud Computing.

Criterion	Fog computing systems	Cloud computing systems
location	At the edge of the network	At the internet
Geographical distribution	Localized	Centralized
The distance between the client and the serving node.	Single hop	Multiple hops
Providing real-time services.	Perfectly suited to real-time services	Provide delay in real time services
Providing location-based custom content, application, and services.	Provide	Do not provide
Mobility support	Fully support	Limited support

Researchers presented privacy and security issues differently. Advanced Encryption Standard (AES) algorithm was used to encrypt mobile transmitted data in fog nodes to secure the data from eavesdroppers [19], and eight security and privacy issues were mentioned by an et al. [20], with their countermeasures. Alrawais [21] and Ni et al. [4] addressed them only in the networks of vehicle sensors, while a fuller discussion was given in [22]. Fog and cloud external attacks were discussed by [4], [6], and [7], and [23] added examples for each attack. The challenges and open problems in fog computing are expected to trigger more research efforts in the future mentioned [4], [6]. In this survey, the privacy and security issues are categorized into five challenges, in order to facilitate understanding them and some of the countermeasures are mentioned in various systems too.

5. CHALLENGES AND OPEN QUESTIONS

Fog computing level is considered as an extension between the cloud computing level to the edge computing level, providing additional storage, networking, and processing facilities closer to IoT devices users. Fog computing consists of FNs distributed geographically, connected to dynamic IoT devices for various services; moreover, these FNs can enter and exit the network continuously. This distributed architecture and associated mobility issues present substantive security and privacy challenges to be considered, as adumbrated below.

5.1 Trust

Fog computing network has a significant role in establishing an initial set of relations. Mukherjee et al. [6] defined the trust relations between the fog node and the IoT devices as a twoways process, as shown in Figure 2, to ensure security and eliabilit1y between them.

The heavy workload is processed by several fog nodes to provide services in real-time. The challenge is how integrity

can be protected if one of these nodes is malicious. Lee et al. [7] and Ni et al. [4] illustrated the relationship between cooperating FNs and IoT devices, as shown in Figure 3.

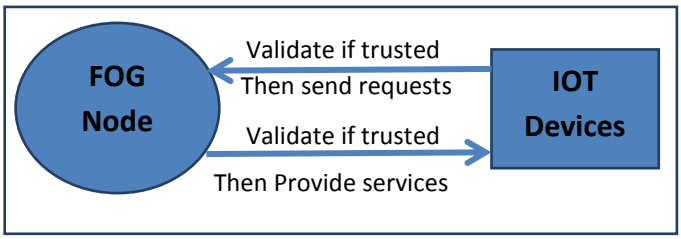

Figure 2: Trust- Relation between Fog Node and Users.

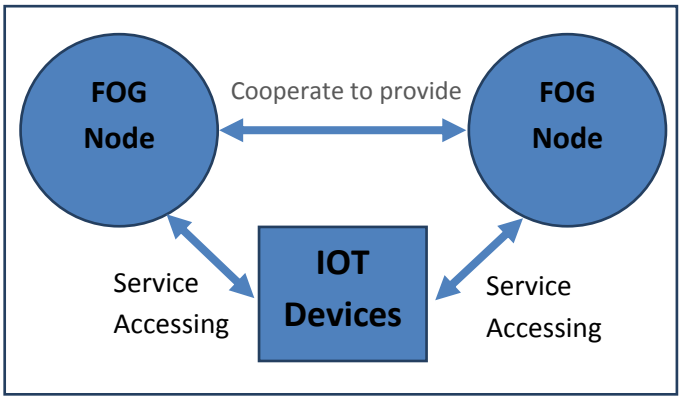

Figure 3: Trust-relation between different Fog Nodes.

To establish trusting relations between FN-IoT devices and between FN-FN, a professional and licensed service provider can deploy secure communications between "third-party" entities enrolled between them [6]. On the other hand, trust between the FNs should be supported when changing network conditions, including the dynamics of FNs and mobility of IoT devices [4].

Fog computing networks consist of widely distributeddynamic FNs, which are vulnerable to security threats, comprising an untrusted infrastructure. As Ni et al. [4] showed, any FN or IoT device may claim to be legitimate and coax others to interact with it. Creating trustworthy FN-IoT and FN-FN relationships is an open question for future research [6].

5.2 Authorization and Authentication

Authorization and authentication are essential requirements to secure the connections between FNs with each other, and with connected IoT devices. Abbasi and Shah [13] defined authentication as being "to identify every connected node as a verified node", and authorization as being "to describe the privileges of each connected node", as each node has its own different capabilities and functions, Mukherjee et al. [6] demonstrated that each IoT device should be authenticated by the fog node system to become part of its network. There are two challenges in this regard. The first is to provide real-time services where FNs work together to track users in large areas, moving from one FN's coverage region to another [4]. In this case, for each FN, the user should be authenticated before delivering any services during travelling, which causes unreasonable latency in real-time services, as the authentication process should be performed in each FN.

Cooperative authentication between FNs schemes can be used to reduce this latency [24]. The second challenge is that during the authentication process, the identities of users should not be exposed to attackers, to avoid exposing their current positions [6].

Authentication and authorization in fog computing systems are a major security issue. Creating lightweight authentication mechanisms should be considered as a priority research area to provide real-time services without latency [6].

5.3 Confidentiality

There are two aspects to be aware of regarding confidentiality in fog computing: secure data storage and secure network communications. IoT devices turn over their data to the nearest FN for storage or processing, which may be compromised by unauthorized modification. As a result, fog computing has a new challenge in designing a secure system ensuring the integrity of the IoT data manipulated in the FNs [25]. In order to ensure the reliability of fog computing systems they must shielded from any eavesdroppers or malicious attackers, including in communication among FNs themselves, and with connected IoT devices and linked FNs [6]. Abbasi and Shah emphasize that any malicious attack on any FN affects the connected FNs, and the challenge is how to isolate each FN to prevent the spread of malicious attacks over other connected ones [13].

Wide-ranging research should be carried out to protect FN-FN, IoTs-FN communications, and IoT data during processing in FNs, to avoid any unauthorized modifications.

5.4 Privacy

Although FNs serve IoT users, they collect sensitive information about users that could violate their privacy. The nearest FN senses the identity and location of the IoT user, and their habits can also be tracked. It is therefore simple for an attacker to expose the privacy of the IoT user if they successfully identify the user, such as by intercepting and monitoring the data of a house smart meter [6], whereby attackers can identify times when a house is empty. IoT users are entitled to share those with whom they want to share their data [9]. In order to ensure such rights, fog computing systems must find a method to identify obfuscation, to avoid violating IoT users' privacy [25].

For researchers, privacy preservation is more challenging, as dynamic FNs collect sensitive data about IoT users, so that any malicious attack on the interconnected network could reveal the data of the users, as well as their locations and habits.

5.5 Malicious Attacks

Any IoT devices or FNs could be malicious entities intending to initiate malicious attacks in the fog computing system. Since a large number of IoT devices and FNs use the same network, it is difficult to discover malicious entities in this environment (or rather, to distinguish them from genuine users). Malicious attacks might be "outsider attacks", where the attacker is an unauthenticated entity, or "insider attacks" where the attacker is an authenticated but unauthorized entity. One of the open questions is how to spot and prevent a malicious attack in the fog computing system [26]. The most well-known and common attacks are described below [7,4,23]

• Man-in-the-Middle Attack: An attacker may get control of an FN (e.g. a gateway FN), or swap it with a fake one. It is not easy to detect these attacks as there is no evidence that could be detected by the fog computing system.

• Eavesdropping Attack: Any clear data transmitted without

encryption can be exposed if an attacker compromises the communication channels.

•Collusion Attack: Two or more attackers may work together to launch an attack on an FN in order to increase their malicious capabilities.

• Denial-of-Service Attack: An attacker may exhaust the FN resources or communications by fake requests, to prevent the FN from delivering its services to IoT users.

6. COUNTERMEASURES

Attackers could violate user privacy by acquiring true identity, location, or even his habits. For instance, attackers can access sensitive information through smart TV remote controls if data is sent to the FN without encryption [14]. However, encrypting all transmitted data is costly and causes latency. By the way users presses and request channels on remote devices, attackers can identify who they are, their habits, and their location. It has been proposed that minimal data for functionality should be sent to the FN to minimize privacy threats, by the following system [14]:

• The FN receives only the most significant extracted features via the remote TV.

•Adding artificial noise to the transmitted data can be removed by the FN by simple computations.

•Data can be sent as broken and shuffled packets without encryption, while the order is sent encrypted, using the public key of the FN to reorder it.

On the other hand, the suggested system could achieve the goal of confidentiality and integrity, and be a good defense against man-in-the-middle and brute force attacks [19].

In this system, instead of the costly option of blanket encryption of all data, the transmitted data is blurred, divided, and shuffled to reduce the user's operations and increase the efficiency of real-time services. Such precautions are also sufficient to prevent man-in-the-middle attackers, eavesdroppers, and brute force assailants from achieving their goals. However, while this proposed system protects user privacy, it requires a lot of simultaneous operations (blurring, filtering, encryption, decryption, and ordering and reordering), which increase the overhead load for both the user and the FN, especially as the TV remote sends data continuously. This research area needs more evaluation of time consumption in order to prove its effect on real-time services, and to reduce overheads for the entities. The "System for Efficient Privacy Preservation Aggregation" (EPPA) focuses on smart meters used in smart grid systems, and purports to improve the security of communications, authentication costs, and privacy concerns [15]. A smart meter is a device to monitor the energy consumption at the user side. Over regular time periods it records the energy consumed and sends this data to the operation center via a region gateway (which plays the role of the FN), and a response is sent back to the smart meter. Taking advantage of the tiny homomorphic data generated by smart meters, this scheme uses the Paillier cryptosystem to achieve the confidentiality objective during data transmission and to prevent FN from decrypting user data. It works as follows:

1. The smart meter data is expressed by the Paillier cryptosystem, which intrinsically protects data against the chosen plain text attack; also, it does not leave a chance for eavesdroppers.

2. Each exported record has a timestamp signature to ensure its validity, and authenticate the smart meter. We think it will also avoid a replay attack.

3. The corresponding FN verifies the signature and the time stamp; if verified, it signs the encrypted record with its signature and sends it to the operation center, without decrypting the data.

4. The operating center checks the signature of the sending FN and then decrypts the user's record by the master key. Lu et al. [15] measured their scheme's.R. Lu et al. [15] measured their scheme's computational performance in comparison with conventional schemes, and the experimental results indicate that it clearly decreased consumer and operating center computing costs, as shown in Figure 4, 5. The system did not achieve the objective of availability as the communication between the devices of FN-users and the FNs-control center is the costly WiFi, which is still threatened by overloading bandwidth.

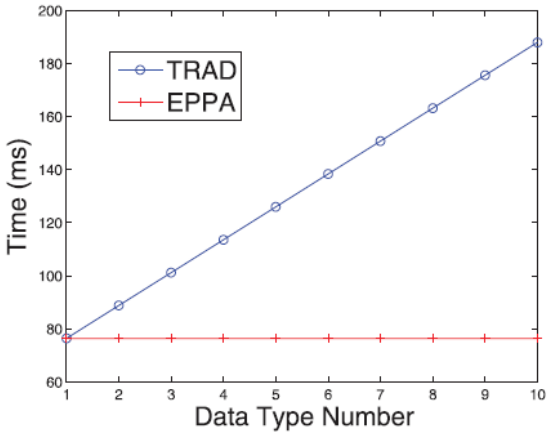

Figure 4: Computation cost of the operation center [16]

A traditional model called Decoy System is used in the security aspect to deploy attackers, discover them, and prevent them from disclosing any data in the FN [27]. Fake information is added to the origin files stored in the FN for fake users, and any attacker attempting to access the data will be trapped. This approach is insufficient because the intruder could also have access to the origin data. In order to improve the efficiency of this method, stored data can be encrypted in the FN to prevent attackers exposing any data, even if they have access to it [19]. This approach took another direction with the use of Advanced Encryption Standard Algorithm (AES) to encrypt mobile transmitted data, which is the most secure encryption method with rapid implementation in terms of both software and hardware requirements [19]. Mobile users send their data to the FN, which uses the AES algorithm to encrypt the data and transfer it to the cloud to be stored. The encrypted data is transmitted to the user from the cloud via the FN again. The mobile user then undertakes the decryption operation. The model evaluation uses three data sets, with different data types and sizes. Testing the use of the CPU and the en/decryption time required to evaluate the performance can be achieved using a mobile phone and a laptop. The results for the small size of the data set are the same. It is better to compare the results with other encryption algorithms to get a more accurate evaluation of performance, or the performance could be compared across different key sizes. In general, it is not recommended to add encryption tasks to the FN. Challenging issue in fog computing systems, commonly adopting the

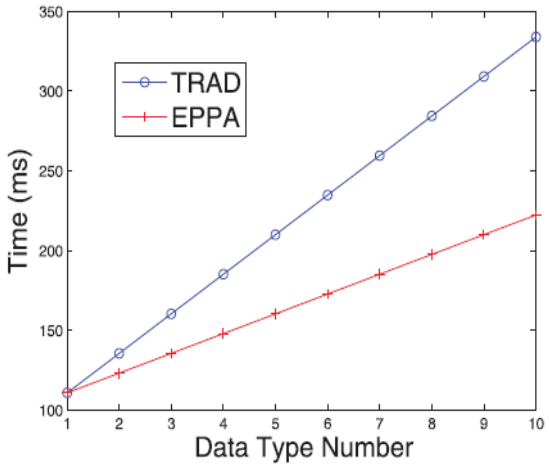

Figure 5: Computation cost of each user [16]

Cipher Text Attribute-Based Encryption (CP-ABE) scheme to support authentication challenges [17], [28], [29]. In CP-ABE the transmitted data is encrypted with a sufficient number of authorized receiver attributes, and receivers are allowed to decrypt the data only if their attributes match the encrypted. The simplicity of this scheme is that, according to their attributes, several cloud receivers decrypt the data, as many users share the same attributes, depending on their environments and their data objects. For their data, the data owners must specify a set of authorized user attributes and a set of attributes for each receiver. In the CP-ABE system, there is a problem related to the revocation operations for both the attributes and the revocation of users, because they are both complex and linked in the data transmission process (but this is outside our survey domain) [18].

Chen et al. [28] suggested a scheme to use CP-ABE in smart grid lowcapacity devices. This scheme should be lightweight on the side of the customer. It works like this:

1. The encryption process (for transmitted data and user attributes) is split between the device of the data owner and the corresponding FN, in order to reduce the overhead on the user's side. The encrypted data is transmitted to the cloud. Proxy keys are stored in the cloud for each authorized user. If the user status is revoked, the proxy key will be removed.

2. The cloud computing system ensures that the proxy key of the user is not removed and transfers the data to the appropriate FN when the end-user makes a request to access the stored data.

3. The decryption operation is divided another time between the FN and the end-user if (and only if) its attributes are compatible with the authenticated attributes.

This scheme protects data confidentiality and integrity because data is kept encrypted between the FN and the cloud computing system during the transmission and storage phases, and only authorized users may access the data. They tested their system by contrasting it to the CP-ABE systems of Chen et al. [28] and Fan et al. [17]. The findings of the analysis indicate that it increased the efficiency of communication and computation.

Fog computing systems have security counter-measures, some of which almost meet security targets, while others do not. Each system should select the appropriate security countermeasure to perform the required tasks of that system.

Table 2 shows a comparison of the countermeasures mentioned in our survey.

7. CONCLUSION AND FUTURE WORK

Fog computing systems are modern decentralized architectures that extend cloud storage, networking, and computing capabilities to the edge of the network to support IoT applications on a large scale. The location awareness of the fog computing system, geographic distribution, and other features provide new security challenges that should be taken into account. In this survey, we offered an overview of fog architecture, a set of its features, and related works. The challenges and open questions of fog computing security wereat the core of this study, and some existing countermeasures were explored in order to guide researchers to find comprehensive solutions to reduce the security risks related to these systems. Future work will explore attacks on fog computing systems and their countermeasures in more depth.

Table 2. Comparison between Fog and Cloud computing systems

Ref	Year	Method	Confidentiality Privacy/Security	Integrity Authentication	Availability
[16]	2012	Paillier cryptosystem	Obtained	Obtained	Not obtained
[14]	2014	Blurring Without decryption	Obtained	Not obtained	Not mentioned
[16]	2015	Decoy System	Not obtained	Not obtained	Not mentioned
[17]	2016	AES cryptosystem	Obtained	Obtained	Not mentioned
[19]	2018	CP-ABE	Obtained	Obtained	Not mentioned
[20]	2018	CP-ABE	Obtained	Obtained	Not mentioned
[18]	2019	CP-ABE	Obtained	Obtained	Not mentioned

8. REFERENCES

[1] A. Samuel and C. Sipes, "Making Internet of Things Real," IEEE Internet Things Mag., vol. 2, no. 1, pp. 10–12, Sep. 2019, doi: 10.1109/IoTm.2019.1907777.

[2] Z. Hong, W. Chen, H. Huang, S. Guo, and Z. Zheng, "Multi-Hop Cooperative Computation Offloading for Industrial IoT-Edge-Cloud Computing Environments," IEEE Trans. Parallel Distrib. Syst., vol. 30, no. 12, pp. 2759–2774, Dec. 2019, doi: 10.1109/TPDS.2019.2926979.

[3] H. Flores et al., "Large-scale Offloading in the Internet of Things."[online].Available:https://github.com/mobile-cloudcomputing/ScalingMobileCodeOffloading.

[4] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Securing Fog Computing for Internet of Things Applications: Challenges and Solutions," IEEE Commun. Surv.

Tutorials, vol. 20, no. 1, pp. 601–628, Jan. 2018, doi:

[5] 10.1109/COMST.2017.2762345.

[6] R. Garg, S. Varadi, and A. Kertesz, "Legal Considerations of IoT Applications in Fog and Cloud Environments," in Proceedings - 27th Euromicro International Conference on Parallel, Distributed and NetworkBased Processing, PDP 2019, Mar. 2019, pp. 193–198, doi: 10.1109/EMPDP.2019.8671620.

[7] M. Mukherjee et al., "Security and Privacy in Fog Computing: Challenges," IEEE Access, vol. 5, pp. 19293–19304, Sep. 2017, doi10.1109/ACCESS.2017.2749422.

[8] K. Lee, D. Kim, D. Ha, U. Rajput, and H. Oh, "On Security and Privacy Issues of Fog Computing supported Internet of Things Environment."

[9] "Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are What You Will Learn," 2015.

[10] A. Munir, P. Kansakar, and S. U. Khan, "IFCIoT: Integrated Fog Cloud IoT: A novel architectural paradigm for the future Internet of Things," IEEE Consum. Electron. Mag., vol. 6, no. 3, pp. 74–82, Jul. 2017, doi: 10.1109/MCE.2017.2684981.

[11] P. Varshney and Y. Simmhan, "Demystifying Fog Computing: Characterizing Architectures, Applications and Abstractions," Proc. - 2017 IEEE 1st Int. Conf. Fog Edge Comput. ICFEC 2017, no. 100, pp. 115–124, 2017, doi: 10.1109/ICFEC.2017.20.

[12] K. Dantu, S. Y. Ko, and L. Ziarek, "RAINA: Reliability and Adaptability in Android for Fog Computing," IEEE Commun. Mag., vol. 55, no. 4, pp. 41–45, 2017, doi: 10.1109/MCOM.2017.1600901.

[13] S. Sarkar, S. Chatterjee, and S. Misra, "Assessment of the Suitability of Fog Computing in the Context of Internet of Things," IEEE Trans. Cloud Comput., vol. 6, no. 1, pp. 46–59, 2018, doi: 10.1109/TCC.2015.2485206.

[14] B. Z. Abbasi and A. Shah, "Fog Computing: Security Issues, Solutions and Robust Practices."

[15] S. Kulkarni, S. Saha, and R. Hockenbury, "Preserving privacy in sensorfog networks," 2014 9th Int. Conf. Internet Technol. Secur. Trans. ICITST 2014, no. 1, pp. 96–99, 2014, doi: 10.1109/ICITST.2014.7038785.

[16] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 9, pp. 1621–1632, 2012, doi: 10.1109/TPDS.2012.86.

[17] S. Chen, M. Wen, R. Lu, J. Li, and S. Chen, "Achieve revocable access control for fog-based smart grid system," in IEEE Vehicular Technology Conference, Sep. 2019, vol. 2019-September, doi: 10.1109/VTCFall.2019.8891162.

[18] K. Fan, J. Wang, X. Wang, H. Li, and Y. Yang, "Secure, efficient and revocable data sharing scheme for vehicular fogs," Peer-to-Peer Netw. Appl., vol. 11, no. 4, pp. 766–777, 2018, doi: 10.1007/s12083-017-0562-

[19] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214–1221, 2011, doi: 10.1109/TPDS.2010.203.

[20] A. Vishwanath, R. Peruri, and J. (Selena) He, "Security in Fog Computing through Encryption," Int. J. Inf. Technol. Comput. Sci., vol. 8, no. 5, pp. 28–36, 2016, doi: 10.5815/ijitcs.2016.05.03.

[21] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges," Futur. Gener. Comput. Syst., vol. 78, pp. 680–698, 2018, doi: 10.1016/j.future.2016.11.009.

[22] H. E. Hudson, V. Forsythe, and S. G. Burns, "Keeping in touch by two-way radio.," World Health Forum, vol. 4, no. 2, pp. 157–161, 1983.

[23] Y. Wang, T. Uehara, and R. Sasaki, "Fog computing: Issues and challenges in security and forensics," Proc. - Int. Comput. Softw. Appl. Conf., vol. 3, pp. 53–59, 2015, doi: 10.1109/COMPSAC.2015.173.

[24] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of Fog computing and its security issues," Concurr. Comput. , vol. 28, no. 10, pp. 2991–3005, Jul. 2016, doi: 10.1002/cpe.3485.

[25] J. Zhou, X. Lin, X. Dong, and Z. Cao, "PSMPA: Patient selfcontrollable and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing system," IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 6, pp. 1693–1703, 2015, doi: 10.1109/TPDS.2014.2314119.

[26] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2015, vol. 9204, pp. 685–695, doi: 10.1007/978-3-319-218373 67.

[27] R. Sandhu, A. S. Sohal, and S. K. Sood, "Identification of malicious edge devices in fog computing environments," Inf. Secur. J., vol. 26, no. 5, pp. 213–228, Sep. 2017, doi: 10.1080/19393555.2017.1334843.

[28] N. S. Dhande, "Fog Computing: Review of Privacy and Security Issues," vol. 3, no.2, pp. 864–868, 2015.

[29] Shan Chen, ndMi Wen, rdRongxing Lu, thJinguo Li, and thSijia Chen, Achieve Revocable Access Control for Fog-based Smart Grid System.

[30] P. Zhang, Z. Chen, J. K. Liu, K. Liang, and H. Liu, "An efficient access control scheme with outsourcing capability and attribute update for fog computing," Futur. Gener. Comput. Syst., vol. 78, pp. 753–762, Jan. 2018, doi: 10.1016/j.future.2016>