Fog Computing and Security Issues: A review

Abdullah Aljumah
College of Computer Engineering and Sciences
Prince Sattam Bin Abdulaziz University, Saudi Arabia
(of Affiliation)
Saudi Arabia
aljumah@psau.edu.sa

Tariq Ahamed Ahanger
College of Computer Engineering and Sciences
Prince Sattam Bin Abdulaziz University, Saudi Arabia
(of Affiliation)
Saudi Arabia
t.ahanger@psau.edu.sa

***Abstract*— The paradigm of fog computing has set new trends and heights in the modern world networking and have overcome the major technical complexities of cloud computing. It is not a replacement of cloud computing technology but it just adds feasible advanced characteristics to existing cloud computing paradigm.fog computing not only provide storage, networking and computing services but also provide a platform for IoT (internet of things). However, the fog computing technology also arise the threat to privacy and security of the data and services. The existing security and privacy mechanisms of the cloud computing cannot be applied to the fog computing directly due to its basic characteristics of large-scale geo-distribution, mobility and heterogeneity. This article provides an overview of the present existing issues and challenges in fog computing.**

Keywords*— *Fog Computing, Cloud Computing, Security, DOS, IDS

I. INTRODUCTION

The concept of fog computing was introduced by CISCO in 2010 to bring the methodical arrangement of computation, storage and network resources between regular clouds and the end points [1]. It is an add-on of regular cloud computing technology towards the edge of the network from the core of paradigm. The basic framework is similar to cloud computing but its lower layers of the architecture have special components that are sensitive to rare time response and with this characteristic feature can control and enhance health care, traffic, parking etc. the concept of fog computing is introduced to deal with limitation of cloud computing and support internet of thing [2]. It also supports virtualizations [3]. Fog cannot exist in standalone approach as it is a add-on of cloud, therefore it exists with the existence of cloud unlike the other technologies like MEC and cloudlet [4]. The interaction between fog and cloud has gathered special attention. Fog computing also offers more flexibility to the overall technology due to its n-tier architecture. The three level architecture of fog is shown in figure 1, which includes cloud, fog and end user.

The fog layers can be devised by single or multiple fog domains, administered by single of multiple providers [5]. The fog domains are created by various fog nodes which includes computers, smart phones, edge routers, set-top boxes, gateways, switches etc. the end user layer is created by two sequential domains that is end user devices and IoT devices [6]. One important fact about these two domains is that one of the two domains may not be present in the layer [7].

Fog computing can resolve many vital issues of cloud computing which includes data security, mobility, latency, heterogeneity and bandwidth. The fog nodes are connected to dedicated fog servers which stores rare data in volatile manner [8].

II. SECURITY ISSUES IN FOG COMPUTING

Cloud computing paradigm is vulnerable to many security threats because of its computing framework and centralized data storage. Its security has emerged as crucial issues which restricts its development. On the other hand its extensive version fog is considered as more secure architecture and the reasons for this include the threats as shown in figure 2

1. The data that is collected is momentarily stored and evaluated on local fog nodes nearest to data source, thus decreasing the dependency on the internet. This storing, exchanging and analyzing the data locally mikes it hard for network attackers to gain access to the data.

2- There is no real time exchange of information between the cloud and the devices, thus, it becomes very difficult for eavesdrop attackers to perceive the personal data of any user.

Since fog computing inherits many features of cloud computing so does it inherits risks also. It cannot be considered fully secure. Following are the security threats in fog computing that may be exploited by the attackers:

978-1-5386-1934-6/18/$31.00 ©2018 IEEE

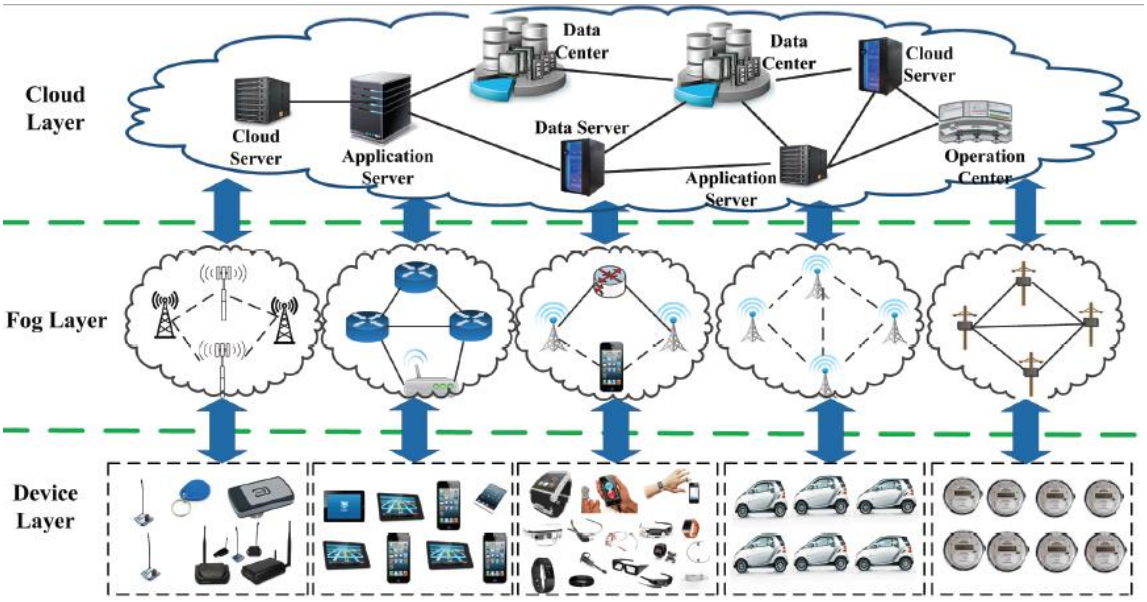

Figure 1 Three level architecture of fog

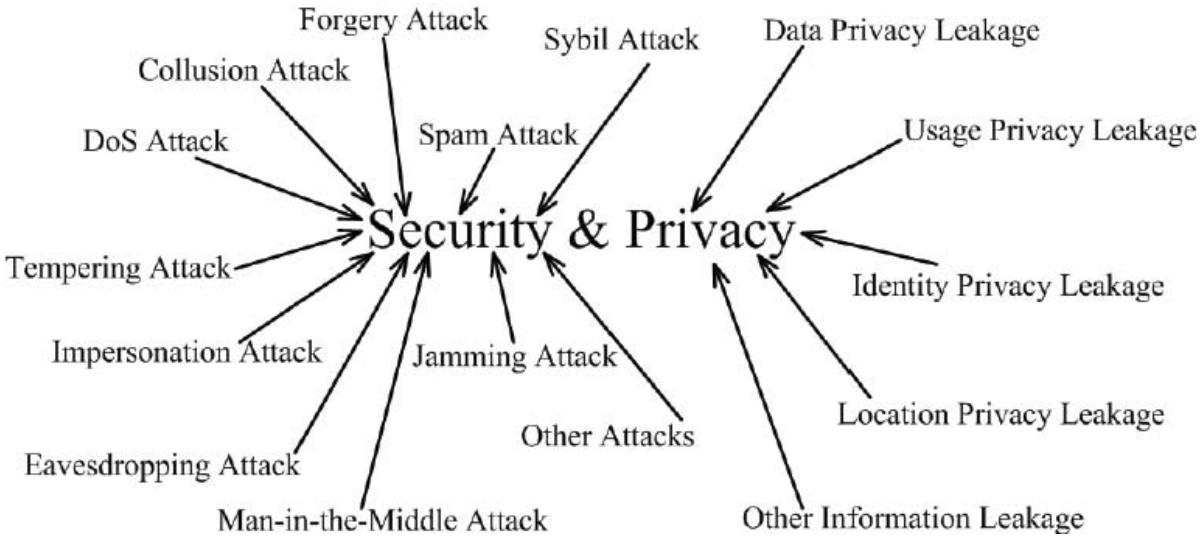

Figure 2: Security threats in Fog Computing

A- Forgery: the network attackers imitate their identities to deceive other entities by generating fake information. It can also damage the network performance by consuming energy, storage and bandwidth due to the fake data packet.

B- Tampering: in order to degrade and disrupt the performance and efficiency of fog computing, network attackers mischievously either modify or delays or drops the data that is being transmitted. Most of the time, this kind of attack is arduous to detect because the user's mobility and the condition of wireless network may cause delay and failure in the transmission.

C- Spam: unwanted data including fake data collected form users, redundant values and information, created and flooded by attackers. Spam results in consumption of vital network resources, privacy exposure and misleading contacts.

D- Sybil: the network criminals use fake name and identities to control the fog computing effectiveness and convert the genuine nodes into compromised nodes. The ruthless effect is that it generates fake crowdsensing reports as the results prepared by these reports are not worth trusting. In addition to this, these attackers can expose the personal information of a legitimate user.

E- Jamming: a network attacker floods a large amount of data packets to jam or consume the transmission channels or its resources in order to restrict the genuine user from having an efficient and reliable network access.

F-Eavesdropping: the attacker gets the control over transmission channel to read or listen the transmission contents without the users' consent. In case the data encryption technique is not efficient then this attack is very affective.

G- Denial of Service: a network attacker sends fake data towards fog nodes and floods them with large number of fake requests to make them unavailable for their legitimate users. These intrusion attacks consume network resources like bandwidth, battery, time thus degrading the performance of fog as the fog resources are limited.

H- Collusion: two or more groups collude cooperatively to trick, cheat or mislead the genuine groups or acquire legal advantages. To increase the attack strength two or more groups can collude to attack a group of IoT nodes or fog nodes or IoT nodes with clouds or fog nodes with IoT nodes.

I- Man-in-the-Middle: a network attacker creates a temporary scenario to stand in between the communicating nodes to relay their communication (data exchange) or modify this communication data without disclosing this to the users as they feel they are exchanging the data with each other directly.

J- Impersonation: a network attacker behaves like a genuine server and offers fake or malicious service to the user by creating an impression of being genuine fog nodes or servers.

Privacy in many means is a serious issue in fog computing as users data is collected, processed, transmitted and shared over fog nodes. None of the users want their data or their privacy exposed but disclosure of privacy under threats or attacks is oblivious. The user's privacy includes the following four aspects:

A- Identity Privacy: a user identity includes the basic attributes of an entity i.e. name, mobile number, home address, visa id, license id and these identities are vulnerable to get exposed for getting authentication of fog nodes by providing all this information.

B- Data Privacy: while communicating on fog nodes the user data may get exposed to an untrusted party. By examining this data, different types of vital information can be obtained e.g. users' address, preferences, and political ideology. For instance, an online voting can expose the user's political preference.

C- Usage privacy: the usage privacy normally means the pattern or order with which the user uses the services of the fog. For instance, the smart meter reading may reveal the users sleeping time or the time when they are not home, thus violating the privacy of the user.

D- Location privacy: in the modern world of technology, most of the mobile applications use users current or saved location. Thus in order to enjoy internet services (including navigation, location based service) the users have to sacrifice the location privacy. But the location privacy is extremely important to be kept secured as it can be used by the attackers to determine the trajectory of the user.

CONCLUSION

Security and privacy are the major issues and are dealt efficiently in cloud computing but most of the existing technologies do not suit the fog computing due to the distinctive features of both along with along with vast range of fog devices. In addition to this new security and privacy concerns are to be faced for the first time as they were not present in cloud computing paradigm. This paper presents an overview of security and privacy issues in fog computing. The focal purpose of this study is to summarize the privacy and security issues in fog computing .

ACKNOWLEDGMENT

This research was conducted at Prince Sattam bin Abdulaziz University, Alkharj, Saudi Arabia during the academic year 2017

REFERENCES

[1] Chiang, M., Ha, S., Chih-Lin, I., Risso, F. and Zhang, T., 2017. Fog Computing and Networking: Part 1 [Guest editorial]. IEEE Communications Magazine, 55(4), pp.16-17.

[2] Roca, D., Milito, R., Nemirovsky, M. and Valero, M., 2018. Tackling IoT Ultra Large Scale Systems: Fog Computing in Support of Hierarchical Emergent Behaviors. In Fog Computing in the Internet of Things (pp. 33-48). Springer International Publishing.

[3] Chang, C., Srirama, S.N. and Buyya, R., 2017. Indie Fog: An Efficient Fog-Computing Infrastructure for the Internet of Things. Computer, 50(9), pp.92-98.

[4] Alonso-Monsalve, S., García-Carballeira, F. and Calderón, A., 2017, May. Fog computing through public-resource computing and storage. In Fog and Mobile Edge Computing (FMEC), 2017 Second International Conference on (pp. 81-87). IEEE.

[5] Kang, J., Yu, R., Huang, X. and Zhang, Y., 2017. Privacy-Preserved Pseudonym Scheme for Fog Computing Supported Internet of Vehicles. IEEE Transactions on Intelligent Transportation Systems.

[6] Dang, T.D. and Hoang, D., 2017, May. A data protection model for fog computing. In Fog and Mobile Edge Computing (FMEC), 2017 Second International Conference on (pp. 32-38). IEEE.

[7] Dastjerdi, A.V. and Buyya, R., 2016. Fog computing: Helping the Internet of Things realize its potential. Computer, 49(8), pp.112-116.

[8] Mouradian, C., Naboulsi, D., Yangui, S., Glitho, R.H., Morrow, M.J. and Polakos, P.A., 2017. A Comprehensive Survey on Fog Computing: State-of-the-art and Research Challenges. IEEE Communications Surveys & Tutorials.