Journal of the Korea Convergence Society
Vol. 9. No. 5, pp. 27-32, 2018

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2018.9.5.027

Research on Security Model and Requirements for Fog Computing: Survey

Sunghyuck Hong
Div. of Information & Communication, Baekseok University

포그 컴퓨팅 보안 모델과 보안 요구사항 연구: 서베이

홍성혁
백석대학교 정보통신학부

Abstract IoT technology is developing with various application areas in 4th Industrial revolution. There are many users using the application services. Sensing data from various environment need to be transferred to cloud computing storage and store in the cloud storage. However, physical distance from the end node to cloud computing storage is far away, and it is not efficient to transfer data from sensors and store the sensing data in the cloud storage whenever sensing data happen. Therefore, Fog computing is proposed to solve these problems which can process and store the sensing data. However, Fog computing is new emerging technology, there is no standard security model and requirements. This research proposes to security requirements and security model for Fog computing to establish a secure and efficient cloud computing environment.

Key Words : Fog computing, Security, Authentication, Secure Communication, Sensor Networks

요 약 4차 산업혁명시대 핵심인 IoT(사물인터넷) 기술이 발전하면서 다양한 적용 분야가 생겨나고 있으며, 그에 따른 서비스를 이용하는 사용자 수도 대폭 증가하고 있다. 주변 환경에 흩어져 있는 수많은 IoT 디바이스들에 의해 생성되는 실시간 센싱 데이터들을 실시간 클라우드 컴퓨팅 환경에 전송하여 저장하는 것은 시간 및 저장 공간에 대한 효율성이 적합하지 않다. 따라서 이러한 문제들을 해결하기 위해서 응답시간을 최소화 하면서 처리 시간이 효율적으로 관리가 될 수 있도록 하는 포그 컴퓨팅이 제안되었다. 그러나 포그 컴퓨팅이라는 새로운 패러다임에 대한 보안 요구사항이 아직 정립되지 않고 있다. 클라우드 끝단에 있는 센서노드들은 컴퓨팅 파워가 높지 않기 때문에 보안 모듈을 적용하기가 어렵고, 보안 모듈 적용 시에 경량화된 프로토콜 적용을 통하여 보안과 효율성을 수립하여야 한다. 따라서 이 논문에서는 포그 컴퓨팅에 대한 보안 모델 제시와 포그 컴퓨팅에 최적화된 보안 요구사항을 제시하여 안전한 포그 컴퓨팅 발전에 기여한다.

주제어 : 포그 컴퓨팅, 보안, 인증, 안전한 통신, 센서 네트워크

1. What is fog computing?

Fog Computing is a newly proposed platform to more efficiently provide data storage, computation and network services between Cloud Computing and IoT devices with geographical dense distribution characteristics. While it is possible to define this fog computing as an extension of cloud computing as a model designed to make the fog node responsible for a part of the existing cloud's burden, there is a clear difference from conventional cloud computing[1-5].

Sensors are attached to unmanned vehicles as well as glasses, watches, shoes, and clothes, exchange body information with servers, analyze and provide

This paper is supported by 2018 Baekseok University Research Fund.
*Corresponding Author : Sunghyuck Hong (shong@bu.ac.kr)
Received April 9, 2018 Revised May 10, 2018
Accepted May 20, 2018 Published May 28, 2018

information. Sensors are attached to various places in the building to check the temperature and humidity, and to maintain a comfortable environment or to be used for security through related devices and equipment. However, there is a problem in storing all of this data in the cloud server. There are some physical things such as storage capacity, but there are also time constraints to exchange lots of data. So what is introduced is fog computing. The cloud (cloud) is separated from us, but the term fog (fog) is around us. In other words, it is the concept that data that is often coming out is processed in a nearby device such as a sensor or router rather than stored in a remote cloud, and only necessary information is sent to the cloud. It is a concept proposed by CISCO, a network equipment manufacturer. In fact, when a sensor is attached, countless data is generated every moment. Data that is generated occasionally is processed by a local terminal (sensor, router, etc.), and only the data that needs to be stored is selected and transmitted to the cloud server and stored. For example, suppose that sensors are attached to a railway track to collect the passage information of the locomotives and create an optimal timetable.

If you send all the information to the cloud even when the locomotive is not passing, this is just garbage information. At this time, it is possible to utilize the information more efficiently by selecting only the information when the locomotive passes by the sensor and sending it to the cloud. With the introduction of the fog computing concept, many sensors and equipment companies are developing technologies. It is possible to process data by attaching a processor that can process basic data, not simply a device that only performs sensing. This technology is also related to the density of semiconductors and battery life. The higher the density, the more space can be utilized and the amount of processing data can be maximized, and the longer battery life can increase the processing time and amount. While fog computing is still in its infancy, these additional technologies will become more active as they evolve. Also, as cloud computing evolves, the role of fog computing in complementary relationship is expected to grow[6-8].

2. Fog system model

2.1 Fog Node

Objects as the Internet developed rapidly, the cloud demanded new characteristics. As a result of various requirements such as large-capacity data processing, real-time service and mobility of devices in a wireless environment as well as a wired environment, a new object called a fog node has been proposed. Such a fog node is a type of service

And the like. For example, if a large number of fog nodes require a large amount of resources, a second cloud (data center) can act as a fog node, and if a large amount of computation is not required, A set-top box or the like can be a fog node. Clearly, we need to efficiently provide services such as real-time services and disaster prevention / response systems for rapid decision-making in close proximity to IoT devices[9,10].

2.2 IoT Devices

IoT devices with geographical density distribution characteristics quickly generate and transmit large amounts of data of various kinds. It also requires fast

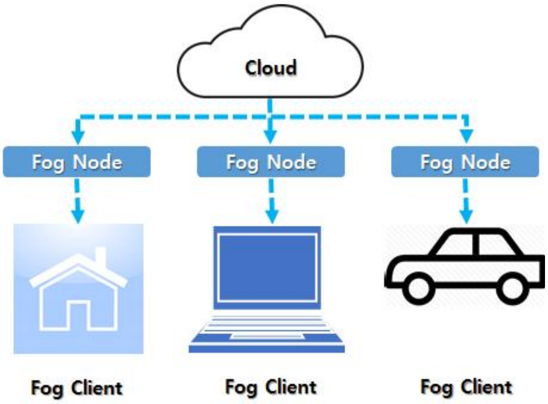

Fig. 1. Basic Fog Computing Model

response time accordingly. It is defined as all the devices which perform the specific service to the user by collecting various types of data connected to the Internet, transmitting them to the fog nodes, or receiving the necessary data from the cloud and fog nodes. Sensors for simple data collection can also be classified as IoT devices[11-13].

2.3 Trust Model

The trust model can vary greatly depending on the type of service to be provided, the nature of the fog node or the IoT device. In this section, we accept these various trust models and define a trust model that takes into account all attack scenarios.

2.4 Cloud

The cloud basically follows the honest but curious model. This is a semi-trust model in which services such as service provision, data management, and computation are performed honestly but there may be attempts to decrypt the encrypted data if necessary. However, when a service provider commits a cloud service to a third party, the cloud can be defined as an Untrust model. If this is the case, it must be able to require proof of encryption, calculation, storage, and secure key management[14-16].

3. Fog Computing Security Requirements

This section introduces the security requirements that should be considered in the overall fog computing environment based on the above defined system model and trust model.

3.1 Replay Attack

An attack is an attack by an attacker who intercepts the authentication information sent to the certification authority and retransmits it. A countermeasure against this attack is to use a session token. The certificate authority sends a session token to the entity it is trying to authenticate and the authentication entity sends the hash value of the session token to the authentication information.

When an attacker intercepts the authentication information and attempts a retransmission attack in another session, the certificate is not accepted because the certification authority has issued a session token for the new session.

3.2 Man-in-the-middle-attack(MITM)

It is a method for avoiding the authentication procedure by forging and falsifying data between the authentication procedures between the certification authority and the entity. Two entities are considered to be authenticated and connected, but in reality they are connected by an intermediary, and all data between two entities is transmitted through the intermediary. Various methods for detecting and defending this have been proposed. However, since this method can not completely prevent the meson attack, it is necessary to establish a defense system capable of detecting and protecting the meson attack in the authentication procedure for the IoT device. In a fog computing environment, a number of IoT devices are connected at the ends. The existing PKI-based authentication system is difficult to apply to fog computing environment due to its low scalability and efficiency. Although an efficient authentication algorithm that can be used in an ad-hoc wireless network has been proposed, in a fog computing environment, a lightweight authentication algorithm suitable for each environment is needed because various network environments besides a wireless network environment must be considered[1].

3.3 Network Security

Network communication between cloud-fog nodes, IoT network communication. An attacker can attack various types of attacks through attacks on connected networks and efficiently design techniques to defend against these various attacks.

3.3.1 DoS / DDoS Attacks

Denial of Service (DoS) / Distributed Denial of Service A Serivce (DDoS) attack is an attack that requires an attacker to do more than the server can handle to stop other services or bring down the system. In a fog environment that requires fast response / processing as an attack to paralyze the network function, slowing the network speed can cause serious problems. Therefore, when building a network environment, it is necessary to protect against DoS / DDoS attacks.

Must be considered.

3.3.2 Intrusion Detection System

The intrusion detection system monitors all kinds of malicious network traffic, behavior, and policy violations that traditional firewalls can not detect. In a fog computing environment, an intrusion detection system monitors fog nodes and can detect malicious behavior. However, in this environment, the number of fog nodes managed by one cloud or the number of IoT devices managed by one fog node may be quite large. IoT devices also move at any time. This is clearly an additional consideration when designing intrusion detection systems.

It is the part that needs to be done. Intrusion detection systems should be implemented in an efficient direction in such a fog computing environment.

3.3.3 Wireless Network Security

The network environment between Fog nodes and IOT devices is likely to be a wireless network environment. There are various security threats due to the special environment of wireless. Jamming Attack is an attack in which an attacker transmits radio frequencies to a wireless network environment to compromise the original message or prevent the message from reaching the receiver, thereby degrading network performance. Sniffer Attack can be a more effective attack in a wireless environment using an open channel. IoT devices and fog nodes must be designed to be secure against vulnerabilities that can occur in a domain called a wireless network.

3.3.4 Storing Reliable Data

Clouds and fog nodes require techniques to deal with the loss or corruption of data that can be caused by system failures in order to provide reliable data storage. By default, data is stored in redundant ways to recover corrupted data due to unexpected errors, but this is certainly not a good way of efficiency. You should consider how to efficiently store reliable data in a fog node or IoT device with a smaller storage capacity than the cloud.

3.3.5 Security Model for Fog Computing

Figure 2 describe the model and its three core components. 1) the Region-Based Trust-Aware component which is a region can be structured by one or several fog nodes; 2) Fog-Base Privacy-Aware Role Based Access Control; and 3) the mobility management component which Fog devices are highly dynamic and frequently switch among regions. It is vital to provide a mobility service at regions handling location requests such as update and query. The mobility management component includes the Mobility Service (MS) and the LRD [17].

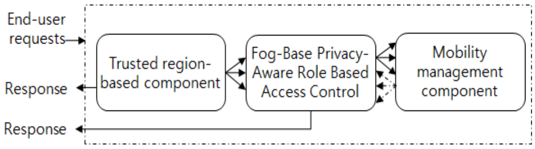
End-user requests
Response
Response
Trusted region-based component
Fog-Base Privacy-Aware Role Based Access Control
Mobility management component

Fig. 2. Security Model of Fog Computing

3.3.6 Safe data operations

It is dangerous to leave any operations to untrusted institutions. If you trust an operation to an untrustworthy cloud or fog node, you need to verify that the operation performed correctly. However, considering the characteristics of the fog computing environment, additional costs incurred during the process of generating or verifying such proofs may be a problem for use in devices with low computational resources.

4. Conclusion

Conventional centralized cloud computing systems have problems that are not suitable for distributed IoT environment due to structural rigidity. Fog computing, which is proposed to provide functions such as latency minimization, context awareness, and mobility, has not been defined to the system model or trust model so far. In this paper, we define these models and summarize the various security issues that can occur. As IoT devices become closer to real life, security becomes important. The system designer should design the system in consideration of the security requirements required in the fog computing service that it intends to provide with new security issues in the fog environment.

REFERENCES

[1] S. Hong. (2017). Research on IoT International Strategic Standard Model. *Journal of the Korea Convergence Society*, *8(2)*, 21-26. doi:10.15207/jkcs.2017.8.2.021

[2] S. Hong. (2014). Analysis of DDoS Attack and Countermeasure: Survey. *The Journal of Digital Policy and Management, 12(1),* 423-429. doi:10.14400/jdpm.2014.12.1.423

[3] C. Gu, Y. Zheng, F. Kang & D. Xin. (2015). Keyword Search Over Encrypted Data in Cloud Computing from Lattices in the Standard Model. Cloud Computing and Big Data Lecture Notes in Computer Science, 335-343. doi:10.1007/978-3-319-28430-9_25

[4] K. Tammemäe, A. Jantsch, A. Kuusik, J. Preden & E. Õunapuu. (2017). Self-Aware Fog Computing in Private and Secure Spheres. Fog Computing in the Internet of Things, 71-99. doi:10.1007/978-3-319-57639-8_5

[5] P. K. Rayani, B. Bhushan & V. R. Thakare. (2018). Multi-Layer Token Based Authentication Through Honey Password in Fog Computing. International *Journal of Fog Computing, 1(1),* 50-62. doi:10.4018/ijfc.2018010104

[6] V. Mushunuri, A. Kattepur, H. K. Rath, & A. Simha. (2017). *Resource optimization in fog enabled IoT deployments.* 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC). doi:10.1109/fmec.2017.7946400

[7] Cloud and Fog Computing. (2017). *Secure Connected Objects,* 238-247. doi:10.1002/9781119426639.ch17

[8] R. Rios, R. Roman, J. A. Onieva & J. Lopez. (2017). *From SMOG to Fog: A security perspective. 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC).* doi:10.1109/fmec.2017.7946408.

[9] S. Hong, S. Lim & J. Song. (2011). Unified Modeling Language based Analysis of Security Attacks in Wireless Sensor Networks: A Survey. *KSII Transactions on Internet and Information Systems,* 805-821. doi:10.3837/tiis.2011.04.010

[10] S. Hong. (2013). Disconnection of Wireless LAN Attack and Countermeasure. *The Journal of Digital Policy and Management, 11(12),* 453-458. doi:10.14400/jdpm.2013.11.12.453

[11] Hong, S. (2015). Two-channel user authentication by using USB on Cloud. *Journal of Computer Virology and Hacking Techniques, 12(3),* 137-143. doi:10.1007/s11416-015-0254-y

[12] S. Hong. (2017). Secure and light IoT protocol (SLIP) for anti-hacking. J*ournal of Computer Virology and Hacking Techniques, 13(4),* 241-247. doi:10.1007/s11416-017-0295-5.

[13] K. Choi & J. A. Yoo. (2015). A reviews on the social network analysis using R. *Journal of the Korea Convergence Society, 6(1)*, 77-83. doi:10.15207/jkcs.2015.6.1.077

[14] G. Ryu. (2015). Development of Educational Model for ICT-based Convergence Expert. *Journal of the Korea Convergence Society, 6(6),* 75-80. doi:10.15207/jkcs.2015.6.6.075.

[15] Y. Joh, Y. (2014). A Framework for IoT-Based Convergence Personalized Menu Recommendation System. *Journal of the Korea Convergence Society ,5(4),* 147-153. doi:10.15207/jkcs.2014.5.4.147.

[16] Fog Computing and compare with Cloud Computing. (2017). *International Journal of Recent Trends in Engineering and Research, 3(12),* 129-131. doi:10.23883/ijrter.2017.3546.pszaf

[17] B. Negash, A. M. Rahmani, P. Liljeberg & A. Jantsch. (2017). Fog Computing Fundamentals in the Internet-of-Things. *Fog Computing in the Internet of Things*, 3-13. doi:10.1007/978-3-319-57639-8_1

홍 성 혁(Sunghyuck Hong) [종신회원]

- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2007년 9월 ~ 2012년 2월 : Texas Tech University, Office of International Affairs, Senior Programmer
- 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수
- 관심분야 : Network Security, Hacking, Secure Sensor Networks
- E-Mail : shong@bu.ac.kr