International Journal of Distributed and Cloud Computing
6 (2) December 2018, 05-11
http://www.publishingindia.com/ijdcc

An Approach Towards the Fog Computing: Stretching Cloud Computing and Internet of Things

Bhoomi Shah[1*] and Hetal Bhavsar[2]
[1]Programme Officer, ADE Section, University Head Office, The M. S. University of Baroda, Vadodara, Gujarat, India. Email: bhoomi.shah.mca@gmail.com
[2]Assistant Professor, Department of Computer Science & Engineering, Faculty of Technology & Engineering, The M. S. University of Baroda, Vadodara, Gujarat, India.
*Corresponding Author

Abstract: Fog computing is a natural extension to cloud computing. It extends the Cloud platform by providing computing resources on the edges of a network. Fog Computing is acting as the intermediate layer for securing the data which is stored inside the cloud. By the year 2025, it is estimated that 75.4 billion IoT devices will be connected to Internet. So in the future this gives challenge to handle huge amount of data and to provide the security for the Data.

1. Internet of Things (IoT) combines information and computing processes to control very large collections of different objects. The IoT devices will produce very large volume of data. It is very difficult to manage these data with traditional system and cloud systems.

2. Fog computing is designed to overcome the limitations of cloud computing. This paper analyses the current developments in the field of fog computing, addresses security issues in fog computing, and based on the observations propose future directions for research.

Keywords: Cloud computing, Edge computing, Fog computing, Internet of Things (IoT).

I. Introduction

The parallel and distributed computing has significantly evolved over the last sixty years [10], [27], [14]. The growth of Smart Things increase in the volume of digitally generated data. In today's world the small as well as large organizations are using cloud computing technology to protect their data and use the cloud resources as and when they needed [5]. Cloud computing only facilitate security features to data and it is difficult to detect invalid access. Whereas the fog computing facilitates security features to data. Fog computing allows for detection of invalid access. There are many limitations of cloud computing that needs to be eliminate. One such technology is fog computing.

Fog computing was first introduced by CISCO. Fog computing terminology refers to a decentralized architecture and serves as an extension to cloud computing. By collaborating with one or more edge node devices, fog computing provides the subsequent amount of localized control, configuration and management, and much more for end devices.

In Cloud computing data needs to access the central mainframe [24], [7], Whereas Fog computing expand their reach to the edge of a network of devices to offer local and quicker accessibility to edge devices.

Fog computing is designed to improve efficiency and reduce the amount of data send to the cloud for processing, analysis and storage. With Fog Computing one can improve efficiency and security of data send to the network.

This research work analyze fog computing and cloud computing. The organization of the paper is as follows. Section 2 gives an in depth study of cloud computing. Fog computing, working of fog computing and applications of fog computing are explained in section 3. The section 4 describes Comparison between Fog Computing and Cloud Computing. The challenging issues for fog computing and related work which had already been done for some of the issues are discussed in section 5. Finally the paper concludes in section 6.

II. Cloud Computing

Nowadays, cloud computing is widely used. Cloud computing allows the user to store huge amount of data and access it from anywhere and everywhere. The users need to have basic internet connection to use the stored information.

Cloud Computing [6] is the term given to the use of multiple server computers via a digital network as if they were one computer. The Cloud itself is a virtualization of resources like networks, servers, applications, data storage and services – which the end user has on-demand access to. These resources can be provided with minimal management or service provider interaction. Cloud computing is a combination of service oriented architecture and many computing strategies such as virtualization, multitenancy, elasticity, service-oriented architecture, and resource pooling. To access the data we always have to depend on the cloud repository, bandwidth allocation and connectivity.

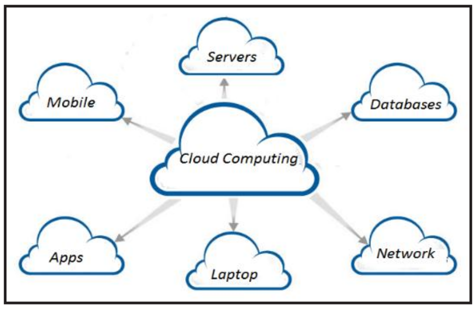

Fig. 1: Cloud Computing Overview

Cloud computing offers the end user resources without the requirement of having knowledge of the systems that deliver it. Additionally, the cloud can provide the user with a far greater range of applications and services.

Cloud computing is becoming a useful technology for many of the organizations with its dynamic scalability and usage of virtualized resources as a service through the Internet. One such application is effective use of cloud computing in educational institutions [36]. Cloud computing is an excellent alternative for educational institutions which are especially under budget shortage.

Another application is Cloud computing in mobile applications [38]. Cloud Computing gives us facility to execute our applications on servers instead of running them locally. Cloud computing help us to overcome the handset's limitation of limited resources to a great extent [16], [11]. And also there will be no need for Mobile application developers to create many versions of same application [22], [32].

Though Cloud computing is very popular and widely used it has several limitations or disadvantages.

Disadvantages of Cloud Computing

a) *Security and Privacy:* Data security is major issues related with personal data and confidential data of organizations. User has to completely depend upon the cloud service provider for their data privacy and security. Cloud systems have been located with the Internet, so user requests, data transmission and system responses need to traverse a large number of intermediate networks.

b) *Technical Issues:* Cloud computing requires reliable Internet connectivity with sufficient bandwidth to access the services [15]. If the link outage occurs due to any reason, the total system would be unreachable making a total blackout. High speed internet connectivity requirement makes the system complex.

c) *Network Latency:* Cloud system is a large heterogeneous network with numerous types, topologies, speeds and technologies with no central control. One issue that affects the quality of service is network latency. Latency is the amount of time a message takes to traverse a system. Real time applications with which users directly interact with are badly affected by latency in networks and Latency variability results in jitter. Jitter is a symptom of network and CPU congestion due to oversubscription and inadequate capacity management. Delay Jitter is a significant issue, particularly for real-time applications. It is very difficult to control the delay and delay jitter arising from latency in a network of Internet scale.

d) *Data Segregation:* Mostly data segregation problem arises in the multi-tenant usage mode, where the different users' virtual machines are co-located on the same hard disks or same server. Here the risk is included to properly separate storage or memory between different users.

e) *Data Location:* The geographic location of the data is also very important to secure the data and information of client. Rules and regulation for certain types of data is different in the different countries. A customer could be involved in illegal issues without even noticing.

f) *Recovery and Back-Up:* Data protection and recovery is an important aspect of cloud. Some times in disaster situations recovery process is quite slow.

The fundamental limitation is the connectivity between the cloud and the end devices. Such connectivity is set over the Internet, not suitable for a large set of cloud-based applications such as the latency-sensitive ones [17].

Furthermore, cloud-based applications are often distributed and made up of multiple components [29].

Some work has been done to overcome the limitation of cloud computing which include connected vehicles [12], fire detection and firefighting [28], smart grid [27], and content delivery [41].

Cloud computing has a requirement of high speed reliable Internet connectivity, has limited bandwidth, does not exercise any data protection mechanisms. Cloud computing is platform dependent and has limited control as well as flexibility. The emerging trends in networking such as large distributed Internet connected sensor networks, Internet of Things (IoT), mobile data networks and also real time streaming applications have characteristics that cannot be satisfied by cloud computing. Thus, Fog computing is a collaboration of Internet of Things and cloud computing.

III. Fog Computing

Fog computing is referred as an extension to cloud computing. Also known as Edge Computing or fogging, fog computing facilitates the operation of computing, storage and networking services between end devices and cloud computing data centers. With fog computing, the data can be accessed locally in between devices without complete dependence on the cloud repository. This will help the user to make data easily accessible and easy to use.

The main objectives of Fog Computing are:

- To reduce the amount of data sent to the cloud.
- To decrease network and Internet Latency.
- To improve system response time in remote mission-critical applications.

A. Working of Fog Computing

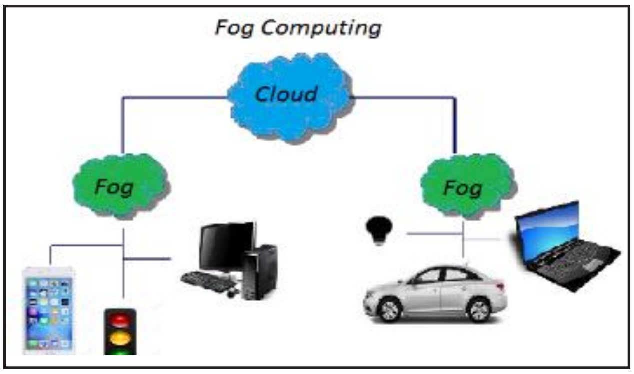

Fig. 2: How Fog Computing Works

In fog computing, Information moves from endpoint devices such as smart phones, computers tablets, sensors, programmable logic controllers (which are used in manufacturing facilities with automation), routers, hubs, and other IP address driven things to the fog, and then to the cloud [1].

The Fog paradigm is well suited for real time big data analytics. Fog computing supports densely distributed data collection points, and provides advantages in entertainment, advertising, personal computing and other applications [8].

Fog computing is considered to be much more secure than cloud computing as in Fog computing information does not need to travel great distances as compared to cloud computing [4]. Response times in Fog computing would be much faster because the distance of end user and Fog nodes is less. Fog computing is more geographically distributed, which results in lower latency and faster data transmission.

B. Advantages of Fog Computing

a) *Bringing Data Close to the User:* Instead of housing information at data center sites far from the end-point, the Fog aims to place the data close to the end-user.

b) *Low Latency:* The data is analyzed where it is generated; hence the round trip time is less leading to low latency.

c) *Better Security***:** Fog nodes can be protected using the same controls, procedures, and policy you use in other areas of IT environment.

d) *Privacy Control:* The sensitive data can be analyzed locally instead of sending it to the cloud for analysis. The IT team can keep track and control the devices that collect, analyze and store the data.

e) *Greater Business Agility:* By utilizing the right set of tools, developers can seamlessly develop fog applications and deploy them whenever needed. Fog applications drive the machine to function in a way according to customer's need [3].

f) *Real-Time Interactions:* Important fog applications involve real-time interactions rather than batch processing.

g) *Reduced Operation Cost:* Fog computing can save network bandwidth by processing selected data locally, instead of sending it to the cloud for analysis.

This advantages makes it possible to use Fog computing in several applications. Some of the applications are as listed follow.

C. Applications of Fog

Many important IOT services uses Fog as a suitable platform and applications. Some of these IOT services are as below:

a) *Smart Traffic Lights:* Video camera that senses an ambulance flashing lights can automatically change street lights to open lanes for the vehicle to pass through traffic. Smart street lights interact locally with sensors and detect presence of pedestrian and bikers, and measure the distance and speed of approaching vehicles. Intelligent lighting turns on once a sensor identifies movement and switches off as traffic passes [19].

Wireless access points like Wi-Fi, 4G, road-side units and smart traffic lights are deployed along the roads. Vehicle-to-Vehicle, vehicle to access points, and access points to access points interactions enrich the application of Fog computing.

b) *Connected Cars:* It's ideal for connected cars, because real-time interactions will make communications between cars, access points and traffic lights as safe and efficient as possible [13].

c) *Self-Maintaining Train:* Another application of fog computing is self-maintaining trains. A train ball-bearing monitoring sensor will sense the changes in the temperature level and any disorder will automatically alert the train operator and make maintenance according to. Thus we can avoid major disasters [19].

d) *Smart Grids:* Allows Fast, Machine-To-Machine (M2M) handshakes and Human to Machine Interactions (HMI), which would work in cooperation with the cloud [19].

e) *Big Data Analytics in IoT:* Fog platform is more suitable for big data analytics in IoT, because it overcomes the drawbacks of cloud, such as high latency and delay. The data will be sent back and forth between the cloud and end-devices which are transmitting data. This takes times and affects the bandwidth and Quality of Service (QoS). With Fog platform in use, the data can be aggregated and mined at Fog servers providing timely feedback to the end-devices and to the cloud server. Detailed analytics and intensive computational tasks then can be processed at the cloud server [7].

f) *Healthcare:* The cloud computing market for healthcare is expected to reach $9.48 billion by 2020, according to market reports Fog computing would allow this on a more localized level. Fog computing could be useful in healthcare, in which real-time processing and event response are critical. One proposed system utilizes fog computing to detect, predict, and prevent falls by stroke patients is described in [1].

IV. Comparison Between Fog Computing and Cloud Computing

Table I highlights the main differences between cloud computing and fog computing at various levels.

Table I: Comparison Between Cloud Computing and Fog Computing

Requirements	Cloud Computing	Fog Computing
Latency	Good	Bad
Delay Jitter	Good	Very Bad
Location of service	Within the internet	At every edge of the local network
Client and server Distance	Multiple hops	Single hop
Security	Less Secure, Undefined	More Secure, Can be defined
Attack on data enroute	High probability	Less probability
Awareness about Location	No	Yes
Geographical distribution	Centralized	Distributed
No. of server Nodes	Less	More
Support for Mobility	Limited Support	Supported
Real time interactions	Supported	Supported
Hardware	Expensive, Robust and hi-tech backbone system with scalable storage and vast computer power	Wireless multi-point interface
Distance to Users	Hosted in remote locations and can only be reached via IP networks	Close to the user and reached via wireless(Wi-Fi) Connection
Bandwidth	More Demand	Less Demand
Time Required for Processing Large Data	More	Less

From Table I, it has been observed that the latency and delay jitter of the cloud computing is high but the fog computing is very low [37]. Location of services of cloud computing is within the internet so there are multiple hops connected between client and server, whereas fog computing is at the edge of local network so the distance between client and server will be very less which results into faster retrieval of data. As fog computing is geographically distributed there is less probability of attack on data enroute as compared to cloud which is centralized. That means keep only that information on the cloud which will be rarely going to be used.

In cloud computing response time is slow and there are scalability problems as there is a dependency on servers that are located at remote places, whereas it is possible to avoid response time and scalability issues in fog computing by setting small servers called edge servers in visibility of users.

On the other hand, it must also be noted that cloud computing is not without its advantages. As fog computing requires more nodes than Cloud computing, and all nodes cannot have large amount of resources, Fog computing makes system unsuitable for small business who have strict budget due to financial reasons. High end business computing such as batch processing jobs, which would require large amounts of resources not being delay sensitive, and can be handled using traditional cloud computing systems successfully more than fog nodes. This concludes that fog computing is not replacing cloud computing [21].

The biggest similarity between these two is the fact that they both are made up of virtual system and have many same attributes providing flexibility and scalability of storage and networking resources. However, Fog computing is more resilient and secure than cloud computing. Fog computing helps to transmit more data in less bandwidth.

It is safe to state that Fog computing is ideal for businesses regularly processing large amounts of sensitive data, Whereas Cloud computing is ideal for small to medium sized businesses. These two technologies are different, yet similar in ways.

V. Challenges Ahead

There are many challenging issues of Fog computing that need to be addressed. Security is the biggest concern when it comes to the fog computing. It is complex to detect which user is attacking the system. Some of the challenging issues are as discussed under.

a) *Trust:* IoT networks are expected to provide reliable and secure services to the End users. This requires all devices that are part of the Fog network to have a certain level of trust on one another. Authentication plays a major role in establishing initial set of relations between IoT devices and fog nodes in the network. But this is not sufficient as devices can always malfunction or are also susceptible to malicious attacks [20]. In such a scenario, trust plays a major role in fostering relations based on previous interactions. Trust should play a two-way role in a fog network. That is, the fog nodes that offer services to IoT devices should be able to validate whether the devices requesting services are genuine. On the other hand, the IoT devices that send data and other valued processing requests should be able to verify whether the intended fog nodes are indeed secure. This requires a robust trust model in place to ensure reliability and security in fog network.

b) *Authentication:* Authentication of networked devices subscribed to fog services is one of the foremost requirement in fog network. To access the services of a fog network, a device has to first become part of the network by authenticating itself to the fog network. This is essential to prevent the entry of unauthorized nodes [20]. Authentication and authorization issues were not studied in the context of Fog computing. They were studied in the context of smart grids and machine-to-machine communications [31]. However, there are security solutions for Cloud computing which may not suit for Fog computing because Fog devices work at the edge of networks. The working surroundings of Fog devices will face with many threats that do not exist in a well-managed Cloud. This part of research also concerns with some privacy issues.

c) *End User's Privacy:* Fog computing paradigm extends the storage, networking, and computing facilities of the cloud computing toward the edge of the networks while offloading the cloud data centers and reducing service latency to the end users. However, the characteristics of fog computing arise new security and privacy challenges. The existing security and privacy measurements for cloud computing cannot be directly applied to the fog computing due to its features, such as mobility, heterogeneity, and large-scale geo-distribution [18]. Has surveyed the storage and security as a limitation of fog. However, this survey is very limited regarding open research challenges in security and privacy Issues for fog computing. A brief overview of fog security and privacy issues is discussed in [34]. Furthermore, some Counter measurements are found in [25], [31], [33], [2], [41], [26] have laid a solid foundation for the understanding of security and privacy issues in fog computing, this article differs from previous surveys in many aspects such as [41] Focused on only fog forensics, whereas [2] discussed a brief overview of privacy and security. However, [20] had discussed security and privacy issues and existing research for fog. Recently, security and privacy preservation are discussed in fog-based vehicular networks [13]. Currently many research is going on the privacy issue so that end user can securely connected to fog nodes and future work will expand on this.

d) *Security:* For the security issues, there is also some future work need to be investigated [3]. An online dictionary attacker in Fog computing makes authentication requests by trying every possible password for a specific user [40]. In normal authentication, such attacks can be prevented using lockout mechanisms to lock out the user account after a certain number of invalid login attempts. But, the same approach does not apply to Stand-Alone Authentication (SAA) in information systems with a large number of Fog devices: An attacker can run SAA with device D1 using its guess P A1, make another login request at device D2 using another guess P A2 and so on. This is like amounting online dictionary attacks on the same user in a distributed way. A solution requires all devices sharing a common user list with failed login requests, but such a coordination would not be easily achievable in the situations need SAA. A satisfactory solution to the distributed online dictionary attack is another direction of future work.

e) *Malicious Attacks:* Fog computing environment can be subjected to several malicious attacks and without proper security measures in place may severely undermine the capabilities of the network. One such malicious attack that can be launched is a Denial-of-Service (DoS) attack. Since majority of the devices connected to the networks are not mutually authenticated, launching a DoS attack becomes straight forward. The attack may be launched when devices that are connected to IoT network request for infinite processing / storage services. Existing defense strategies of other types of networks are not suited for fog computing environment mainly due to the openness of the network. The first major challenge is the size of the network. Potentially, hundreds and thousands of nodes forming an IoT network avail the services of fog / cloud to overcome computation and storage limitations and also enhance performance. Since all these devices cannot be authenticated by fog nodes, they may rely on trusted third party like a certification authority that issues some form of credentials to ensure device authentication. Man-in-middle attack, a very traditional hostile attack has higher probability of taking place [34]. It is hard to avoid and defend the man-in-the-middle attacks. A promising solution would be needed for Fog device. The gateways in the fog area can be spoofed. It would be difficult for the fog nodes and IoT devices to communicate using encryption and decryption as it may utilize more battery of mobile devices. According to [23] solution to this could be using Intrusion Detection System. Intrusion Detection Systems

(IDS) can be used for analyzing and controlling access as well as they generate log files for detecting malicious behavior. These systems can also detect Denial of Service Attacks and port scanning.

Finally, mobility between Fog nodes, and between Fog and Cloud, can be investigated. Fog computing deploys services close to the user where data is most often used. Fog devices are distributed in such a way that are close to the ground, where data is generated and operations are performed. This reduces burden on cloud computing as the required data are within the local context. So Fog computing built strong mobility platform.

Although a few works, such as [8] has proposed algorithm for the fog system. And [33], [13], [9], [35] considered the secure interaction of fog elements, authentication, and authorization for the fog computing, intruder detection, key agreements for fog computing, these approaches are either partially addressed the security and privacy issues or still in very early stages and needs more attention in future.

VI. Conclusion

Fog Computing is not a replacement for Cloud Computing. Limitations of Cloud computing that is probable reason for the birth of Fog computing. According to the present scenario of huge data and IOT Fog computing performs better than Cloud computing.

Fog computing was developed to handle users' needs better than cloud computing in addition to have other characteristics. In spite of many advantages of Fog computing, there are many issues in Fog computing that need to be addressed so that future work can be focus on it.

References

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

[2] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the Internet of Things: Security and privacy issues," *IEEE Special Section on Recent Advances in Computational Intelligence Paradigms for Security and Privacy for Fog and Mobile Edge Computing*, vol. 21, no. 2, pp. 34-42, March 2017.

[3] A. A. Lisbon, and R. Kavitha, "A study on cloud and fog computing security issues and solutions," *International Journal of Innovative Research in Advanced Engineering,* vol. 4, no. 3, pp. 17-22, March 2017.

[4] A. A. Dabhi, T. J. Raval, and K. Chaudhary, "Fog computing: A review and conceptual architecture, issues, applications and its challenges," *IJARIIE*, vol. 3, no. 5, pp. 717-722, 2017.

[5] A. B. Shah, J. Kannan, D. U. Shah, S. B. Ware, and R. S. Badodekar, "Fog Computing: Securing the cloud and preventing insider attacks in the cloud," *International Journal of Engineering and Computer*, vol. 5, no. 3, pp. 16009-16012, March 2016.

[6] A. S. K. Ratnam, M. Vuyyuru, P. Annapurna, and K. G. Babu, "An overview of cloud computing technology," *International Journal of Soft Computing and Engineering*, vol. 2, no. 3, pp. 244-246, July 2012.

[7] B. B. Rad, and A. A. Shareef, "Fog computing: A short review of concept and applications," *IJCSNS International Journal of Computer Science and Network Security*, vol. 17, no. 11, pp. 68-74, November 2017.

[8] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A comprehensive survey on fog computing: State-of-the-art and research challenges," *IEEE Communications Surveys and Tutorials,* vol. 20, no. 1, pp. 416-464, 2018.

[9] D. Koo, and J. Hur, "Privacy-preserving deduplication of encrypted data with dynamic ownership management in fog computing," *Future Generation Computer Systems*, vol. 78, no. 2, pp. 739-752, January 2018.

[10] E. Strohmaier, J. Dongarra, H. W. Meuer, and H. Simon, "The marketplace of high-performance computing," *Parallel Computing*, vol. 25, no. 1314, pp. 1517-1544, 1999.

[11] H. Gupta, S. Chakraborty, S. K. Ghosh, and R. Buyya, "Fog computing in 5G Networks: An application perspective," March 2017.

[12] I. Stojmenovic, "Fog computing: A cloud to the ground support for smart things and machine-to-machine networks," In *2014 Australasian Telecommunication Networks and Applications Conference (ATNAC),* pp. 117-122, 2014.

[13] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Communications Magazine*, vol. 55, no. 6, pp. 146-152, June 2017.

[14] K. Asanović, R. Bodik, B. C. Catanzaro, J. J. Gebis, P. Husbands, K. Keutzer, D. A. Patterson, W. L. Plishker, J. Shalf, S. W. Williams, and K. A. Yelick, "The Landscape of parallel computing research: A view from Berkeley," University of California, Berkeley, *Tech. Rep. UCB/EECS-2006-183*, December 2006.

[15] K. P. Saharan, and A. Kumar, "Fog in comparison to cloud: A survey," *International Journal of Computer Applications*, vol. 122, no. 3, pp. 10-12, July 2015.

[16] K. Gai, M. Qiu, L. Tao, and Y. Zhu, "Intrusion detection techniques for mobile cloud computing in heterogeneous 5G," *Security and Communication Networks*, vol. 9, no. 16, pp. 3049-3058, November 2016.

[17] L. Jiao, R. Friedman, X. Fu, S. Secci, Z. Smoreda, and H. Tschofenig, "Cloud-based computation offload-

ing for mobile devices: State of the art, challenges and opportunities," In *2013 Future Network Mobile Summit*, pp. 1-11, 2013.

[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, October 2014.

[19] R. Waheetha, and S. Fernandez, "Fog computing and its applications," *International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)*, vol. 2, no. sp.19, pp. 56-62, October 2016.

[20] 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. 19293-19304, 2017.

[21] M. Firdhous, O. Ghazali, and S. Hassan, "Fog computing: Will it be the future of cloud computing?," *Proceedings of the Third International Conference on Informatics & Applications*, Kuala Terengganu, Malaysia, 2014.

[22] N. Cranford, "The role of fog computing in 5G,". Available: https://www.rcrwireless.com

[23] P. More, and J. Kulkarni, "Fog computing," *International Research Journal of Engineering and Technology (IRJET)*, vol. 4, no. 2, pp. 1113-1116, February 2017.

[24] P. V. Patil, "Fog computing," *International Journal of Computer Applications, National Conference on Advancements in Alternate Energy Resources for Rural Applications (AERA-2015),* 2015.

[25] P. Kumar, N. Zaidi, and T. Choudhury, "Fog computing: Common security issues and proposed countermeasures," In *Proc. Int. Conf. System Modeling Adv. Res. Trends (SMART)*, pp. 311-315, November 2016.

[26] R. Romana, J. Lopeza, and M. Mambob, "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.

[27] S. Erich, D. Jack, W. Meuer, and H. Simon, "Recent trends in the marketplace of high performance computing," *Parallel Computing*, vol. 31, no. 34, pp. 261-273, 2005.

[28] S. Yangui, P. Ravindran, O. Bibani, R. H. Glitho, N. B. Hadj-Alouane, M. J. Morrow, and P. A. Polakos, "A platform as-a-service for hybrid cloud/fog environments," In *2016 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)*, pp. 1-7, 2016.

[29] S. Yangui, and S. Tata, "The SPD approach to deploy service-based applications in the cloud," *Concurrency and Computation: Practice and Experience*, vol. 27, no. 15, pp. 3943-3960, October 2015.

[30] S. Singh, Y. C. Chiu, Y. H. Tsai, and J. S. Yang, "Mobile edge fog computing in 5G era: Architecture and implementation," *2016 International Computer Symposium (ICS)*, 2016.

[31] 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,* pp. 37-42, June 2015.

[32] S. Kitanov, and T. Janevski, "Energy efficiency of 5G mobile networks in hybrid fog and cloud computing environment," *RTA-CSIT*, pp. 41-46, 2016.

[33] S. Yi, Z. Qin, and Q. Li., "Security and privacy issues of fog computing: A survey," *In Proc. 10th Int. Conf. Wireless Algorithms, Syst., Appl. (WASA)*, pp. 685-695, August 2015.

[34] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: A review of current applications and security solutions," *Journal of Cloud Computing Advances, Systems and Applications*, vol. 6, no. 19, 2017**.**

[35] T. Wang, J. Zeng, Md. Z. A. Bhuiyan, H. Tian, Y. Cai, Y. Chen, and B. Zhong, "Trajectory privacy preservation based on a fog structure for cloud location services," *IEEE Access*, vol. 5, pp. 7692-7701, May 2017.

[36] T. Ercana, "Effective use of cloud computing in educational institutions," Yasar University, Department of Computer Engineering, Turkey, January 2010.

[37] U. A. Deshmukh, and S. A. More, "Fog Computing: New approach in the world of cloud computing," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 4, no. 9, pp. 16310-16316, September 2016.

[38] V. Dubey, D. Sahu, S. Sharma, and A. Tripathi, "Cloud computing in mobile applications," *International Journal of Scientific and Research Publications*, vol. 2, no. 8, pp. 1-9, August 2012.

[39] X. Zhu, D. S. Chan, H. Hu, M. S. Prabhu, E. Ganesan, and F. Bonomi, "Improving video performance with edge servers in the fog computing architecture," *Intel Technology Journal*, vol. 19, no. 1, pp. 202-224, April 2015.

[40] X. Huang, I. Stojmenovic, S. Wen, and H. Luan, "An overview of fog computing and its security issues," *Concurrency and Computation: Practice and Experience*, vol. 28, no. 10, pp. 2991-3005, July 2016.

[41] Y. Wang, T. Uehara, and R. Sasaki, "Fog computing: Issues and challenges in security and forensics," In *2015 IEEE 39th Annual Computer Software and Applications Conference (COMPSAC),* vol. 3, pp. 53-59, July 2015.