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

MUNEER BANI YASSEIN, OMAR ALZOUBI, SAIF RAWASHEH,
FARAH SHATNAWI, ISMAIL HMEIDI
Computer Science Department
Jordan University of Science and Technology
Irbid
JORDAN

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

Abstract: - Fog computing is a promising technology that is used by many organizations and end-users. It has characteristics and advantages that offer services such as computing, storage, communication, and application services. It facilitates these services to end-users and allows to increase the number of devices that can connect to the network. In this paper, we provide a survey of Fog computing technology in terms of its architecture, features, advantages and disadvantages. We provide a comparison of this model with Cloud Computing, Mobile-Edge Computing, and Cloudlet Computing. We also present challenges and issues that face Fog Computing such as privacy and security, control and management, fog networking and task scheduling. Finally, we discuss aspects of Fog computing security and the benefits of integration between Fog computing and other techniques like Internet of Things and Cloud Computing.

Key-Words: - Fog computing, Fog Architecture, Security issues, Merging idea, Privacy issues, Control and management issues, Security Aspects

Received: December 1, 2019. Revised: March 31, 2020. Accepted: April 11, 2020. Published: April 30, 2020.

1 Introduction

Fog computing is new promising highly virtualized computing model that extends the services of cloud computing to the edge network services [1, 2, 3, and 4]. It is suitable for use in wireless sensor networks (WSNs) and IoT [3]. It also supports heterogeneity of appliances, such as Fog appliances, where these appliances are end-users, switches, edge routers, and access points [1]. Fog computing provides many services to the network such as computing, application services, location awareness and quality-of service (QoS) for streaming and real-time applications, storage, networking services between end devices and traditional cloud computing data centers [1, 2].

The basic 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 can benefit from Fog computing, such as augmented reality, smart homes, smart grid, health data management, smart factories, and smart vehicles [4, 7].

The challenges and issues that are facing Fog computing include; data protection, malicious Fog node, detection of intrusions., and Man-in-the-Middle attack, besides others[1, 8]. Security is one of the most challenging issues that face Fog computing [6]. It includes authorization and authentication, network security, access control mechanism, intrusion detection system (IDS), privacy, and virtualization [30]. Many researchers tried to integrate Fog computing with different types of computing such as Cloud Computing. The aim is

to enhance performance and tackle the limitations with these techniques. For example, 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. Similarly, An et al. [10] integrated the Fog, IoT, and artificial intelligence (AI). They aimed 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). Moreover, Munir et al. [11] integrated three techniques to increase scalability, sensor energy, latency, response time, and performance in IoT applications. This paper presents a review of Fog computing, its architecture, applications that may benefit of. It Also illustrates the challenges and issues that are facing Fog computing. Finally, we discuss aspects of Fog computing security and present the advantages of integrating the Fog with other techniques. The rest of this paper is organized as follows: Section 2 provides and discusses related works. Section 3 presents a comparison between Fog computing & other types of such as Cloud. Section 4 describes the Fog computing architecture. Section 5 presents primary Fog computing features. Section 6 explains some applications that may benefit from the Fog. Section 7 illustrates the challenges and issues facing this technology. Section 8 discusses aspects of Fog computing security. Section 9 presenst the benefits of integrating Fog computing and other techniques. Finally, Section 10 concludes the primary findings from each subject investigated and future work.

2 Related Work

In this section, we present some of previous research related to Fog computing in terms of its definition, architecture, applications, issues and challenges, and efforts of integrating Fog computing with other computing techniques.

For example, Varshney et al. [12] studied and reviewed different dimensions of a system consisting of three integrated computing techniques that are Fog, Cloud, and Edge. They discussed the architecture, characteristics of the application, and abstractions of the system. They demonstrated some new capabilities of two types of layers, the physical and application layers, in terms of privacy sensitivity, and mobility of the two layers. Then, they discussed the protentional of Fog computing and its applicability. Finally, they mentioned some challenges and how to solve them in order to maintain a sustained solution. Examples of such challenges included running program in a Fog computing environment, foretell user requirements, and network energy consumption. Similarly, Aazam et al. in [13] explained an integrated system that combines IoT and Cloud computing that can use resources optimally and effectively. They presented an architecture of the technology for data transmission form IoT to the Cloud. This call it Smart Gateway with Fog computing. The main issue was on how to preprocess and trim the data before transmitting to the cloud. They evaluated and tested this technology using bulk-data upload delay, upload delay, bulk- data synchronization delay, synchronization delay, and jitter. Moreover, Luan et al. in [14] presented an overview of the Fog computing techniques. They discussed the architecture used and issues facing Fog computing. These issues included; communications between mobile and Fog, communications between cloud and Fog, and communications between Fogs. Finally, they presented challenges facing the Fog in the deployment process, such as application, scaling, and placement. Additionally, Aazam et al. in [15] described the mechanism of how the Fog works and how the Fog can help IoT. They presented a system that integrated IoT with Cloud Computing, named COT. Both Cloud and Fog computing have common characteristics, such as data resources, application, storage, infrastructure, and computation. However, there is a difference between them in accessing the underlying nodes. Osanaiye et al. [16] presented some applications of Fog computing. The applications are divided into two categories, which are real-time (healthcare, gaming) and non-real time applications (smart city, smart grid). They discussed privacy and security issues that are facing Fog computing. These include; (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. [17] presented a mechanism called a near-optimal resource allocation mechanism, that can be used for allocation of resources to users of IoT. This is done in a hierarchical computing paradigm way that contains the services of Fog and remote Cloud computing. They showed that the usage of Fog computing services can provide

benefits to users after using t he proposed mechanism. Similarly, Jalali et al. in [18] used a method that merges between microgrids and Fo g computing to reduce en ergy exhaustion that IoT applications are concerned. Microgri ds and Fog computing can complement each othe r to achieve green IoT. The green IoT means that consuming of energy is at the lowest level.

Yannuzzi et al. in [19] presented some of the main challenges facing IoT, these include reliable control and actuation, mobility, and scalability. They used Fog computing as an app ropriate platform for IoT. They described the ch allenges that included mobility, reliable control and actuation, and data aggregation, which are IoT aspects. One of the challenges for m obility is how to be able to keep computing and storage res ources near to the things. While the challenges for reliable control and actuation is the lack of computational power in sensing processes. Finally, the challenges for data aggregation are how to deal with a massive amount of data that need to processed and aggregated.

Aazam et al. [20] presented an attracti ve task for IoT and Cloud co mputing applications. This task is called offloading task. They presented an overview of the taxono my of the Fog, Cloud co mputing, and IoT. Then, the y explained the middleware technologies that will be benefiting in cloud-IoT in terms of the uploading. These t echnologies are Cloudlet, mobile edge computing, micro data center, nano data center, and delay -tolerant network. Also, they discussed some of the criter ia used in offloading, such as accessibility, load balancing, and privacy and security. Finally, they mentioned some of the research challeng es in the Fog com puting domain. One example of these res earch challenges is knowing the appropriate am ount of resources that will be requi red for the j obs that are executed at a specific location.

Skarlat et al. [21] illustrated a framework used for providing the Fog resources. This fr amework is called a Fog co mputing framework. They presented an optimization problem that aim s to supply utilization for Fog co mputing available resources in terms of del ay-sensitivity. They showed that the framework helps in decreasing the percentage of delay to 39% when co mpared with the traditional methods. This percentage means that the time of the round-trip is decreasing. Mukherjee et al. [38] provided an overview of two main challenges in Fog computing, which are privacy and security concerns. Then, they mentioned some issues, chal lenges, and research trends of privac y and security for the Fog computing. These issues are trust, a uthentication, secure communications, end user privacy, and malicious attacks. While the challenges that fa ced the Fog computing are F og forensics, malicious or malfunctioning fog nodes, malicious insider attack, and mutual authentication am ong dynamic fog nodes and end-users. The rese arch trends of Fog computing are privacy preservation, a uthentication and key agreement, intrusion detection s ystems, dynamic join and leave of Fog node , and cross-border issue and fog forensic. Yi et al. [39] presented an overview of the promising Fog computing paradigm. They have discussed se curity and privacy issues that faced this computing paradigm. 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. [40] illustrated security and trust issues t hat the Fog faces. They have also mentioned research trends, open challenges and future topics for trust and security issues. The a rchitecture of the Fog com puting that they mentioned in their paper consists of three layers; the Cloud, the Fog, and th e Edge. The research trends and open challenges were 1) Trusted execution environment. 2) Trust and security during Fog orchestration. 3) Acc ess control. 4) Collusion attack. 5) D ata-dependent security and context-aware security. 6) Service trust. While future topics of their paper are: 1) Tr ust management models. 2) Identification of trusted no des. 3) Secure orchestration.

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

Table. 1 shows techniques, applications, challenges, privacy and security issues of Fog computing studies.

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 techn iques that are Fog, Cloud, and Edge	-	1) Can run th e program in fo g computing 2) Foretell the users' requirements 3) Consume the energy in th e network.	1) Fog 2) Cloud 3) Edge	1) Urban Surveillance 2) Smart Power Grid 3) Drones for A sset 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 r equired for the jobs tha t are executed at a specific location.	1) Cloud computing 2) Fog computing	-	Decrease power consumption after performing this task
[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 id ea 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, they are mentioned the security and privacy issues that faced this computing paradigm	-	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.	Fog computing	-	-
[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 Fog Computing Vs. Other Types

There are three technologies that have similarities and differences with Fog computing. These technologies are Edge Computing, Cloudlet, and Micro-data center [36]. Despite the similarities between the Fog computing and Cloud Computing, there are many differences among them, such as Scheduling tasks, latency, determining the schedule computational tasks location, in dependence, Mobility and others [6, 32]. These are 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
Independence	The owner from more organizations	Form one 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 Computing	Mobile-Edge Computing	Cloudlet 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. There is a consensus on 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. The following describes the function of each layer.

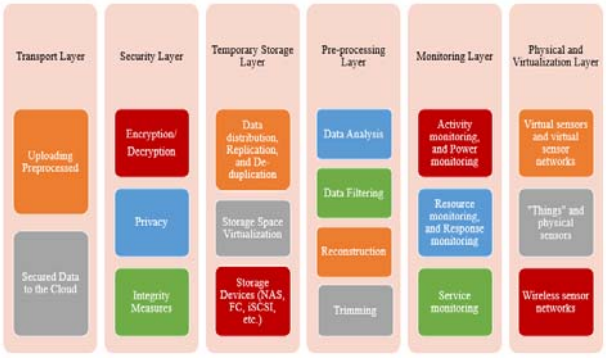

Fig.1 The architecture of the Fog computing

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

Monitoring Layer. Many monitoring tasks occurs at this layer [5, 6, and 26]. These tasks are, usage of the resources, check for nodes availability, task management of nodes, monitoring the amount of energy that is effectively consumed by the nodes.

Pre-processing Layer. The aim of this layer is to analyze the data that are collected in the first layer. The data then preprocessed, trimmed, and filtered [5, 6, and 26].

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

Security Layer. This layer is responsible for data protection. Techniques that applied are applied in this layer include decryption and encryption, and checking data integrity [5, 6, and 26].

Transport Layer. The transport layer is used to send the processed data to the cloud. The data will then be available to end users for extraction and establishing many useful services to users [5, 6, and 26].

5 Fog Computing: Characteristics, Advantages and Disadvantages

The characteristics of Fog computing may include the following; 1) deployment and distribution of services and applications anywhere on the network [6], 2) publishing and distribution of nodes at different locations [6], 3) The possibility of dealing with different service providers and working at 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 being dispersed in the network [27].

Fog computing technology increasingly being adopted, and this is due to a number of advantages that it offers that may include; 1) providing services that are characterized by high quality, high data transfer rate, low latency [4, 14, and 28], 2) reducing 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) appropriate for tasks and queries that happens 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 sending and processing it in the cloud [6], 7) Supporting many applications with latency requirements as low as possible, such as augmented reality and gaming [39].

There are many difficulties and disadvantages of Fog computing, the most prominent and most important includes; 1) companies that use Fog computing need to buy many expensive devices such as gateways, routers, and hubs [29], 2) Very complex system; due to using lot of nodes, and it needs another extra layer compared with the Cloud that has two processes that are storage systems and data processing [29], 3) It is less scalable in terms of the number of devices and services provided in comparison with Cloud computing, [29].

6 Fog Computing Applications

Fog computing maybe applied in many applications such as urban surveillance, smart power grids, drones for assisting in monitoring [12], shopping centers, scenery parks, inter-state buses [14], smart homes, smart vehicles, 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 discuss two applications that are supported by Fog computing as examples.

Augmented Reality (AR). AR is an application that can be run on many devices like tablets ,smartphones, and smart glasses. It needs high power to run the video and high bandwidth to send the data [31]. The time for processing and sending the data must be as low as possible. The Fog computing is able to provide both; it maximizes throughput and minimizes the latency in both processing and sending the data [31].

Mobile Big Data Analytics. It is an important topic for big data architectures in both cloud and mobile

cloud, since the latenc y in both are high. Fog computing can support fl exible resources for huge systems without facing this latency issue [31].

7 Challenges and Issues of Fog Computing

In this sectio n, we will il lustrate in brief so me of challenges and issues facing Fog computing.

Security and Privacy. Fog computing devices face some security and privacy issues. This is because it is spread in locations a nd are not close to the locations that are monitored and protected [1]. For this reason, it is vul nerable to different types of attacks. Fog computing is also vul nerable to m any security attacks becaus e it is deve loped upon traditional networking components, not the m odern components [33].

Fog computing may suffer from the following types of attacks; Data hijack, and eavesdropping [1]. Man-in-the-middle attack; penetration of fog devices that work as a gateway [1, 8, and 41] , Malicious attack; the data in the Fog nodes are not fair and forged by a malicious node [8]. and Denial of services; there are many services and requests in the Fog. Therefore, it is difficult for the Fog in dealing with huge number of services at the sam e time. So, the network becomes busy and does not provi de services for end users [2 7]. It also suffers fro m Rogue Node Detection; a malicious node in IoT that collect the data and ex change it for malicious purposes [34].

Fog computing also suffers from problems in data protection; due to the lac k of resources that help to encrypt or decrypt the data [8]. It has also Issues in data management; where there is a need to ensure and check if the node provides and support the same services for the users [8]. Besides, there is Privacy location issue; that is if the location of IoT devices is known, the data in it can be stolen [34]. Fog computing has also the i ssue of Authentication in the network [41].

There are a number of s ecurity solutions for fog computing issues. One solution is privacy-preserving Fog com puting. It ensures that data is secured between end-user devices and Fog network. This is done in five step s as a follows; 1) collect secure data and extract f eatures from it. 2) Data fuzzing. 3) Segregation. 4) Public Key Infrastructure should be Implemented. 5) Sending the segregated data to Fo g nodes. [36]. In order to solve t he authentication problem in Fog network, a public key infrastructure (PKI) maybe used [36, 41] . Also, advance encryption standa rd (AES) maybe used. It is a suitable algorithm for fog network in term of encryption of data. So, it can be used in any fog computing network to ensure data security [36]. In order to reduce and mitigate the sec urity threats, reducing data theft fro m inside the network is necessary. Components of both Fog and cloud computing can be used together. In t his combined solution, decoy methods and behavior profiling can be used [36].

Control and Management Issues. In Fog computing, the nature of the nodes is m obility; so the changes are frequent which lead to some metrics to also change like latency , storage, bandwidth, and computation [27]. The platform is different from user to use r; so the resources are run in a heterogeneous way [27].

Fog Networking. The Fog network is heterogeneous in nature, because it is pl aced on the Internet edge. Therefore, controlling and m anaging some services such as maintaining connectivity is not easy. In order to provide these servic es in flexible way, there are two emerging techniques that can used. Th ese are network function virtualization (NFV), and software-defined networking (SDN) [31].

Task Scheduling. The scheduling of tasks is not easy in the Fog. This is because the ta sk can move between various physical devices like fog nodes, back-end cloud servers and client devices [32].

Heterogeneous. The nodes in Fog network are heterogeneous, because no gua rantee or confirmation that the sa me sources exist in each node [32].

Power Consumption. Because the huge num ber of nodes in the Fog network, it consu mes a lot of power. In order to reduce power consumption, there are many effective protocols that can be used like effective filtering CoAP, and sam pling techniques [35].

8 Aspects of fog computing Security

Fog computing faces s ecurity issues a nd problems as mentioned in previous section. Ther e are some important aspects that se curity techniques need to handle in thi s regard. In this section, we present these aspects and some brief details of each of them as shown in Fig. 2 [30].

Fig.2 Aspects of Fog Computing Security

Authorization and Authentication. This is an important issue for Fog computing. Because the Fog is an open network that enable a huge number of devices to connect to the network. The definition of each of them is as follows; Authorization referring to the "who is who?" and the Authentication referring to the "who can do what?" [30].

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

Access control mechanism. There is a low difference between the access control and the authorization. Access control guaranteese for each node the right to obtain the authorization [30].

Intrusion Detection System (IDS). The IDS warns the administrator of the system about attacks on the network and allows to protect the system [30].

Privacy. The privacy is an important issue, and this can be; "privacy of services used", "privacy of location", and "privacy of data and information" [30].

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

9 Integrating between Fog computing with other techniques

It is acknowledged that there are some benefits of merging between the Fog computing with other techniques. However, there are some challenges that need to be addressed before the merging process. We present next an overview of some of the efforts of integrating Fog computing with IoT and Cloud.

9.1 Fog computing with IoT

There are many limitations and challenges that IoT face such as latency constraints, network bandwidth constraints, resource-constrained devices, uninterrupted services, and IoT security challenges, as shown in Table 4. In order to mitigate these limitations and challenges, Fog computing can be a suitable technique. In Fog computing, analyzing and managing the data operations are performed near to end-users, thus solving the latency constraints limitation of IoT [6]. Likewise, Fog computing allows data processing based on the application's requirements. This process reduces the data that is sent to the cloud and 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 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 Challenges	The Fog computing plays as a act the proxy for devices that have not enough security.

9.2 Fog computing with Cloud computing

There are many limitations and issues that face the integration of Fog computing in domains like IoT in Healthcare and Cloud Computing. These limitations can be handled as shown in Table 5.

The integration between Fog and Cloud is a possible solution to address the problems and issues that face IoT in Healthcare [9]. These problems are uneven data load, diverse user expectations, heterogeneity of the applications, and latency sensitivity. The main aim of this merging is to construct solutions to diverse applications, such as machine learning, sensors, and recommender systems [9]. Despite these pros, there are challenges for this merging

which are service orchestration, cloud- edge service management, and intelligent health sensors [9].

Cloud computing faces many problems and issues. The architecture is geographically centralized and more than one hop distance from an IoT data source. In order to handle these issues, Fog com puting can be implemented at the edge of the network in order to handle issues that Cloud computing faces [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

In this paper, we discussed Fog co mputing technology, an active research filed, in ter ms of many aspects. We discussed the six lay ers of Fog computing architecture, characte ristics, advantages, and disadvantages, and ap plications of it. We also highlighted the challenges and issues facing Fog computing, such as se curity, privacy, control management, task scheduling, heterogeneity, and power consumption. Then, we presented an overview of aspects of Fog computing Security, such as authorization and authentication, network security, access control mechanisms, IDS, privac y, and virtualization. Finally, we discussed the benefits of merging o f Fog com puting with IoT and Cloud Computing. The Fog provided benefits and addressed problems facing IoT and Cloud computing.

In future wo rk, we aim to buil d a Fo g computing network and implement a real world application. We also aim at p resenting some solutions to the issues discussed in this paper.

References:

[1] I. Stojmenovic, S. Wen, X. Huang and H. Luan, An o verview of Fo g 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 r ole in the inte rnet 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 Com puting Micro Datacenter Based Dynamic Resource Estimation and Pricing Model for IoT", 2 015 IEEE 29th International Conference on Advanced Information Networking and Applications, 2015.

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

[5] M. Aazam, S. Zeadally and K. Harr as, 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. Wil ls, Fog Computing and the I nternet of Th ings: A Review, *Big Data and Cognitive Computing*, VOL.2, NO.2, 2018, p. 10.

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

[8] K. Lee, D. Kim, D. H a, 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.

[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 pr actices, *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. N ovak, S. Yi and Q. Li, Challenges and Software Architecture for Fog Co mputing, *IEEE Internet Computing*, VOL.21, NO.2, 207, pp. 44-53.

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

[34] A. Alrawais, A. Alhotha ily, C. Hu and X. Cheng, Fog Computing for the Internet of Things: Security and Privacy Issues, *IEEE Internet Computing*, VOL.21, NO.2, 20 17, pp. 34-42.

[35] A. Dastjerdi and R. B uyya, Fog Computing: Helping the Internet of Things Realize Its Potential, *Computer*, VOL.49, NO.8, 2 016, 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, Co mparison of edge computing implementations: Fog com puting, cloudlet and mobile edge co mputing, *2017 Global Internet of Things Summit (GIoTS)*, 2017.

[38] M. Mukherjee et al., Securit y and Pri vacy 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 Co mputing: 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 c omputing: A survey , *Future Generation Computer Systems,* VOL.88, 2018, pp. 16-27.

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