On Security and Privacy Issues of Fog Computing supported Internet of Things Environment

Kanghyo Lee*, Donghyun Kim†, Dongsoo Ha*, Ubaidullah Rajput*, Heekuck Oh*§,
* Department of Computer Science and Engineering, Hanyang University, ERICA Campus, South Korea
E-mail: {kanghyo.lee, hds, ubaidullah, hkoh}@hanyang.ac.kr
† Department of Mathematics and Physics, North Carolina Central University, Durham, NC 27707, USA
E-mail: donghyun.kim@nccu.edu
§ Corresponding Author.

Abstract—**Recently, the concept of Internet of Things (IoT) is attracting much attention due to the huge potential. IoT uses the Internet as a key infrastructure to interconnect numerous geographically diversified IoT nodes which usually have scare resources, and therefore cloud is used as a key back-end supporting infrastructure. In the literature, the collection of the IoT nodes and the cloud is collectively called as an IoT cloud. Unfortunately, the IoT cloud suffers from various drawbacks such as huge network latency as the volume of data which is being processed within the system increases. To alleviate this issue, the concept of *fog computing* is introduced, in which fog-like intermediate computing buffers are located between the IoT nodes and the cloud infrastructure to locally process a significant amount of regional data. Compared to the original IoT cloud, the communication latency as well as the overhead at the back-end cloud infrastructure could be significantly reduced in the fog computing supported IoT cloud, which we will refer as IoT fog. Consequently, several valuable services, which were difficult to be delivered by the traditional IoT cloud, can be effectively offered by the IoT fog. In this paper, however, we argue that the adoption of IoT fog introduces several unique security threats. We first discuss the concept of the IoT fog as well as the existing security measures, which might be useful to secure IoT fog. Then, we explore potential threats to IoT fog.**

I. Introduction

Thanks to the recent advances in the embedded and networking technologies, the concept of *Internet of Things (IoT)*, which is a collective network of various computing objects namely IoT nodes, has arisen. While most IoT nodes such as a smart watch have only limited resources, they tend to have a networking capability as well as both audio and visual sensors. It is not difficult to imagine that in the near future, IoT will have a significant impact on our daily lives. However, to unleash the full potential of the IoT, one significant challenge to overcome is the fact that each IoT device is with a limited resource. In particular, most IoT devices are battery-operated as well as they are constraint in size.

In a cloud supported IoT architecture, which is commonly referred as IoT cloud, IoT nodes need to exchange messages with the back-end cloud frequently. Unfortunately, as the size of IoT cloud grows, the network latency increases, which is apparently a critical issue to time sensitive IoT cloud applications. Furthermore, the overheads on the back-end cloud will grow and the bottleneck nodes on the path between the IoT nodes to the cloud will be more congested. This means that the IoT cloud may not be proper to run large-scale latency-intolerant applications. To address this issue, the new concept of fog computing has been introduced [1]. In essence, fog computing is a hierarchically structured cloud computing in which additional computing buffers, which process the data between the cloud and the terminal IoT devices, are introduced. In the traditional IoT cloud, the messages from each IoT device have been directly destined to the back-end cloud. In contrast, in case of fog computing powered IoT cloud, which we name by IoT fog during the rest of this paper, the messages from the terminal IoT nodes could be processed by intermediate fog-like computing servers, and the overhead on the cloud as well as the congestion on the bottleneck nodes will be leased.

It is expected that in the near future, IoT fog will collect and process deeply personal information. As a result, without proper security and privacy-preserving mechanisms, IoT fog cannot be adopted despite of its usefulness. Clearly, IoT fog will suffer from the classical security and privacy issues which are inherited from IoT cloud. In addition, it suffers from unique threats due to the adoption of fog infrastructure such as node-compromised attack. Unfortunately, there have been no serious study conducted on this issue. This paper aims to fill this void by introducing the concept of IoT fog (Section II), by discussing about the existing security and privacy-preserving measures for IoT cloud (Section III), which might be useful to protect IoT fog, and the security and privacy issues in IoT fog (Section IV). In addition, we also discuss about future research directions in Section V.

II. Overview of Fog Computing

In this chapter, we describe fog computing environment and the limitations of cloud as a back-end infrastructure for IoT environments. Based on the perspective of Cisco, fog computing is considered as an extension of the cloud computing paradigm, but is a more highly virtualized platform that provides computation, storage, and networking services between end IoT devices and back-end cloud servers [2]. Because a fog client usually off loads its tasks to the nearest fog node, fog nodes are able to provide location-awareness and low latency to users. The fog paradigm is well positioned for real time big data analysis, supports densely distributed data

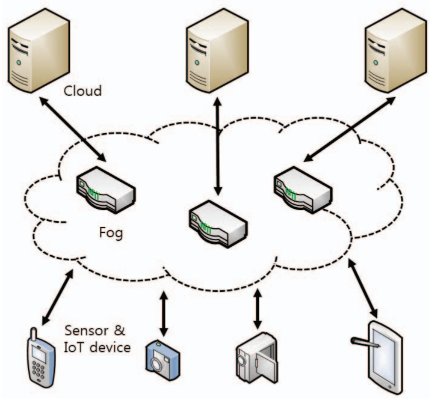

Fig. 1: The hierarchical fog computing architecture

collection points and provides advantages in entertainment, advertising, personal computing and other applications. The hierarchical fog computing architecture is shown in Figure 1.

Conceptually, fog computing consists of 3 main components, (a) IoT nodes, (b) fog nodes, and (c) back-end cloud. The IoT nodes are with various sensors and generate local data. The fog nodes are devices with more computing power than usual IoT nodes. The IoT nodes are connected to the fog nodes through a short-range communications such as Wi-Fi, ZigBee, Bluetooth. As it is expensive and time-consuming to send all of data from terminal IoT devices to the back-end cloud through the high latency network (i.e. Internet), fog layer is positioned nearby IoT devices and autonomously processes data in real time nearby the network edge. Because fog nodes have more memory or storage ability for computing, it is immediately possible to process a significant amount of data from IoT nodes. Those data and computation which needs more computing power are sent to the back-end cloud from the fog nodes through high-speed wire or wireless communication. Situation-awareness information, contextual information is generated by analyzing data collected from devices. Analyzing data based on the situational information can provide more specialized services to users. It can predict possible future situation that helps user make decisions.

III. Relevant Security Technologies

This section examines the state-of-art IoT security technologies, which are possibly useful to secure fog computing environment.

A. *Security Technologies for IoT Network*

The concept of fog computing involves the communication among a number of IoT devices, fog nodes, and back-end clouds. Therefore, it is important to make the communications secure. However, due to the salient features of fog computing, existing solutions for secure communications cannot be applied directly. A node in fog cloud environment is a single object that is represented as the personal, site, or IoT device. Those do not represent the information flow that is reproduced and passed. The wrong information is spread by the authenticated malicious users, or devices. The wrong information causes big problems and leads to a lot of damage. In addition, it is difficult to properly indicate the information flow between fog nodes connected to those things. Although some algorithms establish authentication and securely communicate with things in IoT fog environment, it requires to develop new algorithms.

B. *Security Technologies for Fog Node*

Due to the uniqueness of the fog node, a multi-OS environment is essential. Therefore virtualization technology is basically prevented from access of other operating systems, but if there is a problem in kernal mode, it does not prevent. In fog computing environment, much of the information is gathered into a fog node. If wrong information is spread by exploiting vulnerability, we expect that it is in a big problem. It requires to a dynamic analysis technique to monitor fog node in real time. Typically, the performance overhead of dynamic analysis is high. Therefore, it is difficult to apply to a OS that has a relatively low computational power and maintains a real-time processing.

C. *Security Technologies for IoT Node*

IoT nodes are distributed and work at edge network. The IoT nodes will face many threats that usually do not appear in well-managed cloud environment. In IoT fog environment, various fog nodes provide services that is based on the information collected from the IoT nodes. When some IoT nodes are out of order or provides wrong information, it can affect people. Attacker has many chances to compromise various devices with sensors. Status information that is analyzed from fog nodes involves being of aware what is happning. The attacker is able to predict user behavior and abuse its information.

IV. Security and Privacy Issues in Fog Computing

In this section, we analyze potential security and privacy problems in fog computing.

A. *Man-in-the-middle Attack*

In fog computing, there is the potential of a typical man-in-the-middle. In this attack, gateways serving as fog devices may be compromised or replaced by fake ones. Traditional anomaly detection methods can hardly expose man-in-the-middle attack without noticeable features of this attack collected from the fog [3]. In some scenarios, it is difficult to protect communication between fog node and IoT devices using encryption method. Encryption and decryption methods consume large amount of battery on mobile device.

B. *Intrusion Detection*

Intrusion detection techniques are widely deployed in cloud system to mitigate attacks such as insider attack, flooding attack, port scanning, attacks on Virtual Machine(VM) and hypervisor. This intrusion detection system analyzes and monitors access control policy, a log file, and user log information in order to detect intrusion behavior. It can be run on network side in order to detect malicious activity such as DoS, port scanning. Fog computing based IoT device has limited computing and resources, therefore it is difficult to detect the rootkit. An attacker can obtain kernel level privileges in a specific Operating System(OS) by exploiting vulnerability by using a hardware virtualization technology. The rootkits can cause problems to attack a specific system or export important information by having higher privileges than embedded hypervisor.

C. Malicious Detection Technique in Fog Computing Environments

When some fog nodes are compromised, hybrid detection technique is useful to detect malicious code in fog nodes. It is combined with signature-based detection technique [4] and behavior-based detection technique [5]. However, IoT devices have low computing power. The behavior-based detection technique costs largely overhead. While signature-based detection technique is more efficient than it. However, it is difficult to detect various forms of the malicious code in fog nodes. In order to complement this problem, some computation of behavior-based detection techniques that is running on the cloud is distributed into fog nodes. Suspected malware files on a fog node are sent to cloud. If the file is new malware, a result of analysis is stored in the signature database. The result is transmitted to the fog node and updated signature information.

D. Malicious Fog Node Problem

In order to provide service to user, fog nodes process data received from the IoT devices. If the workloads is heavy, it is divided into several jobs and processed by several fog nodes. If some fog nodes are compounded by a malicious user, it is difficult to ensure the integrity of the data. Before the computation begin, fog nodes must be trusted each other. An authentication protocol is required. Fog nodes should trust cloud, because there is no a fog node that manages other fog node. In order to process a volume of data, fog nodes which is authenticated by the cloud should be only located in fog environment.

E. Data Protection

Messages generated from IoT devices is sent to the nearest fog nodes. It is difficult to process a volume of data on IoT devices. The data is divided into some parts and sent to several fog nodes to process it. At this point, the contents of the data should be analyzed without exposing it. When distributed and processed data is merged, the integrity of the data should be guaranteed. Because of limited resources, it is difficult to encrypt or decrypt data on IoT device. As a result, light-weight encryption algorithms or masking techniques [6] are required.

F. Data Management Issues

IoT fog will have a significant impact on our daily lives and process deeply personal information. Fog nodes are geographically distributed, making it difficult to know data's location. The user wants to be provided with the same services in other areas. It is difficult for user to know whether the node provides the same service. Some fog nodes by having duplicated files will cause a waste of resources. Security issues of personal information is happened on distributed fog nodes by wrong approach by malicious user.

V. Conclusions and Future Work

In this paper, we explore sensor, a fog node and cloud which combine to form a fog computing environment. We also describe security issues in each area. Fog computing provides the improved quality of services to the user by complementing shortages of cloud in IoT environment. IoT technology is utilized in various fields in the future and have to be protected from security threats. In this paper, we highlighted the need to configure the secure fog computing environment through security technologies which we analyzed. The extended work could be to develop a system to efficiently collect and analyze various logs generated in fog computing environment. It provides a meaningful situation information to users.

Acknowledgment

This work was supported in part by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2015-H8501-15-1007) supervised by the IITP (Institute for Information & communications Technology Promotion). This research was also supported in part by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2015-H8501-15-1018) supervised by the IITP. This work was also supported in part by the NRF (National Research Foundation of Korea) grant funded by the Korea government MEST (Ministry of Education, Science and Technology) (No. NRF-2012R1A2A2A01046986). This research was supported in part by US NSF HRD-1345219 and HRD1533653.

References

[1] L.M. Vaquero and L. Rodero-Merino, "Finding your Way in the Fog: Towards a Comprehensive Definition of Fog Computing," *ACM SIGCOMM Computer Communication Review*, vol.44, no.5, pp.27-32, Oct. 2014.

[2] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog Computing and Its Role in the Internet of Things," *Proceedings of the first edition of the MCC workshop on Mobile Cloud Computing (MCC '12)*, pp.13-16, Aug. 2012.

[3] I. Stojmenovic and W. Sheng, "The Fog Computing Paradigm: Scenarios and Security Issues," *Federated Conference on Computer Science and Information Systems (FedCSIS)*, pp.1-8, Sept. 2014.

[4] M. Zhang, Y. Duan, H. Yun, and Z. Zhao, "Semantics-Aware Android Malware Classification Using Weighted Contextual API Dependency Graphs," *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14)*, pp.1105-1116, Nov. 2014.

[5] L. Martignoni, R. Paleari, and D. Bruschi, "A Framework for Behavior-Based Malware Analysis in the Cloud," *Proceedings 5th International Conference Information Systems Security(ICISS 2009)*, pp.178-192, Dec. 2009.

[6] P. Barbosa, A. Brito, H. Almeida, and S. Claub, "Lightweight Privacy for Smart Metering Data by Adding Noise," *Proceedings of the 29th Annual ACM Symposium on Applied Computing (SAC '14)*, pp.531-538, Mar. 2014.