Discussion on Access Control Technology of Cloud Computing

Yibai Wang, Shi Chen*

Changsha Medical University, Hunan, 410219, China

Keywords: Cloud computing; access control; key technology

Abstract: This paper focuses on the discussion on access control technology of cloud computing. On the basis of briefly describing the composition and principle of access control technology, this paper analyzes some problems existing in cloud computing access control. Moreover, it presents key technologies for cloud access control. It is concluded that the scientific and reasonable application of cloud computing access control technology can effectively guarantee the security of cloud computing resources to provide some help to the relevant cloud computing staff.

1. Introduction

Cloud computing access control technology has great significance to ensure the security of cloud computing resources. It is widely used in cloud security protection. However, cloud computing has the virtualization and distributed characteristics, and has high requirements for access control technology. Our research on this aspect is not deep enough. Therefore, based on theoretical practice, this paper discusses cloud computing access control technology as follows.

2. Composition and Operation Management of Access Control Technology

There are three main factors in access control technology: subject, object and control strategy. The subject refers to the visitor who makes the request. In the actual application, the subject can be either a person or a device. Object refers to the actual situation of the subject being accessed, such as the information and resources that can be manipulated as objects. P represents the control strategy, which refers to the subject's access rule set for the object. It needs to be highly valued.

The main body of access control is to make different access to resources, information and data in cloud computing according to the specific policies and permissions of cloud computing access. In the specific application process, the scope of access to subject and object should be controlled comprehensively through some specific constraint authorization. It can effectively prevent illegal elements from accessing the system and illegally access the relevant vehicle resources and information in the cloud computing by legitimate users of the house. The operation principle of cloud computing access control is shown in figure 1.

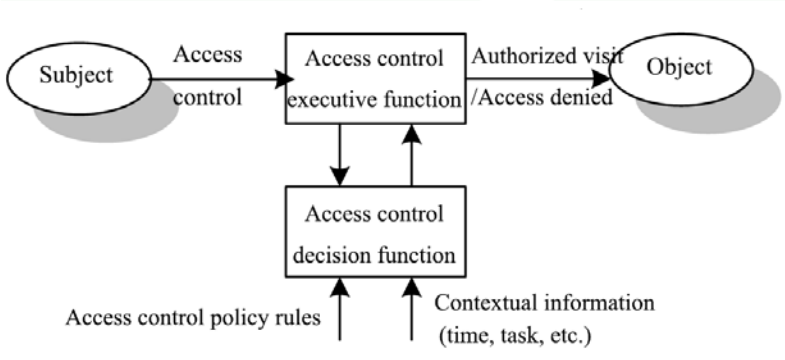

Figure 1. Operation principle of cloud computing access control

It is clear from figure 1 that the main purpose of cloud computing access control is: through a series of methods, the access rights of subject and object are controlled to ensure the security of relevant data and information in the specific application process. To achieve this goal, the cloud

computing access control needs to proceed from the following two aspects: firstly, after identifying the user identity information of the access system, and the authenticated user will be able to match the resource bureau and information. Secondly, the access to resources in a system is set up to ensure that all resources in cloud computing can be legally applied and controlled.

3. Existing Problems in Cloud Computing Access Control

Although in recent years, China's cloud computing, big data, Internet of things technology and so on have achieved good development, there are still a series of problems to be solved in the application process. It mainly reflects the following aspects:

Firstly, there are problems with architecture. With the development of China's social and economic development, the application scope and control methods of many traditional access control systems have been difficult to meet the actual demand of cloud computing architecture. However, with the development of virtual technology and simulation technology in China, the access control technology of cloud computing has gradually evolved from the traditional user authorization to the security access of virtual resources. The security of access control is greatly improved, and the control range and control means are becoming more and more advanced. At the same time, there is a certain conflict between access control decentralized management and centralized management under the background of cloud computing. In addition, under the background of cloud computing environment, the access control strategy in the open dynamic management also puts forward higher requirements for the security management in the cloud environment. If these three points are not effectively solved, the development of access control technology will be greatly limited.

Secondly, there are problems with the mechanism. It mainly reflects the following aspects: (1) Users can easily lead to mutual authorization and resource disclosure when they are accessing cloud computing information and resources. This problem is bound to cause serious damage if it is not solved effectively. (2) Under the background of cloud computing environment [1], the mechanism of virtual resources and the underlying complete acute isolation will make the hidden channel more difficult to be detected. (3) In the current situation of cloud computing development in China, if the trust problem is not solved effectively, it will inevitably affect the access control.

Thirdly, there are problems with the model. During the current development of cloud computing technology in China, the existing access control model has been difficult to meet the actual demand of cloud computing architecture, which limits the development of access control technology. In recent years, China's rapid social and economic development has laid a solid foundation for the development of cloud computing. Access control relationships have also become more complex, and users have changed more frequently. In the application process, the user's access to the data needs to be selected and can be highly distinguished.

4. Key Technologies in the Operation of Cloud Computing Access Control

4.1 Access control technology for cloud computing.

The research on cloud computing technology is relatively late in China, and the research on cloud computing access control model is not deep enough. The access control model of cloud computing is developed from the traditional access control model. In order to better adapt to the specific requirements of cloud computing environment, we can start from the following aspects.

Firstly, the permission attribute dynamic cloud computing access control technology. In the cloud computing environment, a lot of information and resources have become socialization and public. There is a lot of data going on every day, and the need for cloud resources and services is more uncertain. In the application process, it is necessary to adjust in real time according to the actual operation situation, so as to effectively meet the actual demand. This requires dynamic management of cloud user permissions. It is necessary to extend appropriate access control model based on the extensibility of role, trust, task, attribute and so on. In this way, the access control technology for

cloud computing can have the ability of automatic adjustment [2].

Secondly, virtualization - oriented cloud access control technology. Cloud computing is defined as a statistical computer model based on virtualization technology. The main software for virtualization is hypervisor. The main principle is to form an abstraction layer in the technical computer hardware and virtual server. Then, through Vmware vSphere or hyper-v software, the virtualization processing of data is realized in the computer. Compared with traditional access technology, the virtual access control technology has obvious advantages in application effectiveness and reliability. In the virtualized environment, the hypervisor can run on bare hardware, which is hard to compare with other software [3].

Thirdly, the cloud computing access control technology for multi-application domain is usually composed of multiple autonomous domains, which can greatly improve the efficiency of access control. For example: A, B, and C, if A domain is trustworthy to B, and the B domain is also more trustworthy to the C domain, it can be shown that the A domain and the C domain are also mutually trusting relationships. However, in the application process, in order to ensure the security of the data, external trust cannot follow the above methods. In terms of the access control technology of cloud computing, the trust relationship between domain and domain can be broadly divided into two categories: one-way trust, two-way trust [3]. In the application process, it is necessary to have the corresponding access control model to coordinate and manage, so as to give full play to the role and value of cloud computing access control technology.

Because cloud computing is very complex and systematic, it puts forward higher requirements for access control. Under the background of the Chinese cloud computing, China's access control technology has a good development space.

4.2 Security analysis technology of access control strategy.

The security analysis of access control strategy is the main part of cloud computing environment. Through access control strategy security analysis technology, the corresponding information and resources will not leak. The security analysis techniques of access control strategy include the following two aspects:

4.3 Analytical method based on logical derivation.

This method can be divided into three categories: theory-based reasoning, mathematical model and quantitative analysis. Based on the analysis method of theorem reasoning, the correctness of the control model is proved by the corresponding safety axiom. But it is difficult to find the axiom of omni-directional security in all directions. Based on the mathematical model, the digital model is used to replace the access control strategy.

4.4 Analysis method based on state space reasoning.

This method can effectively determine whether the state space in the cloud computing access control is good and can meet the specific requirements. In the specific application process, it can be divided into three steps. The firstly step, the methods for cloud access control strategy need to be determined and implemented in practice. The second step, after the analysis and matching, the first policy condition is found to be inconsistent with the actual situation, and the next strategy is analyzed until the matching is found. The third step, if the conditions and constraints of the policy match in the actual access, the system can be accessed, which depend on the access control settings. The application example shows that this technology can fully prove the integrity of cloud computing access control system. However, in terms of the actual situation of China's current development, the technologies are not mature enough, but they have a very broad development prospect [4].

4.5 Consistency analysis technology of cloud computing access control.

Strategic conflict refers to two or more strategies. Due to the difference of the content of the expression rules, the access control technology is inconsistent in the implementation process. In the cloud computing environment, if the strategy conflicts, the corresponding system will not be carried

out smoothly. Moreover, it will affect the stability and quality of the whole system. In order to solve such problems effectively, we can start from the following two aspects.

4.6 Conflict detection technology of access control strategy.

Strategy conflict detection technology is one of the most widely used technologies in cloud computing access control technology, which can effectively solve the problem of information conflict. The network policy server (NPS) uses the network policy and the input property of the user account to determine whether a connection request should be authorized to treat the network policy as a rule. The NPS checks each connection request according to the first rule in the list [5]. In the cloud computing environment, there is a huge amount of data generated every day, which greatly increases the complexity of access control strategy.

4.7 Conflict resolution technology of access control strategy.

Based on the different stages, the conflict resolution technology of access control strategy can be divided into two types: detect elimination before strategies of creating and the detect elimination during strategies of creating. Detect elimination before strategies of creating is the most direct method. By changing the policy conditions, the conflict can be suppressed. However, it is necessary to find the problem in the formulation of the strategy stage, which greatly increases the difficulty of resolving the conflict resolution. It is more convenient and practical to eliminate the detection in execution strategy. When conflict occurs, seek professional dissolving method [6].

5. Conclusion

From the above, based on the theoretical practice, this paper probes into the technology of cloud computing access control. In the context of the new era, cloud computing security protection technology has been widely used in various fields. Cloud computing itself has the virtual and distributed characteristics, which greatly increases the difficulty of access control technology. In actual operation, there are still some problems to be solved. In order to ensure the security of data and related information in cloud computing, we need to start from several aspects of cloud computing access control model design technology, strategic security analysis and consistency analysis.

Acknowledgement

Key Laboratory Breeding Base of Hunan Oriented Fundamental and Applied Research of Innovative Pharmaceutics (2016TP1029)

References

[1] Long Quanbo. Research on Access Control Technologies for Cloud Computing [J]. Journal of Software, 2015, 26(5):1129-1150.

[2] Wang Yuding, Yang Jiahai, Xu Cong, etc. Survey on Access Control Technologies for Cloud Computing [J]. Journal of Software, 2015, 26(5):1129-1150.

[3] Qi Bin. Survey on Access Control Technologies for Cloud Computing [J]. China New Telecommunications, 2017, 19(3):124-124.

[4] Xiong Dapeng, Chen Liang, Wang Peng, etc. Research Progress on Access Control Technology in Cloud Computing [J]. Journal of Equipment Academy, 2017, 28(2):71-76.

[5] Li Yaqi. Survey on Access Control Technologies for Cloud Computing [J]. China Computer & Communication, 2016(22):47-48.

[6] Lin Guoyuan, He Shan, Huang Hao, etc. Access Control Security Model based on Behavior in Cloud Computing Environment [J] Journal on Communication, 2012(3):59-66.