Key Technologies of Security Access Control in Fog Computing Environment

Sun Bin1,*, Wang Yongjie2
1Weifang Medical University, Weifang, China
2Shandong College of Information Technology, China
*Corresponding author: xxb@wfmc.edu.cn

Abstract. The rapid development of Internet technology has promoted the innovation of mobile communication technology. Following 2G, 3G, and 4G technology, mobile communication has entered the 5G era. At the same time, the trend of interconnection of all things is becoming more and more clear, and the simple cloud computing is gradually changing to more advanced and powerful fog computing. As a near-maturity edge computing model, fog computing is gradually popularized and applied. The security problem is always the most important thing in network technology. Therefore, it is necessary to think about the security access in fog computing environment. This work mainly discussed the security access control technology in fog computing environment, clarified its key parts, and analyzed its effective control technology from two aspects: extended access and hidden access. This work will give users more flexible access control options to thus achieve effective protection of data security and related factors.

Keywords: Fog environment; Secure access; Control; Key technologies

1. Introduction
Fog computing is the fusion product of many technical trends. It is developed on the basis of cloud computing and is suitable for distributed computer storage of Internet of things scenarios. It is scattered on multiple nodes near the user with advantages of low delay and high expansibility. In the era of fog computing, people also pay extensive attention to the problem of safe access. How to ensure the safe access of data must be innovated in technology and make it safe on the basis of giving full play to the advantages of fog computing. In a large number of investigations and studies, it is found that in order to ensure the security of user data, we must strengthen the cooperation and dialogue of each functional module, add a new access structure by confirming the integrity of the data to achieve a higher level of privacy protection. The solution of safety problem will further promote the application of fog computing and make it more valuable.

2. Sketch of Fog Calculation
Fog computing as an extension of cloud computing is proposed, as shown in Figure 1. Fog computing combines cloud services with distributed resources near the edge of the network to make storage and data processing close to the edge of the network devices. It can provide a variety of services such as
outsourcing computing, resource allocation and caching. It is widely used in intelligent medicine, intelligent city and other fields with high demand for low delay. Fog computing is closer to the end user, and the data contains a large amount of user privacy information. Because of the existence of false nodes to obtain data maliciously, it is necessary to design an efficient access control scheme in fog computing environment. Edge device CP-ABE in fog computing is one of the technologies to realize fine-grained access control. The data owner encrypts the data according to the attributes without knowing the exact identity of the user. Only users who satisfy the attributes can access the data.

![Figure 1. Structure diagram of fog computing system](image)

3. Fog Computing Access Control Scheme

3.1. Extended Access Control Scheme for Fog-oriented Computing

The most used function for most enterprises or individual users in cloud architecture is storage function. Its high efficiency and low cost advantages make people more and more dependent on it. By storing the data in the logical storage, the server in the physical location can span multiple locations and multiple servers, which makes the storage of the user's production data more convenient and the information sharing faster. Attribute encryption technology is often used to control the decryption ability of data users in access control of shared data, in which CP-ABE technology is the most widely used. In the CP-ABE scheme, the access structure is first established according to the actual requirements, and then the ciphertext is formed by combining the access structure. The user's key is associated with the attributes assigned by himself. In the practical application scenario, it is often necessary to extend the access structure in time, which means that the users who have satisfied the original access structure also need to have the ability to expand the new users to become legal users and add new access structures. Access control technology has been widely studied in cloud computing. However, considering the difference between fog computing and cloud computing in network architecture and system model, the existing access control strategy for cloud computing can not be directly applied to fog computing field. Especially after introducing fog nodes, how to reasonably allocate the operation and communication overhead between fog nodes and end users and cloud servers in this process, how to form simple, effective and secure access control between cloud, fog and end users, and how to extend access structure while ensuring the integrity protection of raw data have
been the key to realize data security sharing in fog environment. Therefore, a scheme is necessary to extend the access structure by implementing data integrity check in fog environment.

For example, in the scenario in Figure 2, company A sends data such as product identity information into the information system, and the access structure set by company A is accessible to staff with a position above A level. However, when company B also needs to access the data, it cannot be achieved in time if it cannot contact the uploaded staff. However, under the extensible access control scheme, it is allowed to meet the original access structure, that is, the staff above A level in company A position, without destroying the integrity of the original data. The new access structure can be extended to enable company B specific staff to access the data.

![Figure 2. Extended Access Structure Scenario](image)

There are five entities in the extensible access control system for fog computing: trusted mechanism, fog node, cloud server, data uploader, data user, and the system structure is shown in Figure 3. In this scheme, all entities will execute various algorithms truthfully, and there is no collusion attack between different entities. The trusted organization holds the main key of the system. When the data user sends out the registration request, the trusted organization runs the registration algorithm according to the attribute owned by the user, and distributes the private key to the data user and part of the private key to the fog node. Fog nodes are terminals in the system that are closer to the user than remote cloud servers. They undertake part of the calculation operation for the data user and return the calculation results to the user in the subsequent decryption part. In the system, the data uploader first uses the plaintext locking encryption algorithm to obtain the unique value of the unique data, and uses the unique value in the key used for symmetric encryption. Then the symmetric encryption algorithm is used to encrypt the plaintext data until all ciphertext is uploaded to the cloud server.

Data user is the user who needs to access the data uploaded by the data uploader. In the system, each user has its own attribute set. Before accessing the data, the data user will register according to their own attributes to obtain their own private key. The ciphertext is decrypted by private key, and accordingly the plaintext information can be obtained. In the scheme proposed in this chapter, the data users who meet the requirements of the original access structure can expand the access structure so that more users can share the original data information in time. However, data users must ensure that no changes are made to the original data. The fog node will check the new access structure. After the inspection is passed, the new access structure will be added to the cloud server, which not only realizes the access control flexibly, but also expands the scope of data sharing safely. By default, data users in this system do not share plaintext information and private keys with others. The cloud server can
provide powerful storage space for users, save all kinds of ciphertext for data uploads and download ciphertext for data users. When the new access structure passes the integrity check, the cloud server will save the new access structure, thus realizing convenient and fast data sharing.

![Figure 3. Extended access control system for fog-oriented computing](image)

3.2. Access control structure hiding scheme for fog-oriented computing

The most widely used computing architecture in cloud is storage service. Users upload the data they need to store to the cloud server. This service can not only solve the problem of limited storage space for users, but also facilitate cross-regional data sharing. In order to meet the requirements of different levels of data for users to see in different ranges, the data uploader will create a corresponding access structure to encrypt the uploaded data according to his own requirements. Access structure refers to a series of rules that need to be followed by access subject resources, which are expressed in the form of access control table or access control matrix. Because any data uploaded by the user is classified, the security of all data should be considered first. Thus, a hidden scheme of access control structure for fog computing is proposed. Using the idea of Ying, the cuckoo filter algorithm is introduced into the fog computing, and the mapping function in the access structure is hidden by the cuckoo algorithm in the data upload process. The ciphertext is stored separately from the access structure, and the cuckoo algorithm is used to detect whether the attributes of the data user exist in the hidden access structure during the decryption process. If it exists, the reconstruction of the mapping function is sent to the data user, and the data user downloads and decrypts the ciphertext again, which indicates that the data user does not meet the access conditions does not need to download and decrypt the ciphertext.

There are five entities in the access control structure hiding system for fog computing: trusted mechanism, fog node, cloud server, data uploader, data user, as shown in Figure 4. A trusted mechanism is a fully trusted mechanism in the system, which generates system parameters and master keys. Data users are consumers in the system who need to obtain information uploaded by the data uploader. In the registration phase, the private key belongs to the private key by passing the set of properties owned by itself to the trusted organization. Data uploaders are producers in the system who
share data by uploading their own information. As a data producer, the data uploader has the right to make the access structure, to control the shared data, and to encrypt the data to generate ciphertext to the cloud server through the access structure. At the same time, the completely hidden access structure is transmitted to the fog node to facilitate data user attribute set detection. The fog node is responsible for storing the completely hidden access structure in the system. Before the data user downloads the ciphertext for decryption, the properties of the data user are detected to determine whether it conforms to the access structure set by the shared data. The cloud server provides the service of ciphertext storage for the data uploader and the data user. When the data uploader generates the ciphertext according to the specified access structure, it uploads it to the cloud server for storage. The data user downloads the ciphertext to the cloud server after the attribute confirmation.

**Figure 4.** Access control structure hidden system for fog-oriented computing

4. Summary
Fog computing, as a new computing mode, combines its own advantages with cloud computing to form a new technical architecture to provide more timely, convenient and fast virtualization services for end users. Through the special study of access control in fog computing, the extension of access structure is realized by detecting the integrity of raw data, which not only confirms the loyalty of users in the system and reduces the computational overhead of users and cloud servers, but also improves communication rate and offers more secure and efficient data sharing.

**References**
[1] Yakubu, J., Christopher, H. A., Chiroma, H., & Abdullahi, M. (2019). Security challenges in fog-computing environment: a systematic appraisal of current developments. Journal of Reliable Intelligent Environments, 5(4), 209-233.
[2] Huang, Y., Li, B., Liu, Z., Li, J., Yiu, S. M., Baker, T., & Gupta, B. B. (2019). ThinORAM: towards practical oblivious data access in fog computing environment. IEEE Transactions on Services Computing, 13(4), 602-612.
[3] Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M. A., Choudhury, N., & Kumar, V. (2017). Security and privacy in fog computing: Challenges. IEEE Access, 5, 19293-19304.
[4] Aleisa, M. A., Abuhussein, A., & Sheldon, F. T. (2020). Access Control in Fog Computing: Challenges and Research Agenda. IEEE Access, 8, 83986-83999.
[5] Khairnar, S., & Borkar, D. (2014). Fog computing: A new concept to minimize the attacks and to
provide security in cloud computing environment. IJRET: International Journal of Research in Engineering and Technology, 3(06).
[6] Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the internet of things: Security and privacy issues. IEEE Internet Computing, 21(2), 34-42.
[7] Khan, S., Parkinson, S., & Qin, Y. (2017). Fog computing security: a review of current applications and security solutions. Journal of Cloud Computing, 6(1), 1-22.