ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 9, Issue, 4(G), pp. 26022-26025, April, 2018

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

MOVING FROM CLOUD TO FOG: SCENARIOS AND SECURITY CONCERNS

Aradhana *

Department of Computer Science and Applications, Guru Gobind Singh College for Women, Chandigarh, India

DOI: http://dx.doi.org/10.24327/ijrsr.2018.0904.1976

ARTICLE INFO

Article History:

Received 8th January, 2018
Received in revised form 21st February, 2018
Accepted 05th March, 2018
Published online 28th April, 2018

Key Words:

Fog Computing, Cloud Computing, Internet of Things (IoT), Privacy, Security

ABSTRACT

With the increasing needs of on demand availability of data and ubiquitous access to shared pools of system resources cloud computing has emerged as a successful paradigm to meet dynamic user demands. In addition to this the rise in usage of mobile devices, Internet of Things has gained popularity due to its huge potential to connect physical devices to the internet and thus enabling each device to share data with the surrounding devices and virtualized technologies in real time environment. Consequently skyrocketing data access needs require a new paradigm that can provide wide spread geographical distribution, location awareness and low latency. As a result Fog Computing has been recently introduced to provide real time analytics in heterogeneous environments. This paper gives a close look on FC paradigm and investigates its applications in real life. We discuss security and privacy issues in FC and state of the art of Fog Computing.

INTRODUCTION

The increased use of a "pay-as-you-go" cloud computing model has reduced the overall cost of users owning and managing private data centres. This has given rise to increasing user demand for computing, networking, and storage resources as well as the need for efficient management and access to highly virtualized resources. However, current computing models cannot account for and handle the huge data load, and thus require an innovative approach with the capability of communicating more closely with physical devices by extending cloud computing services to the edge of the network (Flavio *et al,* 2012). As a result, fog computing also termed edge-of-network has been recently introduced by CISCO with the vision to enable applications on billions of devices, already connected in the Internet of Things (IoT), to run directly at the network edge (Bonomi *et al,*2011). Fog Computing has all major characteristics of Cloud computing like storage, networking and processing or computation (Stojmenovic *et al,* 2014). In addition, FC supports mobility, location awareness and latency sensitive services. It enables computing directly at the edge of the network so that the data can be shared instantaneously between the physical devices. Major real time applications of FC include Visual security, Wireless Sensors and Actuator Networks, VANETs, Smart Grids and Smart Cities, Healthcare and Mobile computing.

According to the CISCO estimate, the average of connected devices per person will reach 6.58 by 2020 (Luan *et al,* 2015). This prediction is demanding to improve and optimize the services provision by internet. With the process of increasing efficiency and capacity of network as well as cloud and fog computing, it is necessary to keep check and balance on the ever-increasing issues and problems like security, privacy, energy efficiency, resource management and environmental hazards.

Fog Computing Overview

Fog computing is a highly virtualized platform that provides computation, storage and networking to the end users connected to each other in heterogeneous environment. It can be considered as an extension of cloud computing. Its distinguished features such as edge location, location awareness and low latency makes it work more effectively with the internet of things. FC finds its applications in real time analytics such as transportation, industrial automation and network of sensors and actuators. Figure 1 shows how FC can be viewed as virtual platform having close connection of internet of things with fog and how they are interlinked with the cloud.

Corresponding author:* **Aradhana
Department of Computer Science and Applications, Guru Gobind Singh College for Women, Chandigarh, India

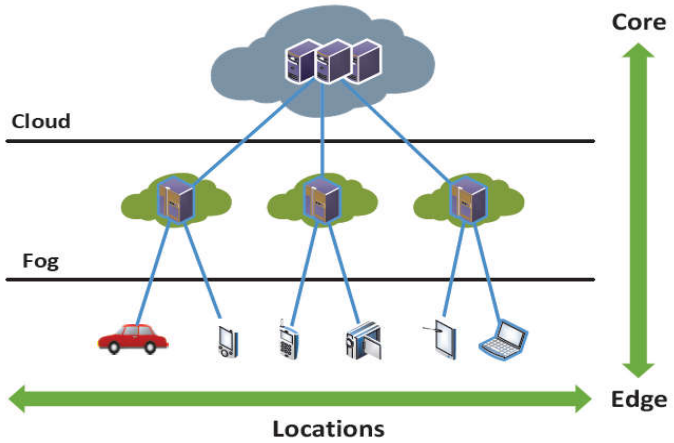

Figure 1 Fog between Edge and Cloud (Stojmenovic *et al,* 2014)

Application Scenarios

In this section we elaborate various real time scenarios of interest in which Fog computing plays a major role:

Smart Grid

Smart Grid illustrates a fruitful interplay between the Fog and the Cloud. As shown in (Fig 2) fog collectors at the edge ingest the data generated by grid sensors and devices. The first layer of the Fog collects and processes the data, and issues control commands to the actuators. It also filters the data to be consumed locally, and sends the rest to the higher layers. The second and third layers deal with visualization and reporting interactions. Fog supports ephemeral storage at the lowest layer to semi-permanent storage at the highest layer. Global coverage is provided by the Cloud with business intelligence analytics (Flavio *et al,* 2012).

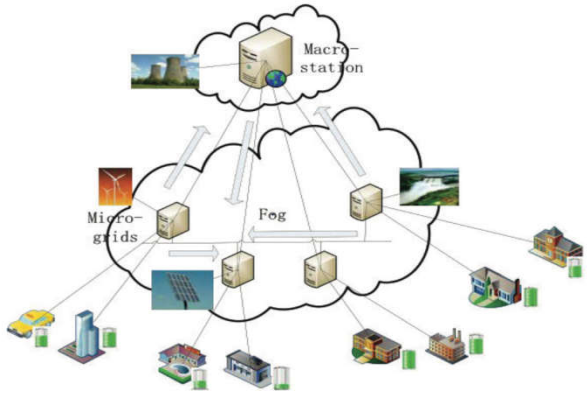

Figure 2 Fog Computing for Smart Grids

Vehicular Ad-hoc networks (VANETs)

Fog computing as a new architecture is a good candidate for VANETs to meet the requirements, such as quick reaction to underlying device, reduce the burden on cloud, analysis real-time data stream with cloud and etc. Smart lights serve as fog devices and synchronize to send warning signals to the approaching vehicles. The interactions between vehicle and access points are enhanced with WiFi, 3G, road side units and smart traffic lights. A highly distributed collector of traffic data over an extended geographically data ensures an acceptable degree of consistency (Bonomi *et al, 2012)*.

The situation of traffic lights can be changed by vehicles pass by as shown in (Fig 3). For example, an ambulance flashing lights can be sensed by video camera automatically. And then, smart street lights interact with the right condition. Neighbouring smart lights serving as fog devices coordinate to create green traffic wave and send warning signals to approaching vehicles (Stojmenovic *et al,* 2014).

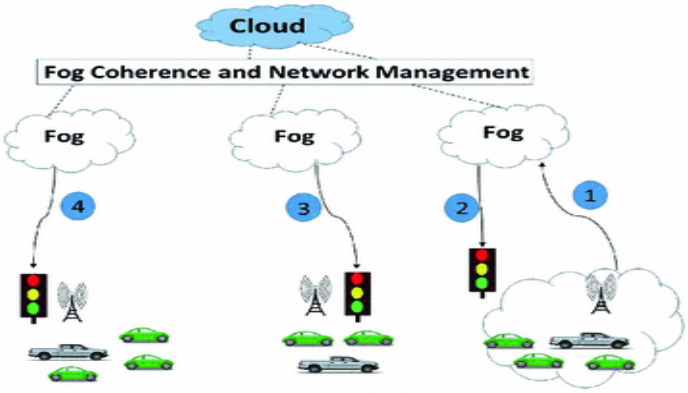

Figure 3 Fog Computing for VANET

Healthcare

Fog Computing can play a major role in bridging the gap between sensors and analytics in health informatics. With fog computing, the location can be dynamic and depend on the current context, environment and application requirements. New sensors can be added to the existing infrastructure. For example heart rate monitoring system needs dedicated infrastructure. Fog computing can also serve as compatibility layer to translate between various standards. Patient mobility can be managed more gradually especially when patients are about to leave the highly instrumented infrastructure of a hospital. Fog computing will also enable entirely new applications: By adding higher levels of autonomy and intelligence at the edge, fog computing will provide latency and response time improvements, as well as energy savings for wearable and low-cost devices, while performing complex tasks. The next generation of healthcare devices will replace costly and complex devices, without resorting to simple algorithms with limited accuracy. These devices will be enabled by fog computing, ultimately leading to the "Internet of Healthcare Things" (Alexander *et al*, 2017).

Mobile Computing Systems

Fog computing highly organizes computing and communication facilities for mobile users. Fog computing explores the predictable service demand patterns of mobile users and typically provides desirable localized services accordingly. With low latency and short distance local connections Fog computing can provide mobile users with demanded services. This significantly improves Quality of Service (QoS) provided to the mobile users and thus saves bandwidth cost and energy consumptions. Fog computing enables the convergence of cloud based Internet and mobile computing.

Security Concerns In Fog Computing

Fog computing has been proved very useful in many real time and near real time applications due to its features such as edge location, location awareness and low latency. But this bliss comes with many security issues which have gained attraction of many researchers. Few of them are discussed below.

Authorization and Authentication

Authentication and authorization are essential parts of basic security processes and are sorely needed in Fog Computing as it is open to community at large. It becomes very important to identity each fog node connected to the network and verify whether it is an authentic one or not. After authentication it is necessary to define set of privileges as each node may have a different set of reasons to join the network and similarly may have different set of capabilities and functions.

The work (Law *et al*, 2013) elaborated public key infrastructure (PKI) based solutions which involve multicast authentication. Some authentication techniques using Diffie-Hellman key exchange have been discussed in (Fadlullah *et al*, 2011).

Network Security

As network is the connecting bridge between the fog devices in this heterogeneous computing platform, it becomes essential to prevent and monitor unauthorized access, misuse, modification or denial of network resources. An effected network not only damages the proper working of that particular network but also can spread the malicious programs and threats to the connected parties. Hence secure network ensure the security of the fog nodes and other connected devices.

Author in (Qin *et al*, 2014) provides a security mechanism for preserving privacy of end users over a radio network. The proposed technique uses commitment scheme along with zero-knowledge proof to preserve the privacy of end user and to protect the data flow over the radio network.

Man-in-the-Middle Attack

Man-in-the-middle attack has potential to become a typical attack in Fog computing. This type of attack will consume only a small amount of resources in Fog devices, such as negligible CPU utilization and memory consumption (Stojmenovic *et al,* 2014). Therefore, traditional anomaly detection methods can hardly expose man-in-the-middle attack without noticeable features of this attack collected from the Fog.

The work presented in (Stojmenovic *et al,* 2014) as shown in (Fig 4) implemented an attack environment by compromising the gateway and inserting malicious code in the compromised system and analyzed using stealth test that in the real world, it is difficult to protect Fog devices from compromise as the places for the deployment.

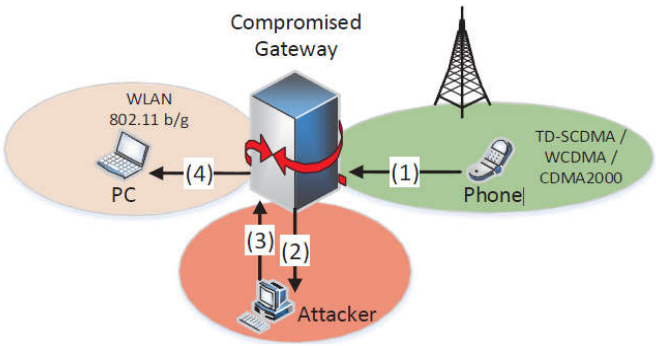

Figure 4 Hijacked communication in Fog (Stojmenovic *et al,* 2014)

Intrusion Detection system

An intrusion detection system monitors the rate and characteristics of Internet attacks on a computer network and filters attack alerts based upon various rates and frequencies of the attacks. The intrusion detection system monitors attacks on other hosts and determines if the attacks are random or general attacks or attacks directed towards a specific computer network and generates a corresponding signal. The intrusion detections system also tests a computer network's vulnerability to attacks detected on the other monitored hosts (Rowland, 2002).

As FC is a distributed system, so we need IDS both at local and global level. The local level IDS ensures the safety of local infrastructure whereas, global level IDS ensures the security of core infrastructure as well as it has to keep an eye to detect any malicious activity going on in the local infrastructure that is beyond the strength of local IDS (Stojmenovic *et al,* 2014).

Network Monitoring and Intrusion Detection System to watch the traffic, Traffic Isolation and Prioritization system can be used to prevent attack by shared resources, Network resource access control system helps to get access control on SDN (Open Control), Network Sharing System can help the fog node router to be open to guests considering the security issues as well.

Privacy

Privacy is one of the most important concerns of security which include data as well as location privacy. It is one of the most challenging security issues in fog computing due data delivery at the edges. So it becomes very easy for the attacker to collect and steal important information.

The concept of fog computing at user end can provide rich information about the network, its traffic information, its client information which can be used for optimization. The location information may become dangerous for both side - client end as well as fog nodes. One can easily get the location of client end if it's a fog node and of fog node if it's a client end.

The author in (Kanuparthi *et al*, 2013) proposed hardware and embedded security mechanisms to tackle with the issues of data access control, authorization and authentication, trust and privacy. Author proposed integrated sensing with PUF technology to ensure controlled data access and authentication. He proposed a lightweight cryptography technique for ensuring privacy. In (Chen *et al*, 2014) the author proposed a Trusted Platform Module (TPM) and named it as cTPM. His proposed module consisting of an extra root key that is shared between the end device and the cloud. The cloud has the authority to access only those information and data, which is protected by the given root key. The rest of the data could not be accessed by the cloud. In this way the authentication and privacy of each end node is imposed as a security measure in (Abbasi *et al*, 2017). Author in (Dsouza *et al*, 2014) proposed a policy based management system for FC in order to make it secure and efficient. A preventive approach for data and location privacy has been proposed by authors in (Praveen *et al*, 2016) which makes use a similar decoy technique with additional benefits. The authors suggested to make fake nodes at every fog connection as well as fake documents and divert the attacker towards the path of fake fog node making it look like legitimate and original.

CONCLUSION

This paper discusses the tremendous potential of Fog computing for Internet of things which motivates us to move one step ahead of cloud. Many real time application scenarios of FC have also been covered. We have provided in depth detail of various security issues arising due to sharing of data on the edges and state of the art work done by various researchers in the same domain. Based on the work of this paper some innovations may be inspired in the future to handle computation, storage and networking.

References

Bonomi, F., Milito, R., Zhu, J. and Addepalli, S. Fog computing and its role in the Internet of things. In Proceedings of the first edition of the MCC workshop on Mobile cloud computing, pages 13-16. ACM, 2012.

Bonomi, F. Connected vehicles, the internet of things, and fog computing, in The Eighth ACM International Workshop on Vehicular Inter-Networking (VANET*)*, Las Vegas, USA, 2011.

Stojmenovic, I. and Wen,S. The Fog Computing Paradigm: Scenarios and Security Issues, Proc. 2014 Fed. Conf. Comput. *Sci. Inf. Syst.*, vol. 2, pp. 1-8, 2014.

Luan,T. H., Gao L., Li, Z., Xiang,Y. and Sun,L. Fog computing: Focusing on mobile users at the edge, arXiv:1502.01815, pp. 1-7, 2015.

Bonomi, F. Milito, R., Zhu, J., *et al*. Fog computing and its role in the Internet of things. Proceedings of the ACM Workshop on Mobile Cloud Computing (MCC'12), Aug 17, 2012, Helsinki, Finland. New York, NY, USA: ACM, 2012: 13−16.

Kraemer, F. A., B, A.E., Tamkittikhun, N. and Palma,D. Fog computing in healthcare-a review and discussion, IEEE Access, 2017.

Law, Y.W., Palaniswami, M., Kounga, G. and Lo, A. Wake: Key management scheme for wide-area measurement systems in smart grid, Communications Magazine*, IEEE*, vol. 51, no. 1, pp. 34-41, January 2013.

Fadlullah, Z., Fouda, M., Kato, N., Takeuchi ,A., Iwasaki, N., and Nozaki,Y. Toward intelligent machine-to-machine communications in smart grid,Communications Magazine*, IEEE*, vol. 49, no. 4, pp. 60-65, April 2011.

Qin, Z., Yi, S., Li, Q. and Zamkov, D. Preserving secondary users' privacy in cognitive radio networks, Proc. - IEEE INFOCOM, pp. 772-780, 2014.

Rowland, C.H. US Patent 6,405,318, 2002.

Zaheer, B.Z., Shah, M.A. Fog Computing: Security Issues, Solutions and Robust Practices Proceedings of the 23rd International Conference on Automation & Computing, University of Hudders field, Hudders field, UK, 7-8September 2017.

Kumar, P., Zaidi, N. and Choudhury, T. Fog computing: Common security issues and proposed countermeasures, in Proc. Int. Conf. System Modeling Adv. Res. Trends (SMART), Nov. 2016, pp. 311-315.

Kanuparthi, A., Karri, R., and Addepalli, S. Hardware and embedded security in the context of internet of things, Proc. 2013 ACM Work. Secur. Priv. dependability cyber Veh. -*CyCAR '13*, pp. 61-64, 2013.

Chen, C., Raj, H., Saroiu, S., Nsdi, I. and Wolman, A. cTPM : A Cloud TPM for Cross-Device Trusted Applications, 11th USENIX Conf. Networked Syst. Des. Implement., vol. 8, pp. 187-201, 2014.

Dsouza, C., Ahn, G. J. and Taguinod, M. Policy-driven security management for fog computing: Preliminary framework and a case study, Proc. 2014 IEEE 15th Int. Conf. Inf. Reuse Integr. IEEE IRI 2014, pp. 16-23, 2014.

How to cite this article:

Aradhana.2018, Moving From Cloud To Fog: Scenarios And Security Concerns. *Int J Recent Sci Res.* 9(4), pp. 26022-26025. DOI: http://dx.doi.org/10.24327/ijrsr.2018.0904.1976

****