

A Survey on Use Cases and Security Issues in Fog Computing

^{*1} Prof. Vaijayanti H. Panse, ² Prof. Bhumika Neole, ³ Prof. Minal Ghatе, ⁴ Prof. Bhagyashree Lad

^{*1} Adjunct Assistant Professor of Practice, VNIT, Nagpur

^{2,4} Assistant Professor, Shri Ramdeobaba College of Engineering and Management, Nagpur

³ Assistant Professor, Guru Nanak Institute of Engineering and Technology, Nagpur

Email: vhpanse@gmail.com, neoleba@rknc.edu, mruy77@gmail.com, ladbv@rknc.edu

Received: 20th September 2018, Accepted: 11th October 2018, Published: 31st October 2018

Abstract

According to the forecast that billions of devices will get connected to the internet by 2020, it will become a challenge for real time applications to handle this huge data generated while considering security issues as well as time constraints. The cloud faces many issues like high latency, network failure, low storage capacity, extra computational capability and high computational power due to centralized server approach. These issues can be resolved by using a new concept called, Fog Computing. Fog computing is an emerging research area for both academia and industry. In this paper, we view and summarize different use case scenarios of fog computing. The recent research contributions on security and privacy issues in fog computing are also discussed in this paper. Finally, this paper also highlights several open issues in fog computing thereby giving light on future research directions for implementing fog computing systems.

Keywords

Fog Computing, Internet of Things (IOT), Cloud Computing, Security, Privacy, Use Case Scenarios, Smart IOT Applications.

Introduction

The Internet of things (IOT) will soon reach a stage when each and everything around us will be connected to the internet. IOT and cloud computing has advanced in a way to bring many significant advantages to different IOT applications. Internet of everything is now becoming a need to ease different activities in industries as well as household applications. It has a key role in designing smart homes, smart industries and smart cities as well.

As huge amount of data is generated by the sensors and applications in IOT, the cloud, as a centralised server, may face issues like high latency, high computational power, inadequate storage, etc. The solution to these issues was first introduced by CISCO[1]. This new technology called Fog Computing focuses on bringing the cloud closer to end devices. This reduces the time required to send the data to cloud, which is very important issue while handling real time applications, like navigation. Also, Fog Computing can be used to pre-process the data before sending it to cloud so that only required data will be forwarded. This will help to reduce the network bandwidth required.

Fog computing is an intermediate layer between cloud and the terminal devices. The fog nodes or gateways are designed in such way as to store and pre-process the data locally before sending it to cloud[2]. The data which requires storage for long time can only be sent to cloud. Instead of using cloud as single server, distributed approach of fog computing is used to reduce the computational power and storage capacity as shown in Figure 1. The fog nodes have significant storage and computational capabilities to handle the devices in their region. The fog nodes or gateways will communicate with terminal devices at one end and cloud at the other end.

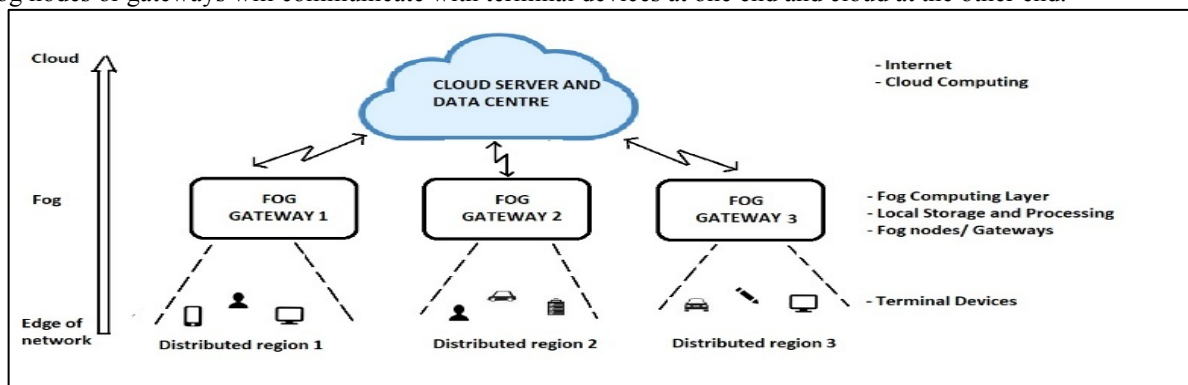


Figure 1: Distributed Approach of Fog Computing

Fog computing brings many benefits for IOT applications as summarized below [2]:

- **Low Latency:** There are certain latency sensitive real time applications where emergency responses are required. Fog computing assures low latency as compared to cloud computing.
- **Interoperability:** IOT brings different devices having different sets of rules or protocols. Fog nodes are capable of interoperating with different protocols.
- **Distributed Approach:** The distributed approach of fog computing help to reduce the overall storage and computational resources required.
- **Scalability:** As fog node is closer to the end devices, it can allow to scale the number of connected devices.

It is always required to give a better experience of service to the end user. The main QoS parameters can be identified as reliability, energy consumption, latency, support for network virtualization, connectivity and cost.

Reliability: The fog-based system must give reliable results in context of real time applications. The results provided must be correct at the same time minimizing the delay. Fog computing must address reliability issues like electromagnetic interference, end to end packet reliability, etc. SDN like architectures can be used to ensure end to end reliability in fog-based systems [3].

Energy Consumption: Energy consumption of all devices in fog network has a trade off with latency required [4]. Several works have highlighted this issue. Energy requirement of fog nodes for computations and data processing must be addressed to take care of energy constraints of networked devices.

Latency: Maximum allowable latency for a particular service or application can be set as the threshold to achieve desirable quality of service. This is the most important QoS parameter since this is the reason to switch to fog computing from cloud computing.

Support for Network Virtualization: SDN and NFV are the main techniques that allow virtualization of network devices. These are very popular because of their wide range of services [4]. The support for implementing fog computing along with SDN is the key parameter for improving the QoS of fog-based systems.

Connectivity: Un-interrupted communication between end devices in fog computing is necessary for network management. Several researches have already worked on this issue and developed different fog models for connectivity management and resource discovery [4].

Cost: Cost is an important factor in service provisioning of the fog networks. Cost is equally influential for both user as well as service provider. This cost can be considered as network cost related to bandwidth requirement, deployment cost for the infrastructure and finally, the execution cost while performing different computations [4].

In this paper, we present different inspiring use cases of fog computing and security issue as one of the important challenges in the implementation of fog computing. The rest of the paper is organised as follow: Section 2 surveys different use case scenarios of fog computing, Section 3 discusses about the challenges faced while implementing fog with IOT. Section 4 focuses on the security and privacy issues faced by fog systems along with the related work to solve the issue. Section 5 presents the possible open issues and finally, Section 6 concludes this paper.

Use Cases of Fog Computing:

Fog computing is used in variety of real time applications. This paper surveys selected applications that use fog computing with IOT. There is significant improvement in different aspects of quality of service of the given application or use case. Figure 2 illustrates different use case scenarios considered in this paper.

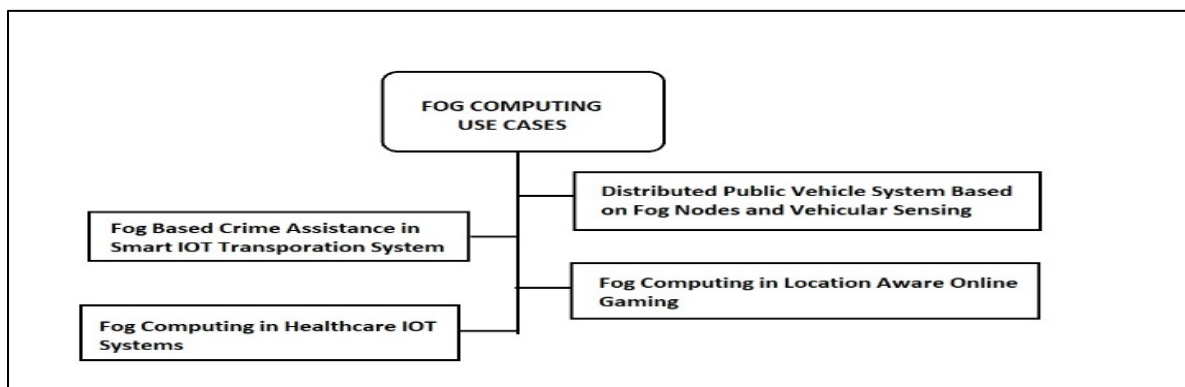


Figure 2: Use Case Scenarios of Fog Computing

Yongxuan Lai, et al. (2018) proposed a distributed public vehicular system based on fog nodes and vehicular sensing. Distributed public vehicular systems such as Uber or Ola have brought a big change in our lives. The proposed system studies on real world data to demonstrate that the scheme using fog nodes achieves higher service

ratio of requests and better efficiency. The framework of fog based public vehicle scheduling system (FPVS) consists of two procedures. First is metadata gathering and cost estimation. In this part, sensors on vehicles generate the data which is directed to fog nodes where local calculations are carried out to map the position of vehicular node on given road segment. The cost is estimated and uploaded on fog nodes. In second part, the request from user is sent to the cloud and route is decided by the cloud. The corresponding processed data would be dispatched to fog nodes to find the matched vehicles. Overall performance of the system is observed to be improved in terms of service ratio, waiting time and share factor. This research integrates fog nodes and vehicular sensing for request responsive scheduling systems[5].

Augusto J. V. Neto, et al. (2018) applied fog computing in smart video surveillance system to enhance crime assistance in a cost-efficient way. This research aims at providing fog-based approach to support efficient smart video surveillance that detect and predict crime incidents quickly and automatically. The system consists of three tiers. First tier has in-vehicle fog nodes which capture local sensory data and implement crime analytics. The second tier has fog computing infrastructure with high level crime analytics. It also tries to find the response police vehicles to quickly deal with the crime incident. The third tier is the mobile application that report the crime to the police within short latency. The laboratory outcomes indicate significant improvement in CPU usage by around 27.76% and energy saving (62.14%) efficiency. This approach also required much less network bandwidth (51.98%) resources to make it more scalable and cost effective[6].

Blesson Varghese et al. (2017) highlighted the benefits of using fog computing for an online game use case. The use case was an open source version of location aware online game, called iPokemon. In this game, the user through his smartphone or tablet locates and captures the Pokemons which are distributed over a city. This requires real time GPS tracking to update the user position, global view of every peer user and location of Pokemons. In this paper, they partitioned the servers such that cloud server to maintain a global view of Pokemons and fog servers to have a local view of users. According to their preliminary results, they found an improvement of 20% in the average response time for a user when fog computing is used as compared to only cloud computing model. Also, the data traffic was observed to be reduced by 90% for the said use case[7].

Amir M. Rahmani, et al. (2017) proposed the concept of fog computing in healthcare IOT systems. They formed a geo-distributed intelligent intermediate layer between sensor nodes and the cloud. The design demonstrates improvement in overall system parameters like intelligence, energy efficiency, security and reliability. The sensing to actuation latency of fog -based system was found to be 21ms which was significantly low as compared to its counterpart cloud-based system (161ms). An enhanced IOT healthcare system is realised using a network of smart e-health gateways at the fog layer. A prototype of smart e-health gateway (UT-GATE) is also presented where some of the high-level features are discussed. A fog-assisted medical case study called Early Warning Score (EWS) targeting patients with acute illness is implemented and analysed in detail. The research work demonstrates complete data flow from sensor nodes to cloud and the end users in effective way [8].

Challenges in Fog Computing

Since Fog Computing is an emerging research area, it requires more work to address all the aspects of challenges and open issues. This would help the researchers to get proper research direction towards implementing an efficient fog computing mechanism. Figure 3 indicates some of the research challenges faced while implementing fog computing with IOT [2].

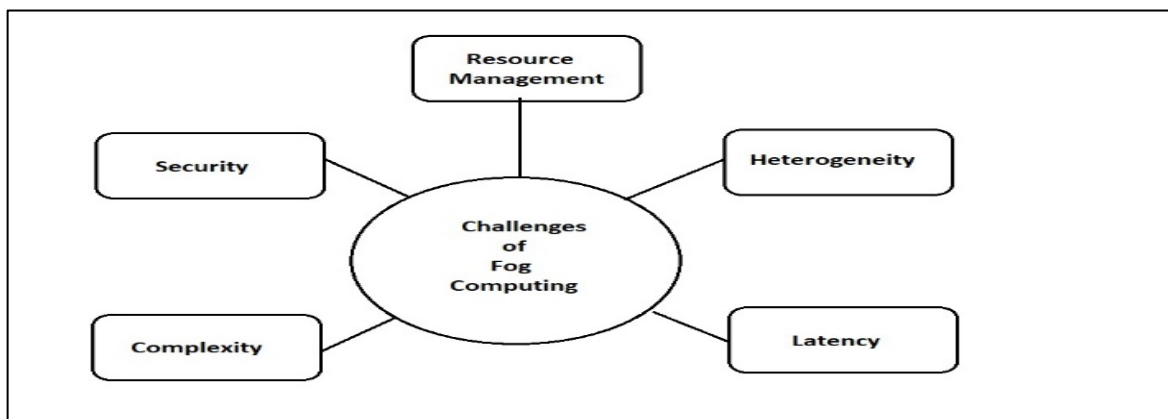


Figure 3: Challenges of Fog Computing

- **Security:** Since fog nodes are at the edge of network, these are more prone to cyber-attack. The tools or processes that are used in cloud computing for security purpose are not suitable for fog computing because

of different formats, mobility and heterogeneity. Thus, more research is required to ensure security in fog-based systems.

- **Resource Management:** Fog computing requires fog servers and data storage facilities at the edge of the network to speed up the processing. The management of these additional computing and storage resources introduces management and maintenance costs. Thus, research should focus on fog-based system to be properly analysed for effective management of fog servers.
- **Heterogeneity:** There are variety of IOT devices and sensors communicating with fog servers. They may have different protocols, storage capabilities, sensor characteristics, etc. The coordination between these devices and fog server as well as communication between geographically distributed fog servers is a big challenge.
- **Latency:** Latency is very important parameter to look upon. Low Latency was the main reason to bring cloud closer to end device through fog. Hence, if latency requirement is not satisfied, the performance would be degraded resulting in user dissatisfaction.
- **Complexity:** As there are large number of sensors and IOT devices available, the selection of an optimal device is a challenging task. The complexity would increase if the specified software or hardware is to be collaborated for a particular user requirement. Difference in IOT devices characteristics, hardware configurations, etc. increases complexity of the system resulting in difficulty of operation.

Security and Privacy Issues in Fog Computing:

Data communicated over fog computing systems are more vulnerable to cyber-attacks as compared to cloud computing. Many research papers provide studies and models for encryption and other security mechanisms in fog computing. Still, further research is required to implement security and privacy measures to improve the network security in fog computing. In this paper, we surveyed some of the related works for securing fog computing in IOT applications.

M. Mukherjee, et al. (2017) identified different issues in security and privacy of fog networks. One of the important issues is the trusted environment. Certain level of Trust is must among the devices used in fog networks which requires a robust trust model to take care of reliability and security of fog networks. Several works have been proposed to identify the attributes to define the trust of fog service. However, the challenges faced requires to re-address the issue [9]. The author also discussed other security and privacy issues like authentication, secure communication, end user's privacy and malicious attacks. The author also well studied several existing researches for security and privacy challenges in fog services [9].

Abebe Abeshu Diro, et al. (2018) analysed security challenges in reference to cyber-security principles and proposed a novel lightweight encryption scheme for fog computing. The scheme consists of five processes: key generation, client encryption, fog encryption, fog decryption and client decryption. In the distributed fog network any one node may be considered for generation of key and as a co-ordinator. The scheme is analysed for encryption and decryption runtime efficiencies for 32 bytes, 64 bytes and 128 bytes of data. This outsourcing of security function to fog nodes was found to be effective and improved the efficiency of the IOT applications [10].

Thanh Dat Dang, Doan Hoang (2017) focus on providing a data protection model which allows users to access the resources securely. The model consists of three core components, namely, Region based Trust Aware Control, Fog-Based Privacy-Aware Role based Access Control and the Mobility Management component. This model takes care of trust translation among fog nodes, providing access to newly joined devices and managing the mobility to handle location requests in the defined region. The model was evaluated using a test bed which included authorization and mobility services. The fog system with security model was compared with cloud model which showed much improvement in execution time and overall system performance [11].

Open Issues and Research Trends in Fog Computing:

Security is a critical issue in fog computing which requires great attention. The fog nodes or gateways must be designed in such a way to provide appropriate protection and authentication services to the fog-based systems. Security may be achieved by employing different encryption and decryption schemes, firewalls and configurable hardware settings to detect unauthorized entry in the network. Hence, both software and hardware approaches may be studied to provide security and privacy of data in fog-based IOT applications.

Designing a fog platform that can function with different protocols is itself a challenge. A common platform is required to be designed, especially for industrial IOT applications which will integrate all heterogeneous computing and communicating devices and will support their interoperability.

Minimizing the response time is another open issue for all real time applications like navigation, video streaming, etc. The fog computing resources must be so designed and deployed as to minimize the response time of the network application. Appropriate distribution of fog nodes for optimum performance is also a separate research approach that can be considered while implementing fog-based systems.

Optimum utilization of computing resources like CPU or microcontrollers is becoming a new research paradigm. CPU efficiency and usage should be improved to implement more energy efficient systems. The work focusing on energy efficiency of fog computational devices gives scope for further research in this domain.

- Looking at the current research trends in fog computing, we will focus on designing of a novel fog gateway using embedded systems along with reconfigurable FPGAs. These gateways can be implemented on fog nodes by applying NFV (Network Function Virtualization). Switches and firewalls can also be virtualized and placed on fog nodes [12].
- This proposed gateway is expected to perform all the necessary functions such as embedded data collection as well as pre-processing of data, communicating over different protocols, scalability to large number of devices and having considerably low power consumption. However, the performance of virtual networked devices is an important aspect while applying NFV in fog computing [12].
- The current research trends also include different communication paradigm like software defined networking (SDN) using fog computing. SDN together with fog computing can help in efficient management of heterogeneous networks. The demands of future vehicular networks applications like connectivity, intelligence, scalability, etc can be effectively solved by using SDN – based fog computing [12].

Conclusion

Fog computing is an emerging area for IOT applications. Fog computing is an intermediate layer between the cloud and end users. In fog-based systems, major part of computing and processing of IOT data is performed at the fog nodes which reduces the response time in case of latency-sensitive applications. In this paper, our objective was to review recent use case scenarios of fog computing in the world so that the functionality and parameters used by these cases could be used for future research directions. This survey discussed about the improvement in performance of these use cases considering different parameters. We also presented the challenges faced by fog computing and the research contributions to handle security and privacy issues in fog computing. Based on our survey, we have highlighted some major issues which are needed to be addressed while integrating fog computing with IOT.

References

- [1] Bonomi, F; Milito, R; Zhu, J; Addepalli, S. Fog computing and its role in the internet of things. In proceedings of First Edition of the MCC Workshop on Mobile Cloud Computing-MCC'12, Helsinki, Finland, 17 August 2012; pp. 13-15.
- [2] Hany F. Atlam, Robert J. Walters and Gary B. Wills; Fog computing and the internet of things: A Review; Big Data and Cognitive Computing; 2018,2,10; doi:10.3390/bdcc2020010.
- [3] Shubha Brata Nath, Harshit Gupta, Sandip Chakraborty, Soumya K Ghosh; A survey of fog computing and communication: Current researches and future directions; IEEE Communication Surveys and Tutorials; April 2018.
- [4] Redowan Mahmud, Ramamohanarao Kotagiri, Rajkumar Buyya; Fog Computing: A Taxonomy, Survey and Future Directions; Springer; Part of the Internet of Things book series (ITTCC); pp 103-130; October 2017.
- [5] Yongxuan Lai, Fan Yang, Lu Zhang and Ziyu Lin; Distributed public vehicle system based on fog nodes and vehicular sensing; IEEE Access Journal; Volume6; DOI: 10.1109/ACCESS.2018.2824319; May 9, 2018.
- [6] Augusto J. V. Neto, ZhongliangZhaho, Joel J. P. C. Rodrigues, Hugo Barros Camboim and Torsten Braun; Fog based crime assistance in smart IOT transportation system; IEEE Access Journal, Special section on cyber-physical-social computing and networking; Volume 6; DOI: 10.1109/ ACCESS.2018.2803439; March 16, 2018.
- [7] Blesson Varghese, Nan Wang, Dimitrios S. Nikolopoulos and Rajkumar Buyya; Feasibility of Fog Computing; arXiv:1701.05451v1 [cs.DC] ; 19Jan 2017.
- [8] Amir M. Rahmani, Tuan Nguyen Gia, BehailuNegash, Arman Anzanpour, Iman Azimi, Mingzhe Jiang and PasiLiljeberg; Exploiting Smart e-Health Gateways at the edge of Healthcare Internet-of-Things: A Fog Computing Approach; ELSEVIER, Future Generation Computer Systems 78 (2018); pp. 641-658; DOI: 10.1016/j.future.2017.02.014; February 10, 2017.
- [9] Mithun Mukherjee, Rakesh Matam, Lei Shu, LeandrosMaglaras, Mohamed Amine Ferrag, Nikumani Chaudhury, Vikas Kumar; Security and Privacy in Fog Computing: Challenges; IEEE Access Journal; Volume5; DOI: 10.1109/ACCESS.2017.2749422 ; pp:19293 – 19304, 06 September 2017.
- [10] Abebe AbeshuDirol, Naveen Chilamkurti and Yunyoung Nam; Analysis of Lightweight Encryption Scheme for Fog-To-Things Communication; IEEE Access Journal, Special section on real-time Edge Analytics for Big Data in Internet of Things; Volume 6; DOI: 10.1109/ACCESS.2018.2822822; June 5, 2018.
- [11] Thanh Dat Dang and Doan Hoang; A Data Protection Model for Fog Computing; IEEE Conference; 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC); 2017 IEEE; pp. 32-38.
- [12] Pengfei Hu, SahraouiDhelim, Huansheng Ning and Tie Qiu; Survey on Fog Computing: Architecture, Key Technologies, Applications and Open Issues; ELSEVIER Journal of Network and Computer Applications 98 (2017); DOI: 10.1016/j.jnca.2017.09.002; September 12, 2017