Features, Challenges and Issues of Fog Computing:
A Comprehensive Study

MUNEER BANI YASSEIN, ISMAIL HMEIDI,
FARAH SHATNAWI, SAIF RAWASHEH, OMAR ALZOUBI

Computer Science, Jordan University of Science and Technology, Irbid

JORDAN

masadeh@just.edu.jo, Hmeidi@.just.edu.jo, ffshatnawi16@cit.just.edu.jo,
sarawashdeh16@cit.just.edu.jo, oaalzoubi@just.edu.jo

Abstract: - Fog computing is one of the most important technologies and promising computing model used by many end-users, organizations, and companies. This model has many qualities, characteristics, advantages and offers many services to end-users like compute, and application services. So, it facilitates the services that provided it to the end-users and allows us to increase the number of devices that connect the network. In this research paper, we survey the Fog technology in terms of the architecture and the primary features (i.e. advantages, and disadvantages). Then, we compare this model with Cloud computing, Mobile-Edge Computing, and Cloudlet Computing. Also, this paper is constructed by illustrating the importance of several challenges and issues that facing Fog computing like "privacy and security: issues and solutions", control and management issues, fog networking and task scheduling. Finally, we mention the six aspects of fog computing security and the benefits of merging between Fog computing and other techniques like "Internet of Things and Cloud". This paper will contribute to providing the researchers who want to study the Fog computing in terms of aspects that previously mentioned.

1 Introduction

Fog computing is new promising computing model and highly virtualized that extended the services of cloud computing to the edge network services [1, 2, 3, and 4]. It appropriates for Wireless sensor networka (WSNs) and IoT [3], and supports heterogeneity appliances, such as Fog appliances, which the appliances are end-user, switches, edge routers, and access points [1]. Fog computing provides many services in the network, such as compute, application services to end-users, data, "location awareness and improves quality-of services (QoS) for streaming and real-time applications", storage, "networking services between end devices and traditional cloud computing data centers", and low latency [1, 2]. The constituent layers of Fog computing architecture are "physical and virtualization layer", "monitoring layer", "preprocessing layer", "temporary storage layer", "security layer", and "transport layer" [5, 6]. There are several applications that are taken a benefit from Fog computing, such as augmented reality, smart home, smart grid, health data management, smart factory, and smart vehicle [4, 7].

Muneer Bani Yassein,
Ismail Hmeidi, Farah Shatnawi,
Saif Rawasheh, Omar Alzoubi

The challenges and issues that are facing Fog computing are (1) protecting the data. (2) Malicious Fog node. (3) Malicious detection technique in Fog computing environments. (4) Detect the intrusion. (5) Man-in-the-middle attack and others [1, 8]. One of the most issues that faced the fog computing is security issue [6]. There are many aspects and things are important for security techniques to handle the security issues and problems that faced Fog computing, which are "authorization and authentication", network security, access control mechanism, intrusion detection system (IDS), privacy, and virtualization [30].

There are many researchers, which merged the Fog computing with different types of computing and other techniques. The aim of this merged; to enhance the limitations that facing the and other techniques alone. The Mahmud et al. in [9] merged the Fog with Cloud computing to solve the latency sensitivity problem in healthcare application of IoT. The merged approach is called Cloud-Fog Interoperability. The An et al. in [10] merged the Fog, IoT, and artificial intelligence (AI). This merge aims to make the AI services clever, reliable and faster than the first generation of IoT services. The merged approach is called Elastic-IoT-Fog (EiF). Munir et al. in [11] integrated three techniques to increase many things in IoT applications. These things are scalability, energy in an efficient way, latency in the lower level, quicker response time, and performance.

The main goal of this paper is to present an overview of Fog computing in terms of the definition, applications that are taking the benefits of it, and the architecture. Also, to illustrate the challenges and issues facing the Fog computing. Finally, we mention the aspects of Fog computing security and present the advantages of the merge between the Fog and other techniques.

The rest of this paper is organized as follows: Section 2 describes the related works. Section 3 presents a comparison between fog computing & other types. Section 4 describes the Fog computing architecture. Section 5 provides information about primary Fog computing features. Section 6 explained some applications that applied the Fog idea. Section 7 illustrates the challenges and issues facing this technology. Section 8 mentioned the aspects of fog computing security. Section 9 discusses the benefits of integrating between the Fog computing and other techniques. Finally, Section 10 concludes the primary findings from each subject investigated and future work about this paper.

2 Related Work

In this section, we will present some of the previous studies related to fog computing in terms of many aspects. The aspects are definition, applications, challenges, and issues facing. Besides, some studies have merged the Fog computing with other techniques to reduce and solve the problems.

Varshney et al. in [12] study and review the different dimensions of a system consisting of three techniques that are Fog, Cloud, and Edge in terms of three things. Those things are the architecture of this system, characteristics of the application, and abstractions of the system. They demonstrate some new capabilities of two types of computing layers in terms of some things that are "privacy sensitivity, a nascent runtime environment, and the mobility of the physical and application". Then, they clarify the gap between things related to fog computing that are its possibilities and the real reality of Fog. Finally, they mention some challenges and how to solve them to sustain the solution for as long as possible. Examples of these challenges can run the program in fog computing, foretell the users' requirements, and consume the energy in the network.

Aazam et al. in [13] explain the IoT and merge with Cloud computing to 1) improve and provide to the users. 2) Use resources optimally and effectively. Then, they present the architecture of the technology that can solve the problem that occurs for the data before sending to the cloud. This technology is called Smart Gateway with Fog computing. The problem is how to preprocess the data and trimmed before transmits to the cloud. This problem is called data trimming. Also, they evaluate and test this technology using bulk-data upload delay, upload delay, bulk-data synchronization delay, synchronization delay, and jitter.

Luan et al. in [14] present an overview of the Fog computing techniques in terms of the definition,

Muneer Bani Yassein,
Ismail Hmeidi, Farah Shatnawi,
Saif Rawasheh, Omar Alzoubi

major features. Then, they describe the architecture of it and mention some of the issues facing the Fog computing. These issues are "communications between mobile and fog", "communications between cloud and fog", "communications between fogs". Finally, they present the challenges facing the Fog in the deployment process, such as application, scaling, and placement.

Aazam et al. in [15] describe the mechanism of how the Fog is work and how the fog helping the IoT. Then, they integrate the IoT with Cloud computing, named COT. However, both cloud and fog computing have common characteristics, such as data resources, application, storage, infrastructure, and computation. With these similarities, there is a difference between them that is accessing the underlying nodes.

OSANAIYE et al. in [16] describe the architecture of fog computing and some applications. The applications are divided into two categories, which are real-time (healthcare, gaming) and non-real time applications (smart city, smart grid). Finally, they discuss the privacy and security issues that are facing the Fog computing. These issues are (1) shareability and distributed characteristic. (2) selection the ciphertext attack. (3) potential attack nature. (4) privacy leakage. (5) data protection. (6) vulnerable of sensor networks against the threats.

Mansouri et al. in [17] present one of the computing types in terms of providing the allocation of resources of this type to the users of IoT. This providing is done in a hierarchical computing paradigm way that contains the services of fog and remote cloud computing. Then, they propose a new mechanism to solve the time problem of the potential game approach. This mechanism is called a near-optimal resource allocation mechanism. The results show that the usage of fog computing services will be a benefit for many users after using the proposed algorithm.

Jalali et al. in [18] use a method that merges between two things to reduce energy exhaustion that the IoT applications are consumed. These things are microgrids and Fog computing. Microgrids and Fog computing are used together and complement each other to achieve green IoT. The green IoT means that the consuming of the energy at the lowest level. The results show that the usage of microgrids and

Fog computing together is consuming energy at the lowest level as possible.

Yannuzzi et al. in [19] present some of the main challenges facing the IoT. These challenges are reliable control and actuation, mobility, and scalability. They use Fog computing as an appropriate platform of the IoT and how Fog computing is the interplay with Cloud computing in recent years in the IoT domain. Then, they mention the challenges and issues that are related to the mobility, "reliable control and actuation", and data aggregation. These three things are IoT aspects. One of the challenges for mobility is how to able to keep the storage resources and the compute near to the things. while the challenges for reliable control and actuation are the computational power is lack is sensing process. Finally, the challenges for data aggregation are how to deal with a massive amount of data that is needed to apply a set of operations, such as processed and aggregated it.

Aazam et al. in [20] present an attractive task for IoT and Cloud computing applications. This task is called offloading task. They present an overview of the taxonomy of the fog, cloud computing, and IoT. Then, they explain the middleware technologies that will be benefiting in cases cloud-IoT in terms of the uploading. These technologies are Cloudlet, mobile edge computing, micro data center, nano data center, and delay-tolerant network. Also, they discuss some of the criteria used in offloading, such as "accessibility", "load balancing", and "privacy and security". Finally, they mention some of the research challenges in the Fog computing domain. One example of these research challenges is knowing the appropriate amount of resources that will be required for the jobs that are executed at a specific location.

Skarlat et al. in [21] illustrate an architecture of the framework used for providing the fog resources. This framework is called a Fog computing framework. Then, they present an optimization problem that aims to supply utilization for fog computing available resources in terms of delay-sensitive. Finally, the results show that the usage of this framework after applies the idea of the optimization problem, the percentage of delay decreases to 39% when compared with the traditional methods. This percentage means that the time of the round-trip is decreasing.

Muneer Bani Yassein,
Ismail Hmeidi, Farah Shatnawi,
Saif Rawasheh, Omar Alzoubi

MUKHERJEE et al. in [38] overviewed about two concerns and terms of Fog computing, which are privacy and security concerns. Then, they have mentioned some issues, challenges, and research trends of privacy and security for the Fog computing. These issues are trust, authentication, secure communications, end user's privacy, and malicious attacks. While the challenges that faced the Fog computing are "fog forensics", "malicious or malfunctioning fog nodes", "malicious insider attack", and "mutual authentication among dynamic fog nodes and end-users". Finally, for the research trends of fog computing are "privacy preservation", "authentication and key agreement", "intrusion detection systems", "dynamic join and leave of fog node", and "cross-border issue and fog forensic".

Yi et al. in [39] presented an overview of the promising computing paradigm, which called Fog computing. Then, they have mentioned the security and privacy issues that faced this computing paradigm. The overview is about the definition and the characterization of the Fog. The security and privacy issues are 1) Trust. 2) Authentication. 3) Network Security. 4) Secure Data Storage. 5) Secure and Private Data Computation. 6) Privacy. 7) Access Control. 8) Intrusion Detection.

Zhang et al. in [40] illustrated the Fog computing architecture and the security and trust issues that the Fog is faced. Then, they have mentioned the research trends open challenges and future topics for trust and security issues. The architecture of the fog computing that they are mentioned in their paper is consisting of three layers: The Cloud, the Fog and the Edge. The research trends open challenges are 1) Trusted execution environment. 2) Trust and security during Fog orchestration. 3) Access control. 4) Collusion attack. 5) Data-dependent security and context-aware security. 6) Service trust. While the future topics of their paper are: 1) Trust management models. 2) Identification of trusted nodes. 3) Secure orchestration.

In the following table, the techniques, applications, challenges, privacy, and security issues of the previous studies about Fog computing are presented.

Table 1 shows the techniques, applications, challenges, privacy and security issues of the previous studies about fog computing.

Ref.	Objective of their study	Framework or approach used	Challenges & Issues	Computing type	Applications that mentioned or future topics	Results
[12]	They study and review the different dimensions of a system consisting of three techniques that are Fog, Cloud, and Edge	-	1) Can run the program in fog computing 2) Foretell the users' requirements 3) Consume the energy in the network.	1) Fog 2) Cloud 3) Edge	1) Urban Surveillance 2) Smart Power Grid 3) Drones for Asset Monitoring	-
[13]	They explain the IoT and merge with Cloud computing to 1) improve and provide to the users. 2) Use resources in an optimal and effective manner	Smart Gateway with Fog computing	Data trimming	Fog computing	-	After using the Smart Gateway with Fog computing and CoT, it provides rich and many services to users.
[20]	They present an attractive task for IoT and Cloud computing applications	Offloading task	Knows the appropriate amount of resources that will be required for the jobs that are executed at a specific location.	1) Cloud computing 2) Fog computing	-	Decrease power consumption after performing this task

Muneer Bani Yassein,
Ismail Hmeidi, Farah Shatnawi,
Saif Rawasheh, Omar Alzoubi

[21]	They illustrate an architecture of this framework used for providing the fog resources	Fog computing framework	Delay-sensitive for fog computing available resources	Fog computing	-	Usage of this framework after applies the idea of the optimization problem, the percentage of delay decreases to 39% when compared with the traditional methods.
[22]	They study the essential characteristics of the IoT to prevent the scaling of the GDP.	Global Data Plane (GDP)	1) Scalability 2) Privacy and Security 3) Modeling 4) Latency 5) Bandwidth	Cloud computing	1) Put the sensors in building, homes, etc. 2) Real-time applications	-
[23]	They present the data interplay approach for the Fog of Things and addresses the problems between the infrastructures of Cloud and Fog.	Data Interplay approach	-	1) Cloud computing 2) Fog computing 3) Edge computing	-	This approach is flexible and can be reconfigured to run other scenarios in IoT. Also, this approach can handle the big volume generation between the infrastructures of Cloud and Fog.
[24]	They study the effect of the extended cloud on two things: 1) current communication. 2) Models of the cloud networking service.	-	1) Less control over three things, which are the data, software, and hardware. 2) The cost is important in case of the cloud failure. 3) Jamming attacks 4) Weak authentication	1) Cloud computing 2) Fog computing 3) Edge computing	1) High-quality camera 2) GPS 3) Barometer	-
[25]	They are explained the enable to apply the IoT in many applications, such as healthcare and medicine and mention some challenges facing the IoT.	IoT ehealth ecosystem	1) Data management 2) Scalability 3) Regulations 4)Interoperability device-network-human interfaces 5) Security 6) Privacy	1) Cloud computing 2) Fog computing	1) Healthcare 2) Medicine 3) Ambient Assisted Living 4) IoT Medication 5) Smart Medical Implants	-
[38]	They are overviewed about two concerns and terms of Fog computing, which are privacy and security concerns, some issues and challenges.	-	1) Trust 2) Authentication 3) Secure communications 4)End user's privacy 5) malicious attacks	Fog computing	-	-
[39]	They are presented an overview about promising computing paradigm, which called Fog computing. Then,	-	1) Trust. 2) Authentication. 3) Network Security. 4) Secure Data Storage.	Fog computing	-	-

Muneer Bani Yassein,
Ismail Hmeidi, Farah Shatnawi,
Saif Rawasheh, Omar Alzoubi

	they are mentioned the security and privacy issues that faced this computing paradigm		5) Secure and Private Data Computation. 6) Privacy. 7) Access Control. 8) Intrusion Detection.			
[40]	They are illustrated the Fog computing architecture and the security and trust issues that the Fog is faced. Then, they have mentioned the research trends open challenges and future topics for trust and security issues	-	1) Trusted execution environment. 2) Trust and security during Fog orchestration. 3) Access control. 4) Collusion attack. 5) Data-dependent security and context-aware security. 6) Service trust.	Fog computing	Future topics: 1) Trust management models. 2) Identification of trusted nodes. 3) Secure orchestration	-

3 Comparison Between Fog Computing & Other Types

There are three similar technologies for Fog computing that there are difference and similar between them. These technologies 1) Edge Computing. 2) Cloudlet. 3) Micro-data centre [36].

Despite the similarities between the Fog Computing and Cloud Computing, there are many differences among them, such as Scheduling tasks, latency, determine the schedule computational tasks location, independently, Mobility and others [6, 32] as shown in Table 2.

Table 2 Comparing between Fog and Cloud computing.

	Fog	Cloud
Scheduling tasks	Complex	Simple
latency	The latency of the application is unpridicable	The latency of the application is pridicable
schedule computational tasks location	Difficult	Not difficult
independently	The owner from	Form one

	more organizations	organization
Mobility	The applications are deployed in defferent nodes	The applications are deployed in only one cloud at a time
Location awareness	Yes	No
Deployment	Distributed	Centralized
Security measures	Hard to define	Defined
Distance between client and server	One hop	Multiple hops
Working environment	Outdoor (e.g., Streets, gardens) or indoor	Warehouse-size building with air conditioning systems
Attack on data	High probability	Less probability

Table 3 shows the comparison between Fog Computing, Mobile-Edge Computing and Cloudlet Computing based on Node devices, Node location, Software Architecture, Context awareness, Proximity, Access Mechanisms, and Internode Communication [37].

Table 3 Comparison between Fog Computing, Mobile-Edge Computing and Cloudlet Computing.

	Fog	Mobile-Edge	Cloudlet

Muneer Bani Yassein,
Ismail Hmeidi, Farah Shatnawi,
Saif Rawasheh, Omar Alzoubi

	Computing	Computing	Computing
Node devices	Routers Switches Access Points Gateways	Servers running in base stations	Data Center in a box
Node location	Varying between End Devices and Cloud	Radio Network Controller/Macro Base Station	Local/Outdoor installation
Software Architecture	Fog Abstraction Layer based	Mobile Orchestrator based	Cloudlet Agent based
Context awareness	Medium	High	low
Proximity	One or Multiple Hops	One Hop	One Hop
Access Mechanisms	Bluetooth, Wi-Fi, Mobile Networks	Mobile Networks	Wi-Fi
Internode Communication	Supported	Partial	Partial

4 Fog computing Design

Fog Computing has an architecture that contains several layers. All the researchers are agreed to the number of layers, which are six layers. These layers are "physical and virtualization layer", monitoring layer, pre-processing layer, temporary storage layer, security layer, and transport layer [5, 6, and 26] as shown in figure 1.
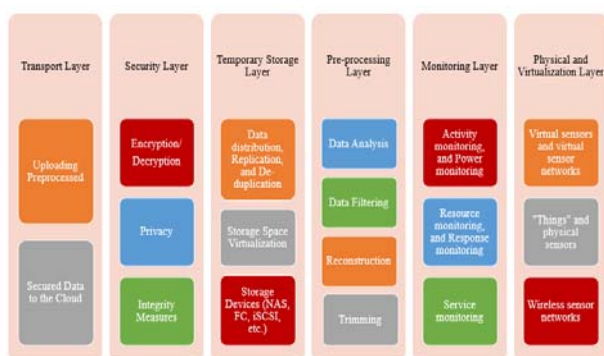

Fig.1 The architecture of the Fog Computing

4.1 Physical and virtualization layer

This layer includes several kinds of nodes like virtual sensor networks, virtual nodes, and physical nodes. These nodes are controlled based on the requirements that needed and their types. The aim of these nodes is sending the data that are collected to the monitoring layer and other upper layers. Due to the data need for more filtering and preprocessing steps [5, 6, and 26].

4.2 Monitoring Layer

Many monitoring tasks happened in this layer [5, 6, and 26]. These tasks are 1) usage of the resources. 2) Check if the nodes are available or not. 3) Managing all the tasks in the networks that the nodes will do it. 4) Monitoring the amount of energy that is effectively consumed by the nodes.

4.3 Pre-processing Layer

The aims of this layer are analyzing the data that are collected in the first layer and applied the preprocessing, trimming, and filtering processes on the data [5, 6, and 26].

4.4 Temporary storage Layer

This layer is used to store the data after filtering and preprocessing processes in the previous layer [5, 6, and 26].

4.5 Security Layer

To protect the data, many techniques and measures that applied in this layer, such as decryption or encryption, and integrity techniques [5, 6, and 26].

4.6 Transport Layer

In the last layer, after applying the decryption or encryption, integrity techniques, filtering and preprocessing, the data is sent to the cloud to extract and establish many useful services to the users [5, 6, and 26].

5 Fog Computing: Characteristics, Cons and Pros

This section will provide insights into the characteristics, several advantages and

disadvantages of Fog computing, which can facilitate the readers to understand this technology easily. We will illustrate the characteristics, several advantages and disadvantages in details as follows:

5.1 Fog Computing Characteristics

For anything or type found on the Internet network, it has several characteristics that distinguish it from others. In this subsection, we will present the characteristics of Fog computing that shown as follows:

1) Fog computing can deploy and distribute services and applications anywhere on the network [6].

2) Fog computing can publish and distribute the nodes in different locations [6].

3) The possibility of dealing with different service providers and working in different areas at the same time [6].

4) Ability to handle and process data that is within the range of end devices [6].

5) Ability to deal with different devices and different platforms [6].

6) The data in Fog computing is secure and private by applying many techniques, such as encryption and isolation [27].

7) The Fog nodes do not consume a lot of energy; due to the nodes are dispersed in the network [27].

5.2 Fog Computing Advantages

By the presence of the Fog computing in our life and its quick spreading in several locations in the computing network. The users were increased because it has many advantages and benefits, such as:

1) Fog computing provides services that are characterized by high quality compared to computing, high data transfer rate, time service latency is low [4, 14, and 28].

2) This computing reduces the back and forth movement between the cloud and the users of the mobile devices; which lead to improving network efficiency and reducing power consumption [4, 14].

3) Fog computing is appropriate for the tasks and queries that happened in IoT [4].

4) Fog computing allows increasing the number of devices connected to the network [6].

6) Saving the bandwidth; data is processed locally instead of sent and processed in the cloud [6].

7) It supports many applications with latency requirements as low as possible, such as augmented reality and gaming [39].

5.3 Fog Computing Disadvantages

There are many difficulties and disadvantages of Fog computing, the most prominent and most important are:

1) Companies that used Fog computing, needed to buy many expensive devices such as gateways, routers, and hubs [29].

2) Very complex system; due to using a lot of nodes, and it needs another layer compared with the cloud to two processes that are storage systems and data processing [29].

3) Compared with cloud computing, it is less scalable in terms of the number of devices and services provided [29].

6 Fog Computing Applications

In the Fog Computing, there are many applications used that apply the Fog idea. These applications are urban surveillance, smart power grid, drones for asset monitoring [12], shopping center, senary park, inter-state bus [14], smart home, smart vehicle, health data management [7], healthcare, augmented reality, caching and preprocessing [4], real-time applications (i.e. video streaming, and gaming) and near-real-time applications (i.e. smart cities) [16] smart environments, vehicular fog computing web optimization [27], and mobile big data analytics [31].

We explained two applications that supported by the Fog computing as examples:

6.1 Augmented Reality (AR)

Muneer Bani Yassein,
Ismail Hmeidi, Farah Shatnawi,
Saif Rawasheh, Omar Alzoubi

AR is a famous application om many devices like tablet smartphone, and smart glasses. It is needing a high power to run the video and high bandwidth to send the data [31]. So, the time of processing and sending the data must be as low as possible. The Fog computing provided this time; it maximizes throughput and minimizes the latency in both processing and sending the data [31].

6.2 Mobile Big Data Analytics

It is an important topic for big data architecture in both cloud and mobile cloud. So, the latency in both are high and facing some issues. For these reasons, the fog computing support flexible resources for a huge system that used to process the data without facing the reasons [31].

7 Challenges and Issues of Fog computing

Many challenges and issues facing Fog computing. In this section, we will illustrate in brief some of these challenges and issues.

7.1 Security and Privacy: issues and solution

7.1.1 Security and Privacy: Issues

Fog computing devices are facing some security and privacy issues and attacks; because it is spread in locations are not close to the locations that are protected and monitored [1]. For this reason, it is suffering from different attacks, as follow:

1) Data hijack, and eavesdropping [1].

2) Man-in-the-middle attack; penetration of fog devices that work as a gateway [1, 8, and 41].

3) Malicious attack; the data in the Fog nodes are not fair and forged by a malicious node [8].

4) Problems in the data protection; due to the lack of resources that help to encrypt or decrypt the data [8].

5) Issues in manage the data; ensure and check if the node provides and support the same services for the users [8].

6) Denial of services; there are many services and requests in the Fog. It is difficult of the Fog is dealing with the huge number of services at the same time. So, the network is busy and does not provide and services for the end-users [27].

7) Fog computing is threatened and vulnerable to many security attacks because it is developed upon traditional networking components, not the modern components [33].

8) Rogue Node Detection; malicious node in IoT collect the data and exchange it for malicious purposes [34].

9) Privacy location; if the location of IoT devices is known, the data in it can be stolen [34].

10) Authentication problem in the network [41].

7.1.1 Security and Privacy: Solutions

There are a lot of security solutions of the issues that faced the fog computing, such as:

1) Fog computing: Privacy-preserving: to ensure that the data secured between end-user device and Fog network, there are five steps as a following: 1) collect secure data and extract features from it. 2) Data fuzzing. 3) Segregation. 4) Public Key Infrastructure should be Implemented. 5) Sending the segregated data to Fog node. [36].

2) Reducing data theft from inside the network: to reduce and mitigate the security threats, it should be used the components of both Fog and cloud computing together. This combined between two things to mitigate the threats: decoy methods and behaviour profiling [36].

3) Using Public key infrastructure (PKI) to solve the aauthentication problem in Fog network [36, 41].

4) Using advance encryption standard (AES): it is suitable algorithm for fog network in term of encryption of data. So, it should be used in any fog computing network to ensure the security of the data [36].

7.2 Control and management issues

1) The nature of the nodes is mobility; so the changes are frequently that lead to some metrics

also changes like latency, storage, bandwidth, and computation [27].

2) The platform is different from user to user; so the resources are run in a heterogeneous way [27].

7.3 Fog Networking

The fog network is heterogeneous because it placed on the internet edge. So, controlling and managing some services is not easy, such as providing services, maintaining connectivity and network. To do these services in flexible ways, there are two Emerging techniques that used. These Emerging techniques are network function virtualization (NFV), and software-defined networking (SDN) [31].

7.4 Task Scheduling

The scheduling of the task is not easy in the fog computing, because the task can move between the various physical devices like fog nodes, back-end cloud servers and client devices [32].

7.5 Heterogeneous

The nodes in Fog network are heterogeneous, because no guarantee or confirmation that the same sources exist in each node [32].

7.6 Power Consumption

Because the huge number of nodes in the Fog network, it consumes a lot of power. To reduce the power, there are many effective protocols that are used like effective filtering CoAP, and sampling techniques [35].

8 Aspects of fog computing Security

There are many aspects and things are important for security techniques to handle the security issues and problems that faced Fog computing as mentioned in the previous section. In this section, we will be presented these aspects and shallow details of each of them as shown in Fig.2 [30].
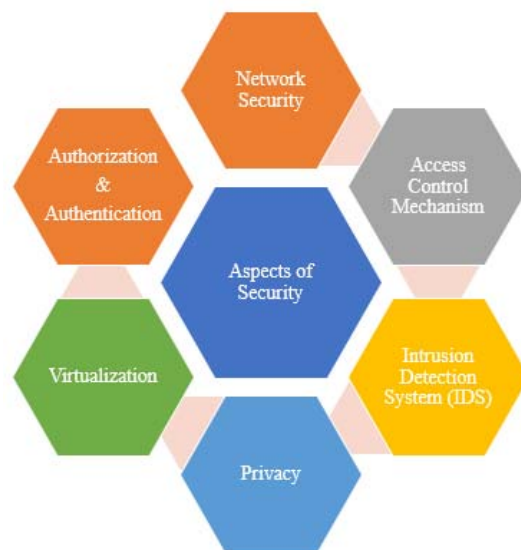

Fig.2 Aspects of Fog Computing Security

8.1 Authorization and Authentication

These techniques are important for Fog Computing, because the Fog computing is an open network that enable for a huge number of devices connect with the network. So, the definition of each of them as a following: the authorization referring to the "who is who?" and the authentication referring to the "who can do what?" [30].

8.2 Network security

The network acts as a bridge between the network components, such as end nodes, local infrastructure, and core infrastructure. So, if the network ensures the security between these components, the whole system is also secure [30].

8.3 Access control mechanism

There is a low difference between the access control and the authorization. The access control it is guarantee for each node the right to obtain the authorization [30].

8.4 Intrusion Detection System (IDS)

The IDS warm the administrator of the system from any attack that faced the network; to protects the system [30].

8.5 Privacy

Muneer Bani Yassein,
Ismail Hmeidi, Farah Shatnawi,
Saif Rawasheh, Omar Alzoubi

The privacy is important term of security techniques in terms of "privacy of services used", "privacy of location", and "privacy of data and information" [30].

8.6 Virtualization

The virtualization is a necessary mechanism in the network to check and ensure the system security in terms of smooth working [30].

9 Integrating between Fog computing with other techniques

In this section, we present the benefits of merging between the Fog computing with other techniques, and what the challenges that the single techniques are facing before the merging process.

9.1 Fog computing with IoT

There are many limitations and challenges that the IoT facing, such as latency constraints, network bandwidth constraints, resource-constrained devices, uninterrupted services, and IoT security challenges as shown in Table 4. To handle and to mitigate these limitations and challenges, Fog computing is popular and suitable technique. For example, the latency constraints limitation, the Fog computing is performing all the operations that near to the end-users [6]. These operations are analyzing and managing the data. While for the network bandwidth constraints limitation, the Fog computing allowing the data processing that based on the application's requirements; this process is reducing the data that sent to the cloud, so, the bandwidth of the network is saved [6].

Table 4 Limitations of IoT and Fog solutions

Limitations of IoT	Solutions of Fog
Latency Constraints	Fog computing is performing all the operations near to the end-users.
Network Bandwidth Constraints	The data processing is enabled and performed based on the applications needed. So, the bandwidth of the network is reduced.
Resource-Constrained Devices	It used to run operations that need a huge amount of resources. So, costs and power consumption are reduced.
Uninterrupted Services	It runs independently to make the services in the network continuously.
IoT Security	The Fog computing plays as a act the

Challenges	proxy for devices that have not enough security.

9.2 Fog computing with Cloud computing

There are many limitations and issues that faced in the many domains like IoT in Healthcare, Cloud Computing, when they performed the Fog Computing alone or with other computing types; these limitations can be handled as shown in Table 5.

To address the problems and issues that facing the IoT in Healthcare, the merging between the Fog and cloud is the possible solution [9]. The problems and issues are uneven data load, diverse user expectations, heterogeneity of the applications, and latency sensitivity. The main aim of this merging is to construct the solutions to many things, such as machine learning, sensors, and recommendation systems [9]. Despite these pros, the challenges of this merging are service orchestration cloud-edge service management, and intelligent health sensors [9].

Although, the cloud computing only facing many problems and issues like the architecture is geographically centralized and more than one hop distance from the IoT data source. To handle these issues, a new computing type called Fog Computing is used at the edge network. This type has met the issues that Cloud computing faced [9].

Table 5 Limitations of cloud and Fog solutions

Limitations		Solutions
The limitations that facing the IoT in Healthcare domain	Uneven data load	When merge the Cloud computing with the Fog Computing, these limitations are handled and reduced.
	Diverse user expectations	
	Heterogeneity of the applications	
	Latency sensitivity	
Cloud Computing	Architecture is geographically centralized	When it performed the Fog Computing at the edge network, these limitations are met and handled.
	More than one hop distance from the iot data source	

10 Conclusion and Future work

Muneer Bani Yassein,
Ismail Hmeidi, Farah Shatnawi,
Saif Rawasheh, Omar Alzoubi

In this paper, we illustrated the widely used technology among researchers in the present era in terms of many aspects, which called Fog computing. These aspects are the six layers that the architecture consists of, and the primary features of it that are "characteristics, advantages, and disadvantages" and applications of it. Also, the challenges and issues facing Fog computing, such as security issues, privacy issues, control management issues, task scheduling, heterogeneous, and power consumption are highlighted. Then, we mentioned the Aspects of Fog Computing Security, such as "authorization and authentication", network security, access control mechanism, IDS, privacy, and virtualization. Finally, we discussed the benefits of the merging of fog computing with IoT and Cloud separately. Some of these benefits are solved and reduced the problems facing the IoT and Cloud.

In the future work, we will discuss in details the challenges and issues and we will present some solutions to these issues. Also, we will learn how to apply one of these applications mentioned in this paper in the real world. Finally, we will build a Fog computing network. Similar studies can be found in [42], 43], [44].

References:

[1] I. Stojmenovic, S. Wen, X. Huang and H. Luan, An overview of Fog computing and its security issues, *Concurrency and Computation: Practice and Experience*, Vol.28, NO.10, 2015, pp. 2991-3005.

[2] F. Bonomi, R. Milito, J. Zhu and S. Addepalli, Fog computing and its role in the internet of things, *Proceedings of the first edition of the MCC workshop on Mobile cloud computing - MCC '12*, 2012.

[3] M. Aazam and E. Huh, "Fog Computing Micro Datacenter Based Dynamic Resource Estimation and Pricing Model for IoT", 2015 IEEE 29th International Conference on Advanced Information Networking and Applications, 2015.

[4] A. Dastjerdi, H. Gupta, R. Calheiros, S. Ghosh and R. Buyya, Fog Computing: principles, architectures, and applications, *Internet of Things, 2016,* pp. 61-75.

[5] M. Aazam, S. Zeadally and K. Harras, Fog Computing Architecture, Evaluation, and Future Research Directions, *IEEE Communications Magazine,* VOL.56, NO.5, 2018, pp. 46-52.

[6] H. Atlam, R. Walters and G. Wills, Fog Computing and the Internet of Things: A Review, *Big Data and Cognitive Computing*, VOL.2, NO.2, 2018, p. 10.

[7] S. Yi, Z. Hao, Z. Qin and Q. Li, Fog Computing: Platform and Applications, *2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*, 2015.

[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, *2015 6th International Conference on the Network of the Future (NOF),* 2015.

[9] R. Mahmud, F. Koch and R. Buyya, Cloud-Fog Interoperability in IoT-enabled Healthcare Solutions, *Proceedings of the 19th International Conference on Distributed Computing and Networking - ICDCN '18*, 2018.

[10] J. An et al., EiF: Toward an Elastic IoT Fog Framework for AI Services, *IEEE Communications Magazine*, VOL.57, NO.5, 2019, pp. 28-33.

[11] A. Munir, P. Kansakar, and S. Khan, IFCIoT: Integrated Fog Cloud IoT Architectural Paradigm for Future Internet of Things, *arXiv preprint arXiv:1701.08474,* 2017.

[12] P. Varshney and Y. Simmhan, Demystifying Fog Computing: Characterizing Architectures, Applications and Abstractions, *2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC),* 2017.

[13] M. Aazam and E. Huh, Fog Computing and Smart Gateway Based Communication for Cloud of Things, *2014 International Conference on Future Internet of Things and Cloud,* 2014.

Muneer Bani Yassein,
Ismail Hmeidi, Farah Shatnawi,
Saif Rawasheh, Omar Alzoubi

[14] T. H. Luan, L. Gao, Z. Li, Y. Xiang, G. Wei, and L. Sun, Fog Computing: Focusing on Mobile Users at the Edge, *arXiv:1502.01815 [cs]*, Feb. 2015.

[15] M. Aazam and E. Huh, Fog Computing: The Cloud-IoT\/IoE Middleware Paradigm, *IEEE Potentials*, VOL.35, NO.3, pp. 40-44, 2016.

[16] O. Osanaiye, S. Chen, Z. Yan, R. Lu, K. Choo and M. Dlodlo, From Cloud to Fog Computing: A Review and a Conceptual Live VM Migration Framework, *IEEE Access*, VOL.5, 2017, pp. 8284-8300.

[17] H. Shah-Mansouri and V. Wong, Hierarchical Fog-Cloud Computing for IoT Systems: A Computation Offloading Game, *IEEE Internet of Things Journal*, VOL.5, NO.4, 2018, pp. 3246-3257.

[18] F. Jalali, A. Vishwanath, J. de Hoog and F. Suits, Interconnecting Fog computing and microgrids for greening IoT, *2016 IEEE Innovative Smart Grid Technologies - Asia (ISGT-Asia)*, 2016.

[19] M. Yannuzzi, R. Milito, R. Serral-Gracia, D. Montero and M. Nemirovsky, Key ingredients in an IoT recipe: Fog Computing, Cloud computing, and more Fog Computing, *2014 IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2014.

[20] M. Aazam, S. Zeadally and K. Harras, Offloading in fog computing for IoT: Review, enabling technologies, and research opportunities, *Future Generation Computer Systems*, VOL.87, 2018, pp. 278-289.

[21] O. Skarlat, S. Schulte, M. Borkowski and P. Leitner, Resource Provisioning for IoT Services in the Fog, *2016 IEEE 9th International Conference on Service-Oriented Computing and Applications (SOCA)*, 2016.

[22] B. Zhang et al., The Cloud is Not Enough: Saving IoT from the Cloud, *presented at the 7th {USENIX} Workshop on Hot Topics in Cloud Computing (HotCloud 15)*, 2015.

[23] L. Andrade, M. Serrano and C. Prazeres, The Data Interplay for the Fog of Things: A Transition to Edge Computing with IoT, *2018 IEEE International Conference on Communications (ICC)*, 2018.

[24] S. Shirazi, A. Gouglidis, A. Farshad and D. Hutchison, The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog From a Security and Resilience Perspective, *IEEE Journal on Selected Areas in Communications,* VOL.35, NO.11, 2017, pp. 2586-2595.

[25] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant and K. Mankodiya, Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare, *Future Generation Computer Systems*, VOL.78, 2018, pp. 659-676.

[26] M. Aazam and E. Huh, Fog Computing: The Cloud-IoT\/IoE Middleware Paradigm, *IEEE Potentials*, VOl.35, NO.3, 2016, pp. 40-44.

[27] 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, 201, pp. 27-42.

[28] M. Firdhous, O. Ghazali, and S. Hassan, Fog Computing: Will it be the Future of Cloud Computing?, 2014, p. 8.

[29] M. Chakraborty, Fog Computing Vs. Cloud Computing, *SSRN Electronic Journal*, 2019.

[30] B. Abbasi and M. Shah, Fog computing: Security issues, solutions and robust practices, *2017 23rd International Conference on Automation and Computing (ICAC)*, 2017.

[31] S. Yi, C. Li and Q. Li, A Survey of Fog Computing, *Proceedings of the 2015 Workshop on Mobile Big Data - Mobidata '15*, 2015.

[32] Z. Hao, E. Novak, S. Yi and Q. Li, Challenges and Software Architecture for Fog Computing, *IEEE Internet Computing*, VOL.21, NO.2, 207, pp. 44-53.

[33] R. Mahmud, R. Kotagiri and R. Buyya, "Fog Computing: A Taxonomy, Survey and Future Directions", Internet of Things, pp. 103-130, 2017.

Muneer Bani Yassein,
Ismail Hmeidi, Farah Shatnawi,
Saif Rawasheh, Omar Alzoubi

[34] 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, NO.2, 2017, pp. 34-42.

[35] A. Dastjerdi and R. Buyya, Fog Computing: Helping the Internet of Things Realize Its Potential, *Computer*, VOL.49, NO.8, 2016, pp. 112-116.

[36] S. Khan, S. Parkinson and Y. Qin, Fog computing security: a review of current applications and security solutions, *Journal of Cloud Computing*, VOL.6, NO.1, 2017.

[37] K. Dolui and S. Datta, Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing, *2017 Global Internet of Things Summit (GIoTS)*, 2017.

[38] M. Mukherjee et al., Security and Privacy in Fog Computing: Challenges, *IEEE Access*, VOL.5, 2017, pp. 19293-19304.

[39] S. Yi, Z. Qin and Q. Li, "Security and Privacy Issues of Fog Computing: A Survey", Wireless Algorithms, Systems, and Applications, pp. 685-695, 2015.

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

[41] I. Stojmenovic and S. Wen, The Fog Computing Paradigm: Scenarios and Security Issues, *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems*, 2014.

[42] Roumen Trifonov, Slavcho Manolov, Georgi Tsochev, Galya Pavlova, Automation of Cyber Security Incident Handling through Artificial Intelligence Methods, *WSEAS Transactions on Computers,* Volume 18, 2019, pp. 274-280

[43] Csilla Czeglédi, Klára Veresné Valentinyi, Eszter Borsos, Éva Járási, Zoltán Szira, Erika Varga, News Consuming Habits of Young Social Media Users in the Era of Fake News, *WSEAS Transactions on Computers*, Volume 18, 2019, pp. 264-273

[44] Nursel Selver Ruzgar, Comparison of Classification Algorithms on Financial data, *WSEAS Transactions on Computers,* Volume 18, 2019, pp. 256-263