IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Fog Computing, Applications, Security and Challenges: - A Survey

Ashutosh Kumar Choudhary
Assistant Professor, ASET
Amity University, Chhattisgarh

Suniti Purbey
Assistant Professor, AIIT
Amity University, Chhattisgarh

Ankit Mishra
Assistant Professor, ASET
Amity University Chhattisgarh

Abstract

The internet of things originates a world where on daily basis objects can join the internet and interchange information and in addition process, store, gather them from the nearby environment, and effectively mediate on it. A remarkable number of services might be imaginedby abusing the internet of things. Fog computing which is otherwise called edge computing was introduced in 2012 as a considered is a prioritized choice for the internet of things applications. As fog computing extend services of cloud near to the edge of the network and make possible computations, communications, and storage services in proximity to the end user. Fog computing cannot only provide low latency, location awareness but also enhance real-time applications, quality of services, mobility, security and privacy in the internet of things applications scenarios. In this paper, we will summarize and overview fog computing model architecture, characteristic, similar paradigmand various applications in real-time scenarios such as smart grid, traffic control system and augmented reality. Finally, security challengesare presented.

Keywords: *Internet of Things; Cloud Computing; Fog Computing; Security*

1. Introduction

The concept of the internet of things (IoT) belonging to the environment in which interrelated objects called things are communicated through the internet without human involvement. [1]. IoT consists of making each intelligent object part of the internet, for example, sensors, portable devices, smartphones, cameras, and vehicles. In the coming years, IoT devices will invade the world since many tens of billions of objects will be connected by 2020 [2]. NumerousIoT applications are being produced and /or structured in different industries including smart city, smart grid and home support, also in health care services, inventory system, and transportation. Basically, the basic goal of the IoT is to provide connectivity between the billion of smart things with internet and this promising technology can bring very useful future for smart cities[3]. In order to achieve all these advantages of the internet of things, it is necessary to provide sufficient network and computing infrastructure for IoT applications with high speed and response time. As a result, cloud computing has been considered as an ideal choice for IoT enabler applications with large storage and processing power[4].

Cloud computing store a large amount of information and can be accessed anywhere in the world. Due to high storage and high computation power, data can be accessed efficiently. However as the paradigm of cloud computing model is centralized in nature, mostly all activity takes place in the cloud [5]. Due to centralization, the cloud computing is unable to respond to high mobility, location awareness, and low latency requirements. Therefore, to control problems of cloud computing Cisco introduced a promising concept name fog computing [6]. Fog computing eliminates the aforementioned problems and provides low latency, location awareness and improves the quality of services (QoS) for real-time applications [7].

The word fog means cloud near to the ground, so in fog computing, data and computation are put close to the end user [8]. The fog computing also interconnects IoT and cloud to persuade the essential additional functionalities for application to perform particular processing. For example, before the transmitting of data to the cloud, it must be filtered and aggregated in fog. It should be able to choose how to send content and when to send ”content, data format, time.” Fog computing deletes some un-necessary or wrong information and combined the necessary matching data in the space with respect to time [9].

Fog computing operates as a bridge between IoT devices and cloud computing. Different new information can be transferred through fog computing devices. These devices are usually composed of traditional networking devices such as set top boxes, access point, roadside units, cellular base station and proxy server etc [10].

This review paper is grouped into two parts. The first part con- tains architecture and characteristic of fog computing and reviews a wide range of applications of fog computing. This section also included similar technology to make the review more comprehensive and favorable. The second part contains security challenges and conclusion.

1.1. Architecture of fog computing

In the recent time, there have been many architectures that have been used for fog computing. Some of them were obtained from the basic three-tier structure. The general architecture of fog computing is

represented in Figure 1 contains cloud layer at the top, the fog layer in the middle and the terminal nodes contains different IoT devices and the sensors at the bottom layer.

1. Device layer
   Device layer contains different IoT devices and end devices such as mobile phone, smart vehicles, smart cards etc. These devices are distributed geographically. Generally the terminal devices sensed information from different physical objects or events. The information are Collected and sent to the top layer for further processing and storage [11].
2. Fog layer
   The fog computing layer is deployed between cloud and IoT devices. This layer plays an important role in the transmission between the cloud computing layer and the device layer [12]. Fog layer contains network devices such as router, access points, gateways, switches, and video surveillance cameras. These devices act as a fog server, geographically distributed among end devices and cloud. Fog servers collect informations from end devices. Also, they have the ability to manage the process and temporally store sensed information. The fog server performs real-time analyses as well as accomplished latency sensitive information [5]. Fog server can be also used statically at a fixed point. for example inside a shop installed similar to as a Wifi or mobile placed on a moving vehicle like system GreyhoundBlue system [13, 14].
3. Cloud layer
   The cloud layer is the top layer in the fog computing environment. It corresponds to cloud intelligence and can store and process massive amounts of data, depending on the capabilities of the data center [15]. The cloud data center is responsible for analyzing and making all decisions and is responsible for permanent storage. The cloud can also assign part of the task to the fog node because fog is often more meaningful for local analysis and quick decision making. If the fog does not require in-depth analysis, it only needs to actively filter the local data and selectively retransmit the data to the cloud. Therefore, transmission efficiency can be significantly improved for widely distributed networks [16, 17].

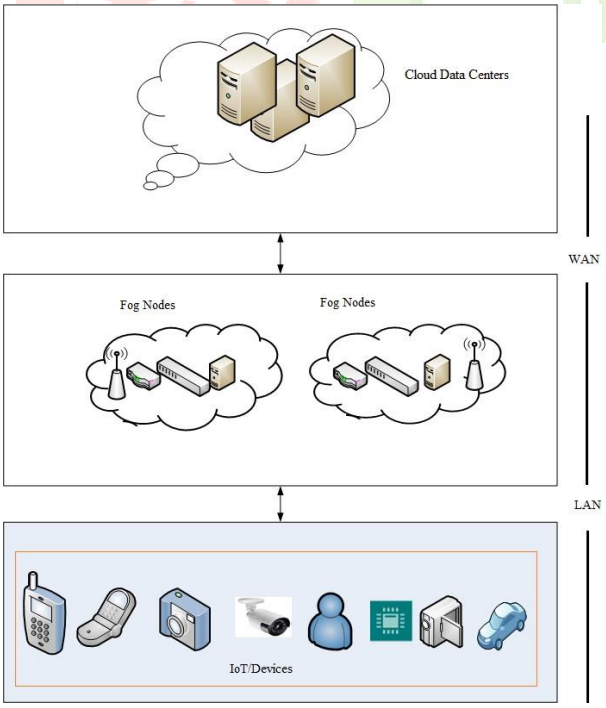

Figure 1: Architechture of fog computing

1.2. Characteristic of fog computing

Fog computing services are close to the end devices. Due to proximity to the end devices, this computing paradigm is a significant advantage over other traditional computing models. Some significant characteristic are shown in Figure 2.

- Geographical distribution
  The fog nodes are geographically distributed. They are deployed in several places. For example, it can be fixed on highways and roads, on cellular base stations and on the museum floor and so on [18].
- Decentralization
  The fog computing architecture is decentralized. There is no central server to manage computing resources and services. Therefore, fog nodes are self-organizing and collaborate to provide end users with real-time IoT applications [19].
- Location Awareness
  Location awareness is the ability to find out the geographical location of a device. The fog node is connected to the nearest fog node, the fog node knows where the fog client is located. Location awareness can be used for targeted advertising or in emergency conditions [20].
- Real time interaction
  Fog computing supports real-time interaction rather than batch processing. Real-time processing includes augmenting reality, gaming and real- time stream processing. Due to close to the edge, fog computing provides rich network information about local network condition, traffic information and status informations as well.
- Save storage space
  Fog computing is one of the best options to avoid improper or unrelated data to move to the whole network, thus will save storage space and decrease the latency [21].

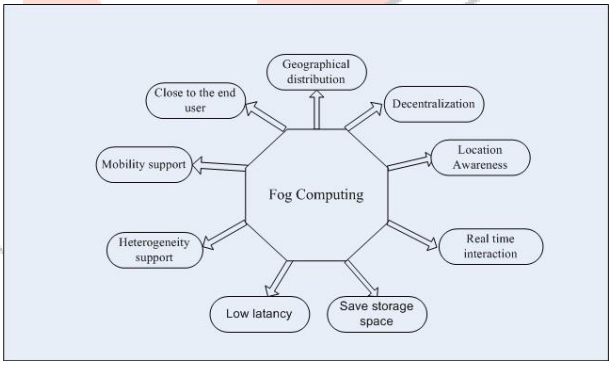

Figure 2: Characteristic of Fog computing

- Low latency
  In the cloud and IoT enviornment, sensors generated information are transfered to cloud data center, which is located remotly from IoT devices. Therefore, end-to-end delay occur,such as delay in transmission from IoT devices to remotely data center, the delay of analyzing of the data and the delay of back response of cloud to the end user. Hence cloud computing have high latency. The fog computing node is close to the IoT device, providing computing services and taking decisions based on local data without using the cloud. Therefore, the latency in response is much less than that of cloud computing [22, 23].
- • Heterogeneity support
  The fog computing system contains heterogeneous nodes. They vary from high-end servers, edge routers, access points, set- top boxes or even end nodes. For example vehicles, sensors, mobile phones, and so on. These nodes are structured in a different environment with different duties [24]. They have

high-performance servers, edge router, access points and gateway etc operated by the different operating system which has a different level of computation power and storage capabilities. Fog computing also provide virtualized platform. Some virtual nodes such as computing nodes and virtual network nodes can also be used as fog nodes. Therefore, fog nodes is heterogeneous [25, 26].

- Mobility support
  Mobility support plays a vital role for some fog computing applications to empower direct communication with mobile devices through the use of protocols. For example, the Cisco Locator / ID separation protocol, which uses a distributed directory system to separate the host's identity from the site's identity [27].
- Close to the end user
  To eliminate delays in data transmission fog allows data to be closer to users than stored in remote data centers [21].

1.3. Similer Paradigm

- Cloud computing
  Cloud computing has been extensively accepted as next generation computing infrastructure. It gives the facilities to the users to access massive amount of data in different format online [29]. Cloud computing provides three services models. i.e. Software as a services (SaaS) , Platform as services (PaaS) Infrastructure as services (IaaS), These all services are used by the cloud client. SaaS provides interface to the end user to pay for the platforms and allows them to send their own application and software on the cloud side. Third party vendor managed and delivered the applications to the end user. PaaS provides opportunity to the end user to pay for the application and services to access the cloud from anywhere. IaaS control and man- age the system in terms of applications, network connectivity and storage [21, 30]. These services provided by cloud service provider for example Google, Amazon and salesforce.com. The end user access the services related to different enterprises and educational facilities at very low cost [31].
  Besides these benefits as mentioned before, cloud computing is centralized in nature and all the servers are remotely situated from the end user which causes delay in processing. Therefore, cloud computing is not well suited for real time applications. To overcome on the limitation of the cloud edge computing is introduced.The computation domain of cloud computing ,fog computing, edge computing, mobile cloud and mobile edge computing are shown in Figure 3.
- Edge computing
  The fundamental idea of edge computing is to bring the computation facilities near to the end user. All data processingis handling close to edge of the network. Edge network is the combination of two types of devices.i.e, end devices and edge devices. End devices contain mobile phone, smart ob- jects etc. Edge devices consist of the border router, set-top boxes, gateways, bridges, base stations and wireless access point etc.edge devices are connected with end devices or withcloud. Therefore, edge computing provides high response com- putation facilities to the end user. This type of computing is not associated with the services of cloud models e.g. IaaS, PaaS, SaaS [32, 33]. Mostly computation can be handled lo- cally in edge computing and do not require any interference from the cloud. Therefore edge computing is the best choice toreduce latency and provide real-time applications. It supports mobility due to rich accessibility and geo-distribution in nature. Edge computing can be implemented in three types for example mobile cloud computing, Fog computing and cloudlet [34].
- Mobile cloud computing(MCC)

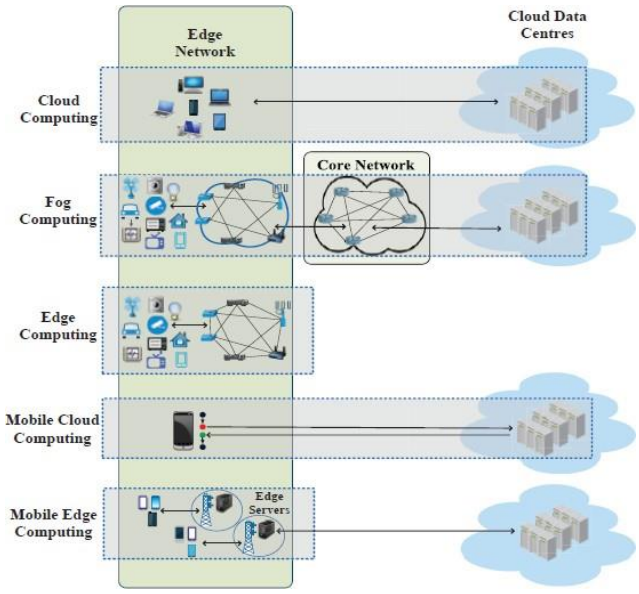

Figure 3: Similer pardigm of fog computing [10]

Cloud computing and mobile computing, integrated into mobile cloud computing to bring new sorts of administrations for mobile user [35]. In mobile cloud computing data storage and processing both take place externally of the mobile devices. Mobile cloud applications are used to transfer the computing power capability and storage capability from mobile phone to the cloud. Also, provide a different large number of applications for Smart phone as well as for mobile subscriber. MCC gives the facilities to the user to access the massive amount of data in the cloud [36]. However, MCC has the inherent limitation that it is a long distance from the end user to the remote center, which will lead to excessively large scalability of mobile applications. Therefore, MCC does not apply to a wide range of mobile applications that are critical to mobility [37]. MCC efficiently combined the services of three technologies such as cloud computing, mobile computing and wireless access communication to increased the Quality of Experience (QoE) of the mobile user and to provide better efficiency.

- Mobile Edge computing (MEC)
  Mobile edge computing brings the facilities to combine cloud computing abilities and the IT service environment near to the edge of the mobile network. The essential thought behind the MEC is that by running applications and performing related handling assignment nearer to the cell client. MEC Technology is intended to be executed of the cell base stations and empowers the adaptable and quick distribution of new applications and administrations for clients [38]. The architecture of MEC include three basic components.i.e, edge devices which contains all types of mobile devices and IoT devices connected to the network. The second component comprised on edge cloud, deployed at every base station. The responsibility of edge cloud is to control traffic, filter the traffic and forward the traffic. Edge cloud also hosting various edge applications such as edge health care and smart tracking etc. the third component consists of public cloud.The public cloud is the cloud infrastructure hosted in the Internet [39].
- Fog computing
  Fog computing also performs edge computation. It extends services of the cloud to the end user and processed IoT generated data . Fog computing combines mobile cloud computing and mobile edge computing to support IoT applications [40]. Both

Table 1: Comparison of similar paradigm extended[28]

	Mobile Edge Computing	Fog Computing	Mobile Cloud Computing	Cloud Computing
Ownership	Telco companies	Private entities, individual	Private entities	Private entities
Deployment	Network Edge	Near Edge,Edge	Network edge Or Devices	Core netwrok
Node devices	Routers, Switches, Access points, Gateways	Server running in base stations	Wireless access points, Transmission Towers, Antennas	Large servers
Inter node communication	Partial	Supported	Partial	N/A
Hardware	Heterogeneous server	Server,End devices	Server,User Devices	Server
Net Architecture	Decentralized distributed	Decentralized distributed	Decentralized distributed	Centralized
Mobility	Yes	Yes	Yes	N/A
Latency and Jitter	Low	Low	Low	High
Local awareness	Yes	Yes	Yes	N/A
Scalability	High	High	High	Average
Sharing population	Medium	Small	Large	Large
Location	Radio Area network	Between devices and data center	Larg data center	Faraway from center

edge and fog computing extend the services of cloud computing in proximity to the end user [41].Edge and fog computing is more interchangeable term but fog computing focus on infrastructure side while edge computing focus towards things [42]. Like edge computing, fog also contains servers or nodes and end-user devices. fog nodes contain switches, router, set-top boxes, surveillance cameras etc. Fog node can be deployed anywhere such as in factories, railway tracks, along roadside aeroplane firms etc. Different IoT devices sensed information and then that information can be transfered to the fog node. Fog servers processed the most time-sensitive data in a real-time manner and then forward that informations to the cloud for historical analyses and long time storage. As a result, latency can be reduced to some extent [43].

1.4. Application of fog computing

- Smart grid
  Smart grid is the next generation electric power distribution network. Smart grids contain transmission lines, substations, transformer and so forth. It utilizes bidirectional streams of power and data to create an automated and distributed strengthen energy distribution network. Smart grid gives an obvious energy distribution where service providers and customer can monitor and control their pricing, production and consumption in real time [44]. In big data environment millions of smart meters are fixed in the consumer home. At the edge process, fog collector are used to collect, process and filter information locally and for long storage information can be send to cloud data center [45].
- Health care system
  Health care services and applications are delay responsive and create confidential information of the patients. The data generated includes sensitive and individual data. Similarly, location data can be sensitive in some situations. Increased instability and latency can cause various problems in telehealth and telemedicine applications. Such type of situation can make fog computing an adequate paradigm in health care scenar-ios [46]. Fog computing play an important role in emergency medical service with little latency restrictions associated with implantable medical devices, ambulance communications or portable access to patient medical files [47]. Author in [48] proposed a system for stroke patients.The proposed system using fog computing to detect ,predict and prevents fall by stroke patients. They used fall detection learning algorithm across edge devices and cloud resources. Compared results of the proposed system with other approaches. They came to the conclusion that this system had a shorter response time and consumed less energy than the approaches using in the cloud.
- Augmented reality(AR)
  Augmented reality is the ability to encircle overlay the digital and virtual thing into the real world[49]. The augmented reality information require low latency and a high information handling rate to give the right information as indicated by the clients location[50]. The applications of augmented reality are highly intolerant to latency. A little delays in the response may damage the client skills. Therefore, fog computing can possibly turn into an imperative player in the area of augmented reality [51] .
  Google Glass, Sonny Smart Eyeglass and Microsoft Hololens are the recent product or projects for augmented reality applications. AR applications require computer vision algorithms to process real-time video frames while processing other inputs, such as voice, sensors, and finally generate timely informative content on the screen. In any case, the human is extremely delicate to delays in a number of successive interactions. A processing delay of more than several milliseconds will devastate the user experience and prompts to negative user response. Therefore, fog computing supports augmented reality systems that increase performance and reduce processing delays [52].
- Trafic control system
  In traffic control system, the video camera that detects the flashing lights of an ambulance can automatically change the street lights and open the tracks for the vehicle to cross the traffic. Intelligent streetlights cooperate locally with sensors and identify the occurrence of the person on foot and cyclists, and evaluate the distance and speed of approaching vehicles. Besides these, smart lighting is automatically switched on once the sensor distinguishes the movement and turns off as the traffic passes. Nearby intelligent lights that act as fog devices coordinate to create a green traffic signal and send a warning signal to approach vehicle [53]. Traffic control system is useful in, accident preventions, maintenance of steady ow traffic and collection of relevant data to evaluate and improve the performance of the system [54].
- Vedio streaming system
  In fog computing video streaming application allows mobile users to watch the recent video available on screen [55]. The role of fog computing in the efficient processing and quick decision making is very important. For example, subsequently many targets in a drone video stream, explained in [56] where the live video stream is going to nearest fog node instead of sending to the cloud application. In this environment any mobile devices such as Smartphone, the laptop can act as a fog server running a tracing algorithm and process raw video streams, also be eliminating the latency of transferring data from the surveillance area to the cloud. Moreover, proximal algorithm [57] is used to remove the joint resources issue in fog nodes and to produced better results of a large video streaming. The video data stream generated by the camera sensor is sent to the corresponding fog node where it is stored and processed.

2. Security challenges of fog computing

As fog computing is a promising technology extends the services of the cloud to the edge of the network. Like cloud computing, fog computing also gives services to the end users with data processing

and storage facilities. Fog computing is still in infancy stage. With respect to the issues of fog computing the studied literature identified different security challenges such as authentication, privacy, data security and various malicious attacks. Different author discussed and presented a different proposal for removing of various security issues in the era of fog computing environment. stojmenovi et al. [7] published special issues paper on the overview on fog and its issues. They highlighted the advantage of fog computing with respect to different fog application such as smart grid, smart traffic control system. Also highlighted Man- in-the-middle attack. Showed its stealthy feature of this attack and examined the CPU and memory consumption on fog device.

Alwa Alrawais et al.[58] proposed homo-m-orphic phaillier encryption, Chinese Remainder Theorem and on way hash chain techniques for hybrid IoT devices. The proposed scheme is able to filter the false data from the network, sending by the attacker. Fault tolerance ,privacy and data security are minimized by the proposed system. The simulation results showed by the author at the end which minimized communication overhead and lower computational cost with respect to existing techniques. Similarly Rongxing Lu et al.[59] proposed an efficient key exchange protocol based on attribute based encryption algorithm (CP-ABE) to provide an authentic and confidential communication between the fog nodes . They combine CP-ABE and digital signature techniques to achieve confidentiality, authentication, verifiability and access control. They analyzed protocol with respect to security and performance and compared result with the existing certificate based scheme to show its feasibility.

- Authentication
  Authentication is the most important security issue in various levels of gateways because fog computing provided large services to many end user by front fog node. In fog computing messages and entities must be authenticated [60]. Mai Trung Dong and Xianwei Zhou exaplained that without proper authentication the chance of Man in the middle attack is possible. They provided authentication via public key cryptography and decoy technology. Implemented public key cryptography by using conventional Cryptosystem such as Rivest Shamir Adleman(RSA) and Elliptic Curve Cryptography(ECC) algorithm to verify which algorithm is going to consumes more amounts of resources. At the end they compared both the results coming from RSA and ECC algorithms and concluded that ECC provided best result as compared to RSA in resourced constrained fog devices[61]. Biometric authentication play important role in mobile computing and cloud computing for example fingerprint authentication, face authentication and touched based authentication etc. The implementation of these authentication will become more useful in fog computing which studied in [8].
- Malicious attack
  Fog computing contains various edge devices to perform latency aware processing of collected data. Therefore, to know about the malicious edge devices is more challenging task in fog computing environment [62]. Fog computing suffer from several malicious attacks and without proper prevention can severely damage the system performance. One of the malicious attacks has been launched is called denial of services (DOS). In this type of attack, the attacker takes action when multiple devices connected in IoT environment and request for infinite processing/ storage services [63, 11]. The attacker prevents the legitimate user from accessing the target computing or to spoof the IP address of the several devices and send the fake request for accessing the processing/storage services. This type of attack occur at different level of the system. For example at end user level the attacker can jam the wireless channels forexample malware to avoid certain user communication with the infrastructure. While at a higher level, the attacker can physically destroy a fog node, thus interrupting all the services offered in the local level. Therefore, the intensity of this attack becomes more and more when different nodes simultaneously lunch this attack. Existing prevention strategies of the other type of network are not fitting for fog computing because of the openness of the fog computing network. Another malicious attack is Man-in-the-middle attack. In this type, the gateway that functions as a fog node can be compromised or replaced by the fraudulent one. For example customer of KFC or Star Bar connection to which gives deceptive SSID as public legitimate one. The attackers obtain the control of gateway when the private communication is hijacked [64].
- Data protection
  The exponential information created by IoT increases as the number of IoT devices increases. These informations need not only to be stored at the communication level, but also at the processing level. Due to resource constraints, it is extremely difficult to handle the data on IoT devices [65]. When the IoT device senses data, it sends the data to a nearby fog node. It is hard to deal with a large amount of data in IoT devices. Therefore, the data is divided in sections and forwarded to multiple fog nodes for processing. At this position, the contents of the informations have to be analyzed without reviling it.the integrity of data must be guaranteed during processing of distributed data. Here the encryption and decryption process is very difficult due limited availability of resources. Therefore, light-weight encryption and masking techniques are needed [64].
  The authors in [66] give a solution to protect data from malicious user who use components of cloud and fog computing. They presented two approaches, behavior profiles and decoy system. The basic purpose of these techniques is, to mitigate security attacks. The author further explained that if some reports show anomalous behavior, such as the increasing access to various records at unusual time, the scheme will label the entry as distrustful also stop the corresponding user. Decoy system contains fake information such as honey files, honeypots as well as other types of records that can be utilized to fetched, confused and identify harmful insiders. They proved that the proposed technique can correctly identify abnormal behavior and its average accuracy is greater than 90%.
- Privacy in fog computing
  Privacy in fog computing is a more challenging task. Because fog server is very close to the end user and collects more sensitive data compared to the cloud computing. Security techniques have to give privacy to the end user. In fog computing privacy of data, the privacy of services and privacy of location are very important. Every node in fog computing shares their information with other nodes and can send secret information at any particular time. They have a right to maintain their location secret from other nodes. Therefore for reliable communication fog computing must ensure all these rights [67].
- Access control
  Access control is the process of determining whether a device or a client can get into the resources. Such as reading or writing data, executing programs and controlling actuators. Access control system allows a different node in fog paradigm to get authorization[68]. Authorization of fog computing is very important. It is necessary to check the identity of the different systems, in demand to authorize their request to accomplish various operations. If fog node has no authorization mechanism than anyone can enter into the system and miss use the resources[28]. Similarly, if fog/cloud user want to use the computation services, by the fog/cloud and some policies should be implemented to control to data and services. Therefore, it must be necessary for fog system to implement access control

mechanism and ensure authorization.

- Intrusion Detection system

  An intrusion detection system preventing adversaries from illegal access and decides an appropriate alerts to prevent intrusions or mitigate the effects of intrusion [69]. As cloud system have different types of attacks such as internal attacks, flooding attacks, port scanning and attacks on the virtual machine and hypervisor. Intrusion detection techniques are generally deployed within cloud system to mollify these types of attack. This system analyzes and monitors the access control policy, a log file and user registration information to detect intrusions. It can be keep running on network side to identify malignant movement like DoS and port scanning [64, 8, 70]. In fog computing, intrusion detection system can be sent on the system side of the fog node to recognize sniffing activities by noticing, scrutinizing and asking a lot of detailed questions about access control methodologies, log files and customer login information. In the same way they can be sent at the fog network side to distinguish harmful attacks. For example port scanning and denial of services etc. In fog computing, it gives new prospects to explore how fog computing can offer with intrusion acknowledgment on both client side some help with siding and bound together cloud side [71].

3. Conclusion

This paper discusses the concept of fog computing with the simi- lar paradigm. Fog computing considered a good partner of cloud computing which extends the services of a cloud to the end user. The characteristic of fog computing such as mobility, place close to the end user, location awareness, heterogeneity and their real-time applications, fog computing paradigm is a more suitable platform for the internet of things. Various security issues may encounter in the design and implementation of this technology. This study contains various securities issues such as authentication and privacy. This technology is still in the initial stage, therefore, further investigation may require.

References

[1] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," *IEEE communications surveys & tutorials*, vol. 16, no. 1, pp. 414–454, 2014.

[2] M. I. Naas, P. R. Parvedy, J. Boukhobza, and L. Lemarchand, "ifogstor: an iot data placement strategy for fog infrastructure," in *Fog and Edge Computing (ICFEC), 2017 IEEE 1st International Conference on*. IEEE, 2017, pp. 97–104.

[3] C. Perera, Y. Qin, J. C. Estrella, S. Reiff-Marganiec, and A. V. Vasilakos, "Fog computing for sustainable smart cities: A survey," *ACM Computing Surveys (CSUR)*, vol. 50, no. 3, p. 32, 2017.

[4] A. Yousefpour, G. Ishigaki, and J. P. Jue, "Fog computing: To- wards minimizing delay in the internet of things," in *Edge Computing (EDGE), 2017 IEEE International Conference on*. IEEE, 2017, pp. 17–24.

[5] 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*, 2017.

[6] R. Silva, J. S. Silva, and F. Boavida, "Opportunistic fog computing: Feasibility assessment and architectural proposal," in *Integrated Network and Service Management (IM), 2017 IFIP/IEEE Symposium on*. IEEE, 2017, pp. 510–516.

[7] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in *Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on*. IEEE, 2014, pp. 1–8.

[8] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in *International Conference on Wireless Algorithms, Systems, and Applications*. Springer, 2015, pp. 685–695.

[9] F. Al-Doghman, Z. Chaczko, A. R. Ajayan, and R. Klempous, "A review on fog computing technology," in *Systems, Man, and Cybernetics (SMC), 2016 IEEE International Conference on*. IEEE, 2016, pp. 001 525–001 530.

[10] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog computing: A taxonomy, survey and future directions," in *Internet of Everything*. Springer, 2018, pp. 103–130.

[11] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19 293–19 304, 2017.

[12] T. Wang, J. Zhou, X. Chen, G. Wang, A. Liu, and Y. Liu, "A three-layer privacy preserving cloud storage scheme based on computational intelligence in fog computing," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 3–12, 2018.

[13] P. Sareen and P. Kumar, "The fog computing paradigm," *Int J Emerging Technol Eng Res*, vol. 4, pp. 55–60, 2016.

[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 preprint arXiv:1502.01815*, 2015.

[15] M. Taneja and A. Davy, "Resource aware placement of data analytics platform in fog computing," *Procedia Computer Science*, vol. 97, pp. 153–156, 2016.

[16] Y. Shi, G. Ding, H. Wang, H. E. Roman, and S. Lu, "The fog computing service for healthcare," in *Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech), 2015 2nd International Symposium on*. IEEE, 2015, pp. 1–5.

[17] S. Sarkar, S. Chatterjee, and S. Misra, "Assessment of the suitability of fog computing in the context of internet of things," *IEEE Transactions on Cloud Computing*, 2015.

[18] L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog: Towards a comprehensive definition of fog computing," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 5, pp. 27–32, 2014.

[19] J. Shropshire, "Extending the cloud with fog: Security challenges & opportunities," 2014.

[20] T. S. Dybedokken, "Trust management in fog computing," Master's thesis, NTNU, 2017.

[21] K. Saharan and A. Kumar, "Fog in comparison to cloud: A survey," *International Journal of Computer Applications*, vol. 122, no. 3, 2015.

[22] S. M. H. Ashjaei and M. Bengtsson, "Enhancing smart maintenance management using fog computing technology," in *2017 International Conference on Industrial Engineering and Engineering Management IEEM, 10 Dec 2017, Singapore, Singapore*, 2017.

[23] F. A. Kraemer, A. E. Braten, N. Tamkittikhun, and D. Palma, "Fog computing in healthcare–a review and discussion," *IEEE Access*, vol. 5, pp. 9206–9222, 2017.

[24] T. V. N. Rao, A. Khan, M. Maschendra, and M. K. Kumar, "A paradigm shift from cloud to fog computing," *International Journal of Science, Engineering and Computer Technology*, vol. 5, no. 11, p. 385, 2015.

[25] K. Kai, W. Cong, and L. Tao, "Fog computing for vehicular ad-hoc networks: paradigms, scenarios, and issues," *the journal of China Universities of Posts and Telecommunications*, vol. 23, no. 2, pp. 56–96, 2016.

[26] M. Aazam and E.-N. Huh, "Fog computing: The cloud-iot\/ioe middleware paradigm," *IEEE Potentials*, vol. 35, no. 3, pp. 40–44, 2016.

[27] A. A. Dabhi, T. J. Raval, and K. Chaudhary, "Fog computing: A review and conceptual architecture, issues, applications and its challenges."

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

[29] A. Shawish and M. Salama, "Cloud computing: paradigms and technologies," in *Inter-cooperative collective intelligence: Techniques and applications*. Springer, 2014, pp. 39–67.

[30] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation computer systems*, vol. 28, no. 3, pp. 583–592, 2012.

[31] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *Journal of internet services and applications*, vol. 1, no. 1, pp. 7–18, 2010.

[32] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick, and D. S. Nikolopoulos, "Challenges and opportunities in edge computing," in *Smart Cloud (SmartCloud), IEEE International Conference on*. IEEE, 2016, pp. 20–26.

[33] Y. Sahni, J. Cao, S. Zhang, and L. Yang, "Edge mesh: A new paradigm to enable distributed intelligence in internet of things," *IEEE Access*, vol. 5, pp. 16 441–16 458, 2017.

[34] K. Dolui and S. K. Datta, "Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing," in *Global Internet of Things Summit (GIoTS), 2017*. IEEE, 2017, pp. 1–6.

[35] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," *IEEE Internet of Things Journal*, 2017.

[36] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," *Wireless communications and mobile computing*, vol. 13, no. 18, pp. 1587–1611, 2013.

[37] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.

[38] A. Munir, P. Kansakar, and S. U. Khan, "Ifciot: Integrated fog cloud iot: A novel architectural paradigm for the future internet of things." *IEEE Consumer Electronics Magazine*, vol. 6, no. 3, pp. 74–82, 2017.

[39] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing—a key technology towards 5g," *ETSI white paper*, vol. 11, no. 11, pp. 1–16, 2015.

[40] F. Popentiu-Vladicescu and G. Albeanu, "Software reliability in the fog computing," in *Innovations in Electrical Engineering and Computational Technologies (ICIEECT), 2017 International Conference on*. IEEE, 2017, pp. 1–4.

[41] N. Mohan and J. Kangasharju, "Edge-fog cloud: A distributed cloud for internet of things computations," in *Cloudification of the Internet of Things (CIoT)*. IEEE, 2016, pp. 1–6.

[42] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[43] M. Aazam and E.-N. Huh, "Fog computing and smart gateway based communication for cloud of things," in *Future Internet of Things and Cloud (FiCloud), 2014 International Conference on*. IEEE, 2014, pp. 464–470.

[44] F. Y. Okay and S. Ozdemir, "A fog computing based smart grid model," in *Networks, Computers and Communications (ISNCC), 2016 International Symposium on*. IEEE, 2016, pp. 1–6.

[45] R. K. Barik, S. K. Gudey, G. G. Reddy, M. Pant, H. Dubey, K. Mankodiya, and V. Kumar, "Foggrid: Leveraging fog computing for enhanced smart grid network," *arXiv preprint arXiv:1712.09645*, 2017.

[46] R. Brzoza-Woch, M. Konieczny, B. Kwolek, P. Nawrocki, T. Szydło, and K. Zieliński, "Holistic approach to urgent computing for flood decision support," *Procedia Computer Science*, vol. 51, pp. 2387–2396, 2015.

[47] X. Masip-Bruin, E. Mar´ın-Tordera, G. Tashakor, A. Jukan, and G.-J. Ren, "Foggy clouds and cloudy fogs: a real need for coordinated management of fog-to-cloud computing systems," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 120–128, 2016.

[48] Y. Cao, S. Chen, P. Hou, and D. Brown, "Fast: A fog computing assisted distributed analytics system to monitor fall for stroke mitigation," in *Networking, Architecture and Storage (NAS), 2015 IEEE International Conference on*. IEEE, 2015, pp. 2–11.

[49] M. Chen, C. Ling, and W. Zhang, "Analysis of augmented reality application based on cloud computing," in *Image and Signal Processing (CISP), 2011 4th International Congress on*, vol. 2. IEEE, 2011, pp. 569–572.

[50] Y. Ai, M. Peng, and K. Zhang, "Edge cloud computing technologies for internet of things: A primer," *Digital Communications and Networks*, 2017.

[51] A. V. Dastjerdi and R. Buyya, "Fog computing: Helping the internet of things realize its potential," *Computer*, vol. 49, no. 8, pp. 112–116, 2016.

[52] S. Yi, C. Li, and Q. Li, "A survey of fog computing: concepts, applications and issues," in *Proceedings of the 2015 Workshop on Mobile Big Data*. ACM, 2015, pp. 37–42.

[53] P. V. Patil, "Fog computing," *College of Engg & Tech*, 2015.

[54] P. More, "Review of implementing fog computing," *Int. J. Res. Eng. Technol*, vol. 4, no. 6, p. 2319, 2015.

[55] E. Saurez, H. Gupta, U. Ramachandran, and R. Mayer, "Fog computing for improving user application interaction and context awareness: Demo abstract," in *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*. ACM, 2017, pp. 281–282.

[56] N. Chen, Y. Chen, Y. You, H. Ling, P. Liang, and R. Zimmermann, "Dynamic urban surveillance video stream processing using fog computing," in *Multimedia Big Data (BigMM), 2016 IEEE Second International Conference on*. IEEE, 2016, pp. 105–112.

[57] C. T. Do, N. H. Tran, C. Pham, M. G. R. Alam, J. H. Son, and C. S. Hong, "A proximal algorithm for joint resource allocation and minimizing carbon footprint in geo-distributed fog computing," in *Information Networking (ICOIN), 2015 International Conference on*. IEEE, 2015, pp. 324–329.

[58] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng, "An attribute-based encryption scheme to secure fog communications," *IEEE Access*, vol. 5, pp. 9131–9138, 2017.

[59] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced iot," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[60] M. H. Ibrahim, "Octopus: An edge-fog mutual authentication scheme." *IJ Network Security*, vol. 18, no. 6, pp. 1089–1101, 2016.

[61] M. T. Dong and X. Zhou, "Fog computing: Comprehensive approach for security data theft attack using elliptic curve cryptography and decoy technology," *Open Access Library J*, vol. 3, no. 09, p. 1, 2016.

[62] R. Sandhu, A. S. Sohal, and S. K. Sood, "Identification of malicious edge devices in fog computing environments," *Information Security Journal: A Global Perspective*, vol. 26, no. 5, pp. 213–228, 2017.

[63] R. Rios, R. Roman, J. A. Onieva, and J. Lopez, "From smog to fog: A security perspective," in *Fog and Mobile Edge Computing (FMEC), 2017 Second International Conference on*. IEEE, 2017, pp. 56–61.

[64] K. Lee, D. Kim, D. Ha, U. Rajput, and H. Oh, "On security and privacy issues of fog computing supported internet of things environment," in *Network of the Future (NOF), 2015 6th International Conference on the*. IEEE, 2015, pp. 1–3.

[65] 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, pp. 34–42, 2017.

[66] S. J. Stolfo, M. B. Salem, and A. D. Keromytis, "Fog computing: Mitigating insider data theft attacks in the cloud," in *Security and Privacy Workshops (SPW), 2012 IEEE Symposium on*. IEEE, 2012, pp. 125–128.

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

[68] H. Kim and E. A. Lee, "Authentication and authorization for the internet of things," *IT Professional*, vol. 19, no. 5, pp. 27–33, 2017.

[69] F. Hosseinpour, P. Vahdani Amoli, J. Plosila, T. Hämäläinen, and H. Tenhunen, "An intrusion detection system for fog computing and iot based logistic systems using a smart data approach," *International Journal of Digital Content Technology and its Applications*, vol. 10, 2016.

[70] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2013.

[71] K. A. Fakeeh, "Privacy and security problems in fog computing," *Commun. Appl. Electron.(CAE)*, vol. 4, no. 6, 2016.