AN OVERVIEW OF CURRENT SECURITY THREATS AND EXISTING SOLUTIONS IN FOG COMPUTING

NEDA ABDULLAH BUGSHAN
Computer Science Department, Community College,
Imam Abdul rahman Bin Faisal University, P. O. Box 1982, Dammam, Saudi Arabia
nabugshan@iau.edu.sa;

Manuscript History
Number: **IRJCS/RS/Vol.06/Issue04/APCS10086**
Received: 04, April 2019
Final Correction: 10, April 2019
Final Accepted: 18, April 2019
Published: April 2019
Citation: BUGSHAN (2019). An Overview of Current Security Threats and Existing Solutions in Fog Computing. IRJCS:: International Research Journal of Computer Science, Volume VI, 144-148.
doi://10.26562/IRJCS.2019.APCS10086
Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

Abstract: Due to technology problems with cloud computing and it is unable to fulfill real-time applications requirements such as (low latency, performance, and mobility support) and limited storage and computational power with Internet of Things (IoT) devices, Cisco company proposed a new concept call "Fog computing" or "Fog networking" that extend cloud computing to satisfy customer's needs.. However, fog computing faces some security challenges that inherited from cloud computing in addition to new issues that discovered with using fog services. These security issues need to be addressed with practical solutions to provide successful implementation of Fog System. Information technology Researchers and specialist organizations have proposed many solutions to protect systems from malicious activities like inside and outside network attacks. This paper will provide an overview of existing literature on Fog computing to identify common security threats, the impact of risks on the system, what are the current solutions and the effectiveness of solutions. This paper may help to provide a guide for expert concern on designing, developing, and maintaining Fog systems.

I. INTRODUCTION

Fog Computing is a new technology introduced by Cisco Company in 2014 to extend cloud computing services at the edge of the network. Fog computing aims to reduce latency and improve the efficiency of the network. It facilitates computing, networking and storage services between end-user devices and cloud computing data centres. Due to the fast-growing number of smart devices and applications that connected to cloud computing and consume its services, the new concept called the Internet of Things (IoT) come up to provide more advantages. With the Internet of Things technology, data can be handled efficiently rather than send them to cloud services. In simple words, fog IoT applications will make a smart decision to send data to the best place for processing. If the data is real-time and highly sensitive and need to process as fast as possible, it will send to the nearest fog node (The fog nodes will take different shape such as a router, gateway, switch, and Access Points These fog nodes can collaboratively share storage and computing facilities [1].).But if it can wait for a couple of minutes, it will send to set of fog nodes or cloud for best data analytics.

For example, in a fire detector use case where the alarm is trigger when a sensor detects fire and the respond to an incident must be done as soon as possible to avoid severe damage to the building. Fog computing helps to overcome issues associated with traditional cloud computing (like high latency, security problems, bandwidth and so on) and add more characteristics to current technology [2]:

- Low latency and location awareness: Fog computing supports excellent services at the edge of the network. Promotes geographic distribution: the applications of Fog computing is widely distributed.
- End device mobility
- A capacity for processing a high number of nodes.
- Wireless access.
- Real-time applications: fog computing support real-time interaction to speed service.
- Heterogeneity: Fog computing can support different environment.

Despite all features and characterizes of Fog computing that mentioned above, There are a set of security threats that affect Fog computing performance. Moreover, It inherits some of the issues and problems that affect cloud computing like energy efficiency, resource management and security issues [3]. Most security issues raised in Cloud Computing could be threatened by fog computing. For example [4]:

- Data Breaches.
- Data Loss.
- Account Hijacking.
- Daniel of Service (DOS).
- Distributed Daniel of Service (DDOS).
- Malicious insider.

II. OVERVIEW OF FOG COMPUTING

2.1 FOG COMPUTING DEFINITION

Fog computing is a paradigm that supports computing, storage, control, and networking functions closer to the edge of a network or at data source itself. The basic concept of fog computing is extending cloud services and reduce pressure on cloud servers. Fog Computing makes cloud computing reachable to end users; it provides support for the internet of things (IoT) and many applications that require real-time transactions. Depend on Application that uses fog technology; the size will vary from small single node to a large system[5].To understand the importance of fog computing in a real world, let consider a healthcare sector where data analytics should be done in real time and any delay in transmission even couple of seconds may threaten patients life. Consequently, Fog computing supports efficient, timely manner analytics to provide fast and more precise treatment to patients in the healthcare sector[6]. Real-time experiences are becoming a sign of modern and advanced technology associated with applications that we use in our daily life. For example, if we face a delay or late response with social, chat, and gaming applications, we will search to a competing alternative application like what happened with the popular messaging app Whats App when went down for 4 hours, millions of users switched to Telegram application. Furthermore, the lack of real-time experience for end users in the commercial application could lead to the death for the application, and lack of real-time functionality in industrial use cases lead to real safety issues. Another benefit of Edge computing like Fog Computing is a more fault tolerant, excellent design, which help to reduce the volume of information and complexity in the application architecture [7].

2.2 HOW FOG COMPUTING WORKS

Networks in Fog environment include set of end devices that use to generate and receive data like smart devices (mobile, tablet, phablet, personal computers (Laptop and Desktop)), console games. However, end devices aren't able to perform sophisticated analytics and machine learning tasks so, they need to send data to Cloud server to perform such tasks which are located in a remote location and take time to process data and send it back to clients. Moreover, sharing raw data with the cloud servers over the internet can raise other problems like privacy, security and legal issues, especially when dealing with sensitive data subject to regulations in different countries across the globe. With Fog Technology short-term analytics can perform at the edge.So, The processing can take place in a networking device like a router, switch or gateway, to minimize the amount of data sent to the cloud while the cloud use to perform massive longer-term analytics[5].In fact, Fog computing is not a replacement of Cloud computing; It is considered an extension to the Cloud services.

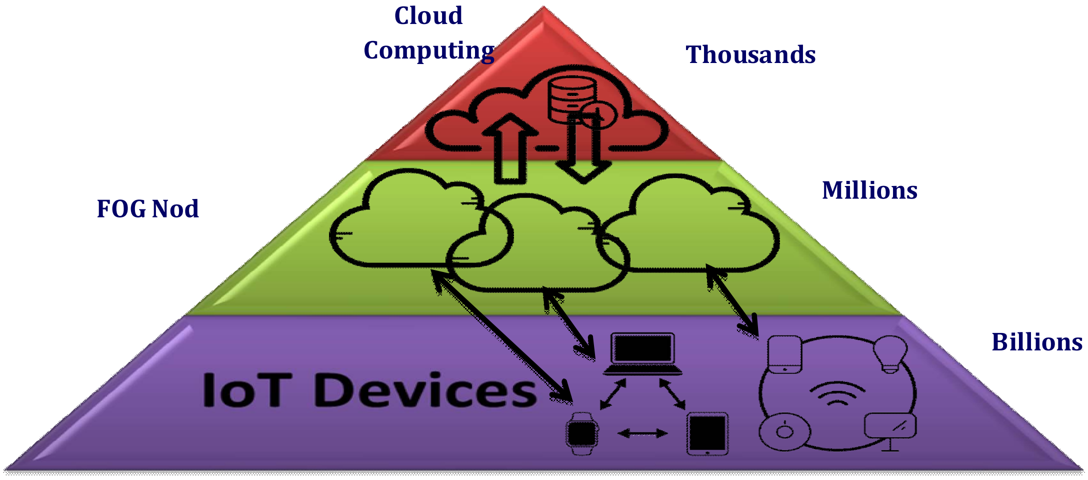

Figure 1: Fog Computing Layers

The figure above illustrates how fog computing works. There are three layers in fog environment: Top layer is Cloud servers, Middle layer is Fog nodes, and the last layer is Smart devise or Internet of Things (IoT) devices. Smart devices or Inter of Things devices will generate data or information and send it to the nearest Fog nodes instead to send data to the cloud to save time. Fog nodes will do further processing that requires less computing power and storage. The Cloud layer will use to manage and analyze massive data that need more computing power and data storage facilities; the cloud is still a better option for operations such as big data management and big data mining.

III. CURRENT SECURITY PROBLEMS AND EXISTING SOLUTIONS

3.1 Authentication and Access Level

Authentication is a process for establishing user identity to gain access to a system. There are two main steps: first, the user needs to identify itself by providing a username or email address; second, the user has to prove that he/she is a legitimate user to use system resources. The access level will determine depending on users privilege (i.e. admin or standard user). There are different methods for authentication:

1. Something you know (i.e. passwords): create a strong password which is a combination of small and capital letters, numbers and special characters.
2. Something you have (i.e. token): use numbers that sent to your smart phone or token device to authenticate yourself for online banking services.
3. Something you are (i.e. fingerprint, facial recognition): is the strongest and hardest method to crack – it's not easy to fabricate a fingerprint or facial recognition.

The nature of Fog Computing allows a wide variety of devices to connect to networks. So, to secure Fog Environment, we need to ensure authorization and authentication are applied well, and each node connected to the network have to be identified as a legitimate node, not an evil node. After verifying the identity of each node, the privileges will assign to each node based on an access level (capabilities and functions) [3].Balfanz etal. [11] have suggested a simple and secure user-friendly solution to the authentication problem in the local ad-hoc wireless network, depending on physical contact for pre-authentication in a location-limited channel. With NFC is possible to identify and authenticate consumables & accessories in IoT devices. Also, it can be used to simplify the authentication process in cloudlet. Furthermore, use biometric-based authentication (i.e. fingerprint authentication, face authentication) in fog computing will help to improve security. Arij et al. [10] introduced a new anonymous and secure authentication scheme in fog-based cloud computing.This method provides mutual authentication between fog servers and fog users with the possibility of roaming between fogs in an anonymous and secure way. Using the AVISPA tool have shown a good improved in security and privacy preservation.

3.2 Network Security& Communication

Network security is a mechanism to protect the usability and integrity of the whole network. Useful security measurement will restrict access to authorized users and prevent malicious users from carrying out any exploits and damage. It helps to minimize threats and stops them from spreading on the network [8]. With fog Computing, communication and networking happen at the end-user device rather than routing all traffic through core networks which help to increase privacy and reduce congestion, but it brings a heavy burden to the network management without easy access for maintenance. To overcome management problem and increase networks scalability, Software Defined Networks (SDN) technology can be adopted. Amir et al. [9]defined a new framework that includes fog nodes integrating with SDNs to improve the resilience of networks. Fog nodes will connect to Open Flow switches to check data packets that pass through the network. Services can then be developed based on the scenarios. Messages are then relayed to the controller to install flow rules accordingly across the network. For testing purposes, the author suggested installing a simple IP sniffer application on Fog nodes. Final Results show the detector application working very well with legitimate traffic and non-legitimate traffic.

3.3 Intrusion Detecting System (IDS)

Intrusion Detection Systems or Prevention Systems, are the application that analyzes and monitor malicious activities in a network, log file, user information to detect intrusion activities and terminate them in case of danger. It can help in sending a warning message against any malicious activity in the network or drop the packets. Intrusion detection techniques are widely used in a cloud system to protect the system from any attacks such as flooding attack, port scanning, distributed denial of service Attack (DOS),and Virtual Machine(VM), and hypervisor attack and it can be deployed on fog node system. However Internet of Things (IoT) devices in Fog computing has limited computing power and resources, so it is difficult to detect the rootkit. Consequently, an attacker can use a hardware virtualization technology to detect vulnerability in victim Operating System to obtain kernel level privilege to do harmful damage to the system [12].

3.4 Confidentiality and Privacy

The terms "Confidentiality" and "Privacy" interchangeably when they apply to the Information Technology world. However, each term has its meanings and their significant roles in its application to data maintenance and data management. Privacy refers to a customer's right to keep his/her information safe from any other third parties. It includes the protection of vulnerable data such as Snapchat, WhatsApp data, and other kinds of demographic data or personal data from being freely exposure over the Internet or sold to third parties. Confidentiality is slightly different from privacy. It always refers to how a supplier or service provider can protect the customer's data. Agreements of Confidentiality are often applied to situations where someone trusted with personal data must safeguard this data from being released [13]. Due to limited resources in the Internet of things (IoT) devices or end devices, the large volume of data will split into a small chunk, and then it sends to nearby fog nodes for further process, and the contents of the data should be analyzed without exposing it to preserve the privacy of data. Thus, light-weight encryption algorithms or privacy-preserving algorithms can be implemented in between the fog and cloud, and homomorphic encryption can be utilized to allow privacy-preserving aggregation at the local gateways without decryption. Another issue with privacy is usage privacy that discloses a lot of information about services used by clients such what time the client uses his devices, what type of service being used. The fog node can easily collect statistics of end-user usage, and the privacy-preserving algorithm cannot be implemented directly in fog computing, due to the lack of a trusted third party. In [14] author suggested that the fog client creates dummy tasks and offloads them to multiple fog nodes, to hide real tasks between the dummy ones. However, this solution will waste resources and energy and increase the fog client's payment. Third privacy issues are location privacy because end devices prefer to use nearby nodes depend on a set of metrics like latency, reputation, load balance, etc. So, the fog node can only know the relative location not the exact location of the fog client. In [14] identity obfuscation can help to confuse fog node from knowing client location. There are many ways for identity obfuscation; for example, a trusted third party can use to generate fake ID for each end user.

3.5 Data Storage

Data collected from or distributed to the Internet of Things (IoT) devices are managed and protected by the distributed infrastructure of secure fog nodes. Thus, that data will be better protected than if stored in the user devices and more available than if maintained in remote data centers [15]. However, it is hard to ensure data integrity, since the outsourced data could be lost or incorrectly modified oraltered by unauthorized third parties.

To overcome these issues [14], auditable data storage service has been proposed ,and homomorphic encryption and searchable encryption are combined to provide integrity, confidentiality and variability for the cloud storage system. Privacy-preserving public auditing could be used for data stored in the cloud, which relies on a third-party auditor (TPA), using homomorphic authenticator and random mask technique to protect privacy against TPA. Erasure codes or network coding could be used to deal with data corruption detection and data repair to ensure data storage reliability. The LT code has been proposed to provide less storage cost, much faster data retrieval, and comparable communication cost.

IV. CONCLUSION

Fog Computing is a promising technology that provides many positives points to cloud computing provider and customers. Thus, to get full advantages of Fog system, the current security challenges must be solved in a proper way. This paper reviewed existing security issues and the possible solutions in Fog system such as Authentication and access level, network security and communication, intrusion detection systems, confidentiality and privacy, and secure data storage. However, the security of fog Computing is still in its infant stage; thus, there are many open issues that need to be considered in the near future.

REFERENCES

1. Margaret Rouse, “fog computing (fog networking, fogging),” https://internetofthingsagenda.techtarget.com/definition/fog-computing-fogging
2. M. Mukherjee et al., "Security and Privacy in Fog Computing: Challenges," in IEEE Access, vol. 5, pp. 19293-19304, 2017.
3. B. Z. Abbasi and M. A. Shah, "Fog computing: Security issues, solutions and robust practices" inTwenty Third International Conference on Automation and Computing (ICAC), Huddersfield, 2017, pp. 1-6.
4. Archana Lisbon A, Kavitha R, “A Study on Cloud and Fog Computing Security Issues and Solutions” in International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Issue 03, Volume 4 (March 2017).
5. Crosser, “Fog Computing Explained,” https://crosser.io/blog/posts/2017/january/fog-computing-explained
6. Adesilva, “Fog Computing,” https://www.terminalworks.com/blog/post/2017/05/13/fog-computing
7. Alexander Spotnitz, “Moving the Cloud to the Edge,” https://www.pubnub.com/blog/moving-the-cloud-to-the-edge-computing/
8. Cisco,”What Is Network Security?”, https://www.cisco.com/c/en/us/products/security/what-is-network-security.html
9. Amir Modarresi, James P.G. Sterbenz, "Toward resilient networks with fog computing," Resilient Networks Design and Modeling (RNDM) 2017 9th International Workshop on, pp. 1-7, 2017.
10. A. B. Amor, M. Abid and A. Meddeb, "A Privacy-Preserving Authentication Scheme in an Edge-Fog Environment,”14th International Conference on Computer Systems and Applications (AICCSA), Hammamet, 2017, pp. 1225-1231.
11. Balfanz, D., Smetters, D.K., Stewart, P., Wong, H.C.: Talking to Strangers: Authentication in ad-hoc wireless networks. In: NDSS (2002)
12. K. Lee, D. Kim, D. Ha, U. Rajput and H. Oh, "On security and privacy issues of fog computing supported the Internet of Things environment," 2015 6th International Conference on the Network of the Future (NOF), Montreal, QC, 2015, pp. 1-3.
13. “What is the difference between, confidentiality and security?”, https://www.techopedia.com/7/29803/security/what-is-the-difference-between-privacy-confidentiality-and-security
14. Yi S., Qin Z., Li Q. (2015) Security and Privacy Issues of Fog Computing: A Survey. In: Xu K., Zhu H. (eds) Wireless Algorithms, Systems, and Applications. WASA 2015. Lecture Notes in Computer Science, vol 9204. Springer, Cham.
15. “TOP 5 WAYS FOG COMPUTING CAN MAKE IOT MORE SECURE”, https://www.openfogconsortium.org/top-5-ways-fog-computing-can-make-iot-more-secure/