IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

Fog Computing: Overview and Research Challenges

A. Ahuja

Department of Computer Science, Guru Nanak Dev University, Amritsar, India

**Corresponding Author: annieahuja89@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 18/May/2018, Published: 31/May/2018

***Abstract*—** With the increasing use of Internet and its services leads to the generation where availability of data has become boundless. The abundant flow of data due to the advent of IoTs is not new and for storing such huge amount of data paved the way for the technology like cloud computing. But with cloud computing still some issues need to be resolved such as high latency, network bandwidth, network congestion, security and others that cannot be compromised in case of real time applications. 'Fog computing' introduces a new dimension to the way cloud works as it focuses on the provisioning of resources and services at the edge of the network that means closer to end devices and hence there is less delay in processing client's request in distributed environment. So in this perspective it is heading the way to cloud computing paradigm. Its evolution is not for replacing cloud computing but to complement in such a manner that its potential can be realized and utilized in an effective manner. This paper highlights the fog computing technology concept and gives an insight details in terms of its characteristics, and the related work done in prospect of challenges.

***Keywords*—** Fog computing, Cloud computing, Edge computing, IoT, Programming model

I. INTRODUCTION

The Internet of Things (IoT) environment facilitates interaction among things and humans in a seamless manner as it revolutionized the way in the making of many items from home appliances to all types to sensors. On the other side, the amount of data generated by IoT environments is quite huge, which proves to be useful on getting into insight details which means the careful exploitation of data [1]. In this regard, cloud computing plays a significant role as it offers on-demand availability for storing data to the organizations or individuals and also able to process services that can scale to IoT requirements. But the main issue with cloud approach lies in managing real time and sensitive applications like emergency response, healthcare monitoring as it is not considered to be good one due to the delay involved in getting response back from the cloud [2]. Moreover, sending too much data to cloud for the purpose of storage and processing also leads to saturation of network bandwidth and no more considered to be scalable. Security concerns also rise as data is now entrusted to a third party provider. Even in the recent analysis of a healthcare-related IoT application that involves 30 million users showed that data goes up to 25000 tuples in a second and in case of real time data sources, the data touches millions of tuples in a second as published by IEEE Computer Society in an article titled "Fog Computing: Helping the Internet of Things Realize its Potential" in 2016. In order to tackle these issues, edge computing comes into existence. Edge computing involves the use of computing resources at the edge of the network that is to be used near IoT sensors for the purpose of local storage and data processing. It would reduce congestion in network and also helps in decision making task to be carried out in a speedy manner. But with edge computing multiple IoT applications cannot be handled that are competing for limited resources which lead to conflict in accessing a shared resource and hence increased latency. This paper explores the concept of fog computing in detail and provides a systematic review on the challenges being faced by this emerging computing technology in each and every aspect as most of the available literature had focussed on security concerns. The researchers who are at initial stage can come to know about the current scenario of fog paradigm and can proceed further in this direction so that the true potential of this technology can be realized with the passage of time. The seamless integration of edge devices and cloud sources is possible with fog computing. Resource conflicts can be avoided at the edge by taking maximum advantage of cloud resources and thus, provides coordination in the use of geographically distributed edge devices.

A. Defining Fog Computing: The term 'fog' in fog computing represents the cloud which is closer to 'end users' networks that is more closer to ground. The term 'Fog Computing' comes into existence in 2012 by the Cisco systems to address the challenges of cloud computing as a backend infrastructure for IoT. Cisco considered fog computing as an extension to cloud computing and not a substitute and provides the services

such as computation, storage and networking between IoT devices/sensors and to the cloud servers that are present at the backend. The fog computing paradigm is well suited for implementing in real time applications like big data analysis, etc. The feasibility of implementing this scenario is the presence of fog node in this paradigm. A fog client submits its task to the nearest fog node, in this way fog nodes provide location awareness and takes less time in handling fog client request that results in low latency which is one of the key requirements in implementing real time scenarios [3].

There are three main components in fog computing environment as represented in Figure1 [3]:

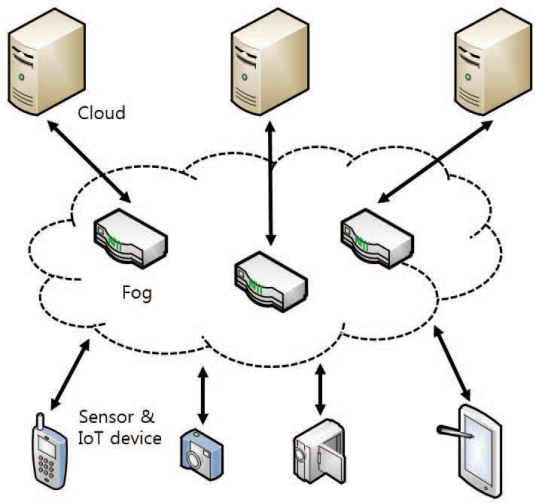

Figure 1. Fog Computing Environment [adapted from [3]]

IoT nodes/devices/sensors, fog nodes and cloud as back-end. Fog computing environment comprises of traditional networking components that have more computing power as compared to IoT nodes. The networking components include routers, switches, set top boxes, and so on which lies closer to the IoT nodes and the connection between IoT nodes and fog nodes is established by providing short-range communications that includes Wireless Fidelity (Wi-Fi), Bluetooth, etc. The fog nodes' capabilities include diverse computing, storage, networking, etc where as IoT nodes are provided with sensors that generate local data. The purpose of having fog nodes in the middle layer is that processing of data in real time can be done more easily nearby the network edge and also it is not feasible to send all the data from IoT nodes to the cloud back-end as it will take much more time to process, therefore, only extensive computation data is sent to the cloud for processing through high speed wireless or wired communication. This scenario reduces the latency as significant amount of data is processed by fog nodes. Networking components plays a vital role in fog computing environment as they help to create large geographical distributions of cloud-based services. Furthermore, the processing of data collected from IoT devices analytically can even predict future situations and thus helps in making decisions. Thus, efficiency of fog computing can be realized in terms of low latency, reduced network congestion, power consumption , etc. and efficiently meets the requirements of IoT as compared to cloud computing [3, 4].

The paper is structured in the following manner: Section I contains the introduction of fog computing and its need, Section II contains the characteristics of fog computing, Section III contains the challenges that are being faced by fog paradigm, and Section IV contains the related work done in terms of providing classification to the discussed challenges.

II. CHARACTERISTICS OF FOG COMPUTING

Fog computing is a distributed deployment framework that involves the use of edge resources for tackling the IoT data generated locally and thus brings convenience of data storage, transmission, and management. Following are the characteristics as represented in Figure 2 of fog computing paradigm that helps to figure out the distinction between cloud computing and fog computing paradigm [5, 8, 9].

A. *Low Latency:* Fog layer is the middle layer in fog computing environment which forms a core component in reducing network latency. The fog nodes are at close proximity to the IoT devices , therefore request made by the fog client that does not involve extensive computation is handled by fog layer itself and hence response time is quite less in comparison to if each and every request is forwarded to back-end cloud.

B. *Location Awareness:* The location awareness refers to the location of fog nodes. In fog computing paradigm, tracing of fog nodes whether actively or passively can be done to provide rich services at the network edge. As IoT nodes generate local data hence, make local IoT applications accessible for devices at specific areas by using fog nodes. Therefore, on the basis of location of fog nodes, devices' region can be figured out.

C. *Heterogeneity:* Heterogeneity refers to the diversity of devices used in fog computing as specifically it focuses on mobile devices.

D. *Decentralization:* Unlike cloud computing paradigm that is based on centralized architecture, fog computing is based on decentralized architecture to manage resources and services. The services and applications that are provided by fog need the geographical distribution of nodes that is nodes to be located at different location in order to facilitate the request of user in an efficient way.

E. Large number of nodes: It is much obvious that due to the distributed deployments required by fog architecture, very large number of nodes are required as a consequence. For example, in sensor networks, Smart Grid, etc.

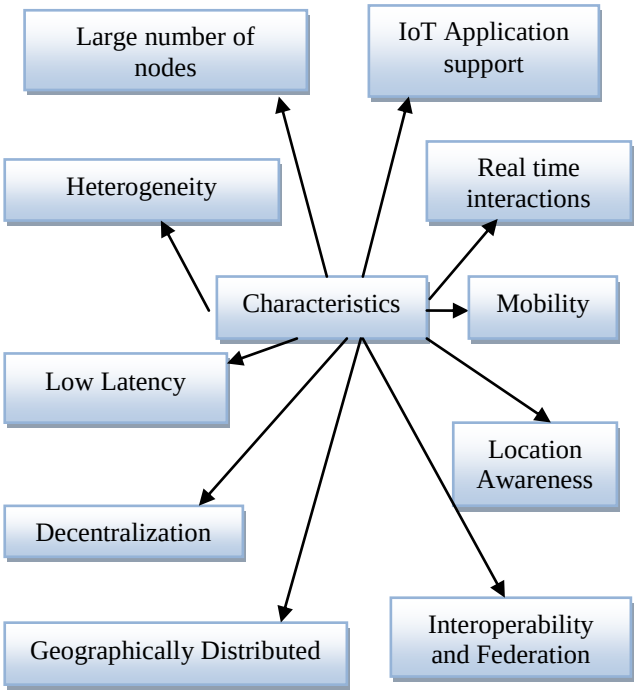

Figure 2. Characteristics of Fog Computing

F. Mobility: There is support for mobility as it is required by many fog applications to have direct communication with mobile devices. The mobility techniques like LISP protocol, etc can be used. LISP is Location/Identity Separation Protocol that efficiently handles the workload virtualization as the data can easily be moved from one place to another and keeps it secure as well.

G. Geographically Distributed: The deployment of fog nodes in a geographically distributed manner at points such as on roadways, along highways, etc. is essential so that high quality data stream can be received by fog nodes from IoT devices.

H. Real-time interactions: Some of the significant fog applications involve real-time interactions like smart traffic lights which automatically changes its colour on detecting the flashing lights of a police car using video cameras.

I. Interoperability and Federation: Some fog applications having high workload require fog nodes that are provided by different providers/owners, therefore, fog components /nodes must be capable enough to interoperate and federation of services across domains.

J. IoT Application support: Fog computing is used to provide support to large scale IoT applications like in managing power grid, monitoring of environment, climate change monitoring, otherwise it put overhead to the centralized cloud but fog has its expertise as well as autonomy to manage billions of IoT devices.

III. CHALLENGES OF FOG COMPUTING

Following are the challenges that need to be addressed in order to realize the potential and for making a fog paradigm a big success:

A. It is difficult to realize the global storage which has no boundary in terms of its size, always accessible and performs in a speedy manner as the data is generated locally. Such an implementation is still an open challenge question for fog computing researchers.

B. In fog computing paradigm, due to the distributed deployment of fog nodes, users can take advantage of various services by moving to a different location as nodes differ from location to location. But to implement this scenario, there is reliance on the implementation of service delivery protocols which is easy to realize. Whenever a specific service is required, the virtual machines are configured in such a manner that they can make the service provisioning in dynamic way as it is done usually. But the associated challenges in a row such as starting and stopping of services, and to predict whether VM-based or container based virtualization be used and so on are hard to implement.

C. It is difficult to implement security and privacy policies on both these computing paradigms due to their heterogeneous nature that makes exchanging of data too difficult between the nodes that manufacturers started simply avoiding these policies which preserve the user's sensitive data.

- Fog nodes that appear to be small cloud and close to end users can face a challenge in terms of even system security due to the deployment of fog devices in the positions that are generally out of surveillance and protection. Therefore, security issues can be arisen even with the traditional malicious attacks like data hijack, etc. Traditional networking components are highly susceptible to malicious attacks.
- Fog computing is exposed to man-in-the-middle attack in which fog devices acting as gateways may be compromised and traditional anomaly detection methods are unable to identify the features of this attack. Moreover, sometimes it is hard to protect the communication between fog and IoT nodes using encryption techniques as

these techniques require more battery consumption on mobile device.

- Intrusion detection techniques are used to analyze the attacks such as attacks on virtual machines, flooding attack, etc. In order to monitor and detect the malicious activity, it monitors log file of user and access mechanism. Moreover, in IoT device that is based on fog computing, it becomes hard to find root kit. An attacker can even attack system using hardware virtualization by gaining higher privileges than embedded hypervisor and can obtain sensitive information as well.
- It becomes a challenge as in case of heavy workload, task is divided among several nodes. This might be the case that some of the fog nodes are under malicious attack, so it is difficult to ensure the security and integrity of data.
- Data must be protected by encryption techniques that are light-in weight or using masking techniques as in fog computing limited resources are available in case of mobile devices[3]. As a result, applying cryptography sometimes not a feasible solution and thus compromises the security in processing large volume of data.

D. Some fog applications require data to be stored locally rather than on cloud such as applications that involve financial and medical institutions. According to IDC report mentioned that 44 zetabytes of data is expected to be generated by various sources like people, process, and things by 2020. So there should be some mechanism such that fog provider can monitor as well as control their data.

E. For resource provisioning, scaling of fog resources as per the users' request must be accomplished in an efficient manner. It is not essential that fog nodes contain similar resources as these are heterogeneous in nature and moreover maintained by different owners the resources can also vary in their implementation such as difference in RAM capacity, Storage utilization, and performance of CPU and bandwidth of network. Furthermore, fog nodes are smaller in size in comparison to cloud servers. The high end computational tasks are still performed on the cloud servers while fog nodes are not as powerful and thus deployed in small batches using components like routers, gaming consoles, etc.

F. It is difficult to identify the appropriate method for the collaboration of nodes as computational fog nodes are deployed in a distributed manner across the edge network. Moreover, it is a hard to achieve to make the components/devices provision for general purpose computation. The compatibility of fog with IoT is in structural way but for other networking systems like vehicular network, Content Distribution Network, etc is quite difficult.

G. Proper mechanism should be followed for the distribution of computational tasks and services among the fog computing infrastructure that comprise IoT nodes, Fog nodes and back-end cloud. It is difficult to design the mechanism for implementing data visualization through web interfaces in fog paradigm. There are many factors that can affect the Service Level Agreement (SLA) like energy consumed, network bandwidth, service cost, etc. Sometimes it is very difficult to predict the metrics for provisioning of service and there corresponding Service Level Objectives (SLOs). But it is highly recommended to retain and maintain the QoS of the fog nodes. This is actually one of the purpose for which the fog nodes are designed.

H. Depending on the fog application, fog devices need to be set up at public places and moreover, in fog paradigm, computation logic also get moved to the edge of network that means third party vendor hardware components are to be utilized which can also cause a security concern and moreover, it is not possible to apply encryption techniques at all levels due to the manifold increase in power consumption.

I. Users' privacy revolves around four aspects that include identity privacy, data privacy, usage privacy, location privacy.

- In identity privacy, concern is to secure the user identity in terms of name, password, license number, pan number, and so on while doing authentication on fog nodes.
- Usage privacy deals with the pattern of utilization of services that are offered by fog nodes that can also violate privacy.
- In Location privacy, the location of user should not be disclosed as it is done by most of the applications on mobile devices as their sole purpose is to collect user location information.
- Data privacy can be breached by exposing to third party when they are on fog nodes or while doing transmission between two parties.

J. In fog paradigm, decentralization architecture is involved to provide configuration on billions of devices so it is hard to find failure of node information as well as to provide patching updates to software. For the critical applications like health-care monitoring, it is hard to realize.

K. Enabling real time analytics refers to taking critical decision that which alternative fog node can be utilized use in order is critical to reduce latency.

L. If the architecture is based on static configurations then it is difficult to realize the scalability and flexibility in fog with IoT application like in Apache Storm and S4. Fog computing requires the dynamic configuration due to mobile devices that can join and leave network anytime.

M. Still no standardization mechanisms are there which can ensure that different providers or owners of fog nodes are using similar standards or compatible one in terms of various resources that are utilized by fog paradigm. Examples of resources includes memory capacity, network bandwidth, etc. The other side is that it involves the geographic distribution of nodes and these fog nodes are maintained by different owners and it might be possible that they employ different standards of security measures. As a consequence, it is not easy for the users to trust different fog nodes.

IV. RELATED WORK

Table I. List of Challenges along with their References and Classification

Challenge	Reference	Challenge Classification
C.	[3], [4], [6], [8], [9], [11]	Security issue
D.	[3], [6]	Data Management
I.	[3],[8], [11]	Privacy issue
F.	[4]	Structural issue
G.	[4], [10]	Service oriented, Quality of Service (QoS)
H.	[6]	Power consumption
J.	[6], [9], [10]	Heterogenous device management
K.	[7]	Real-time analytics
M.	[9], [11]	Standardization
A.	[9], [11]	Storage system
B.	[11]	Service delivery protocols
E.	[11]	Resource Management
L.	[11]	Programming model

In the table 2, author's theoretical findings are presented as list of challenges with their references and category of classification. It is observed that security and privacy issue is one of the biggest challenges that need to be tackled as soon as possible. Moreover, fog computing paradigm has the desired potential of revolutionizing the working of current scenario in mobile web applications but that can be realized only when the above challenges will be addressed by the researchers.

V. CONCLUSION AND FUTURE SCOPE

The emergence of fog paradigms is due to the abundant flow of data generated by IoT devices. Developers choose to adopt this emerging technology as it reduces the time in handling the request locally using fog layer rather than on the cloud for some of the applications. As a consequence, it reduces burden on cloud servers. There is improvement in the quality of service as data gets generated locally and hence, reduced latency time. It is also facing many challenges in terms of security and privacy issues and some of the security and privacy issues are inherited from cloud computing, as both computing paradigms complement each other. The other side of security issues that is being encountered in fog paradigm is only due to the authentication procedures that cannot be applied to the whole framework of fog paradigm because of geographic distribution of nodes and still many more questions are under survey. It is also analyzed by studying literature that fog computing proves to be quite useful for those applications that demands faster processing with less delay while cloud computing fulfils the needs where high end computing that serves the applications that need as well as economical. It has a great potential and future scope as it has the capability to manage application areas such as Virtual Reality, gaming, finance where low latency is required and is quite difficult to achieve with cloud computing as compared to fog computing. Its use cases include smart traffic lights, self maintaining train, Wireless Sensor and Actuator Networks (WSAN), Smart Grids, and many more. Therefore, you cannot evade fog computing in these application areas.

ACKNOWLEDGMENT

I would like to thank my colleagues for their invaluable guidance.

REFERENCES

[1] G. Kaur, M. Sohal, "*IOT Survey: The Phase Changer in Healthcare industry",* International Journal of Scientific Research in Network Security and Communication, Vol. 6, Issue 2, pp.34-39, 2018.

[2] Anitha H M, P. Jayarekha, "*Security Challenges of Virtualization in Cloud Environment",* International Journal of Scientific Research in Computer Science and Engineering, Vol. 6 Issue 1, pp. 37-43, 2018.

[3] K. Lee, D. Kim, D. Ha, U. Rajput, H. Oh, "*On security and privacy issues of fog computing supported Internet of Things environment",* In the Proceedings of 2015 6th International Conference on the Network of the Future (NOF), pp. 1-3, 2015.

[4] R. Mahmud, R. Kotagiri, R. Buyya, " *Internet of Everything",*Springer Publisher, Singapore, 2017.

[5] M. Firdhous, O. Ghazali, S. Hassan, " *Fog Computing: Will it be the Future of Cloud Computing?",* In the Proceedings of 2014 Third

International Conference on Informatics & Applications, Malaysia, pp. 8-15, 2014 .

[6] A. Dasgupta, A. Q. Gill, " *Fog Computing Challenges: A Systematic Review*", In the Proceedings of 2017 *Australian* Conference on Information Systems (ACIS), Australia, pp. 1-8, 2017.

[7] R. Waheetha, S. Fernandez, " *FOG COMPUTING AND ITS APPLICATIONS*", International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST) ,Vol. 2 Special Issue 19, pp.56-62, 2016.

[8] Jianbing Ni, K. Zhang, X. Lin, X. S. Shen, "*Securing Fog Computing for Internet of Things Applications: Challenges and Solutions*", IEEE Communications Surveys & Tutorials, Vol. 20, Issue 1, pp. 601-628, 2017.

[9] S. Kumari, S. Singh, Radha, "*Fog Computing: Characteristics and Challenges",* International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol. 6, Issue 2, pp. 113-117, 2017.

[10] S. Yi, C. Li, Q. Li, "*A survey of Fog Computing: Concepts, Applications and Issues"* , In the Proceedings of 2015 Workhop on Mobile Big Data, China, pp. 37-42, 2015.

[11] Z. Hao, E. Novak, S. Yi, Q. Li , "*Challenges and Software Architectures for Fog Computing",* IEEE Internet Computing, Vol. 21, Issue 2, pp.44-53, 2017.

Authors Profile

Ms. A Ahuja pursued Bachelor of Computer Appli- Cations from Guru Nanak Dev University, Amritsar In 2011 and Master of Computer Applications from Punjab Technical University in 2014. She is currently Working as Assistant Professor in the Department of Computer Science, Guru Nanak Dev University, Amritsar. She has 4 years of teaching experience.

