Research on Access Control Model Based on RBAC Model in Microservice Environment

Jiantao Zhao\textsuperscript{a}, Jin Sun\textsuperscript{b}

Institute of network and information systems, North China Electric Power University, Beijing, China

\textsuperscript{a}zhaojiantao@eplian.com, 86-13811990702
\textsuperscript{b}sunjin@eplian.com, 86-18811384726

ABSTRACT. With the development of cloud platform technology, micro-service has become a very popular software development architecture mode. The micro-service architecture reduces the coupling between application modules, which is conducive to the development, deployment and operation of complex application systems, but also brings many system security problems. Access control model is an important guarantee. This paper discusses the basic requirements of access control in micro-service environment. Through the research of traditional access control technology, the limitations and shortcomings of access control in micro-service environment are analyzed, and an optimization model of access control based on RBAC is proposed.

1. INTRODUCTION

With the rapid development of information age, business system becomes more and more complex after continuous expansion and evolution, resulting in a series of problems such as high application coupling, high code repetition rate, high maintenance cost, long delivery and iteration cycle. A large number of tightly coupled codes lead to increasingly blurred boundaries between application modules, which slows down the speed of repairing problems and modifying changes; when frequent changes are made, a large number of regression tests need to be done, and if problems are found in the test process, they need to be modified again, which prolongs the test time; all functions are put into a release package, which often needs to wait for most or all modules of each other The development and test are completed before unified deployment, which delays the release time. Nowadays, the traditional way is hard to meet the complex development requirements.

In 2012, Martin flower, chief scientist of ThoughtWorks, proposed the concept of microservice Architecture [1]. Microservice architecture is a kind of architecture mode. Microservice architecture develops an application as a set of microservices. These microservices can run their own processes and use lightweight mechanisms such as HTTP resource API to communicate. These microservices are built around business capabilities and can be deployed independently through a fully automated deployment system. These services only have the minimum centralized management, and can be expanded and scaled independently. Each service defines a clear boundary, and can even be written in different programming languages, using different data storage technologies, and can also be managed and maintained by different teams. With the development of docker container technology and cloud computing technology, it provides a good operating environment for microservices, which makes the concept of microservices attract more attention in the field of Internet [2].
Using microservice architecture will also introduce new problems: the application based on microservice architecture is a distributed system, services run independently in different processes, and there is a need for interprocess communication mechanism to support the interaction between services; the application is composed of multiple services, each service can have multiple instances, when a service exists in multiple host nodes, a set of service discovery mechanism is required, so that the service caller can get the correct service address. These are the problems that need to be solved when implementing the microservice framework. Among them, security is a problem that any complete application system must consider, and access control technology is an important means.

2. ACCESS CONTROL MODEL FOUNDATION
Access control refers to the means by which the system limits the ability of users to use data resources on their identities and their predefined policy groups. It is usually used by system administrator to control user’s access to server, directory, file and other network resources. Access control is an important basis of system confidentiality, integrity, availability and legitimate use, is one of the key strategies of network security and resource protection, and is also the different authorization access of subject to object itself or its resources according to some control strategies or permissions [3]. In addition to user access and mutual access between microservices, external third-party systems may also need to access microservices within the system. For example, online stores, external recommendation services may need to access the system to obtain the store catalog information. Compared with the access between internal services, the access request to the external system needs more strict security control. Access control is the process of granting authentication to access users according to the access rights set by the system. It is a very important part of network security. It is the core to ensure that resources are not illegally accessed and used. As one of the core contents of information system, it directly affects the security and efficiency of a system. With the rapid iteration of Internet technology, microservice architecture is widely used in Internet applications because of its flexible expansion, independent deployment and other advantages [4]. Some popular microservice frameworks, such as spring cloud, Dubbo, HSF, etc., play an important role in the main business of Internet companies. At the same time, access control will become more complex in the information system of microservice architecture, so it is of great significance to study this problem.

2.1 Microservice Access Control Defects
The traditional monolithic system is divided into several different micro-service instances according to the business content. The access control module can be separated into a service or into various business services. Comparing with single-body system, the pain points of access control are as follows:

(1) When visitors are not only users, but also other services, the management of access control under the single-body architecture no longer meets the requirements. Considering the scenarios applicable to access entries, there will be many scenarios such as authentication between users and services, authentication between services and other scenarios.

(2) Access requests under micro-service architecture are generally stateless, which leads to the need for access control for each request of users, which makes the access pressure of access control module increase.

(3) The system under the micro-service architecture needs to manage some unique resource information, such as the management of service instance information. Based on the traditional load balancing technology, this management mode can increase the management of access to service instances, and provide service instance information for different access requests, so as to improve the flexibility of system management.

2.2 Role-based access control model RBAC
Both the DAC model and the MAC model grant the access right of the object directly to the user subject, which has many security problems. With the development of computer and network technology, there are more and more functional modules in the system, and the object resources that
need to be protected grow exponentially, which makes the system difficult to maintain and manage. Moreover, the DAC model is too flexible, and the operation authority of the object resource can be granted arbitrarily by the owner of the subject, which will threaten the security of the system. The MAC model has its own defects, and its deployment workload is huge and not easy to manage. Due to the strict authority management mechanism, the authorization efficiency is low and the flexibility of the model is poor. Therefore, it can not be applied to the dynamic open environment. DAC and MAC have been unable to meet the needs of practical applications, so role-based access control model RBAC has emerged.

The above-mentioned autonomous access control and forced access control have their own advantages and disadvantages, and their application scope is limited. Therefore, access control researchers put forward a role-based access control model. RBAC model has the advantages of both DAC and MAC models, and it is quickly recognized by the academic community. Compared with the traditional access control model, RBAC model adds a role as a bridge between users and permissions. First, set appropriate permission set, role set and user set according to the system requirements, and set the allocation relationship between users and roles, roles and permissions. The permissions a user has are the sum of the permissions his role set has. The whole access control process is divided into two important parts: user and role, role and permission, which are many to many relations, thus realizing the logical separation of user and permission.

RBAC is a technology that has been proved to be applicable to large-scale authorization control applications. RBAC is a mature access control scheme based on continuous practice. The practice shows that the right management system based on RBAC model has the following advantages:

1. the change between roles and permissions is much slower than that between roles and user relations, which reduces the complexity of authorization management and management overhead;
2. it can support the security policy of application system flexibly, and has great flexibility to the change of application system;
3. in terms of operation, authority allocation is intuitive, easy to understand and easy to use; hierarchical authority is suitable for hierarchical user level forms;
4. strong reusability.

The model is not suitable for the open network environment, because its user rights cannot be changed dynamically in the interaction process, and the malicious behavior of the user cannot be stopped in time; the model authorization policy is static and fixed enough, and the access rights of the subject to the object cannot be changed properly by predicting the user behavior, and the model has weak scalability [5]. Therefore, RBAC can not be well used in the system with fine-grained authority or dynamic changes and rapid business expansion. We need to continue to find effective methods to improve and optimize RBAC model, so as to avoid the above problems as much as possible, and provide higher security and reliability guarantee for the system.

3. OPTIMIZED RBAC MODEL

3.1 Requirement Analysis

Access control of single-body system usually adopts centralized management mode. The first step is to identify the user's identity information and authenticate the user's identity through the privilege control module; the second step is to restrict the access behavior according to the established access rules; and the third step is to access the business module of the corresponding function. In the same process as the business module, the access control module of the single-body system maintains the stateful user login information for access control, such as Session technology.

The access control mode under the micro-service architecture divides the traditional single-body system into several different micro-service instances according to the business content. The access control module can be separated into one service or into various business services.

Our Goals face many technical challenges. One of the most challenging problems is to implement the role hierarchy (or lattice) used in RBAC into ABE and partial order relations. Although some
cryptographic work has been done to implement RBAC-based hierarchical keys, they can not be
directly used in ABE. In addition, some work in ABE has supported tree hierarchy (called hierarchical
ABE), but they can not support the complete RBAC type hierarchy, that is, the lattice with tree,
inverted tree and general hierarchy. Therefore, it is necessary to develop a new ABE structure with
complete RBAC type hierarchy.

ABE algorithm steps:
Initialize SetUp (d): No input but contains an implicit security parameter d, which outputs the
required public key (PK) and master key (MK) throughout the process.
Key Generation (MK; I): Input the primary key MK and attribute set I, and generate the private key
SK corresponding to user attribute set I.
Encrypt (PK; M; T): Encrypt is executed by the data owner, encrypts plaintext M with public key
PK and access structure T, and obtains ciphertext E.
Decrypt (PK; E; SK): Recursively executed after the user receives the ciphertext E. The public key
PK contains the password E of access policy T and the user private key SK of corresponding attribute
set I as input. If the attribute set I satisfies the access structure T, the output plaintext M can be
calculated.

3.2 Access Control Model in Cloud Environment
In ABE algorithm [6], on the one hand, the user's private key is associated with a set of attributes
composed of any number of describable attributes. On the other hand, when the data owner encrypts
the plaintext, he assigns the access structure for decryption to the encrypted plaintext. Therefore, the
standard of decrypting ciphertext is that the set of attributes in the user's private key must satisfy the
access control strategy in the ciphertext, otherwise it can not be decrypted.

In the aspect of cloud data access, some people put forward an adaptive security management
model based on RBAC model. The model can calculate the security level according to the context
information and adjust the user's role dynamically. It is adaptive and can effectively solve the problem
of dynamic changes of various environment variables in the cloud environment. The advanced
architecture of this storage system is shown in Figure 1.

![Figure 1. Storage Architecture.](image)

In addition, a dynamic access control model based on trust and role is proposed for cloud
computing environment, which is called T-RBAC (tmst-rbac) model, and the formal definition and
execution process of the model are given. Based on the traditional RBAC model, this model adds trust
calculation and trust evaluation module, and introduces the concept of service level. According to the
service level corresponding to trust value, the model dynamically grants access to resources, which
improves the rationality of trust calculation method and the reliability and practicability of T-RBAC
model.

3.3 Access Control Model in Microservice Environment
In the RBAC model, in order to achieve automatic granting between users and roles and more fine-
grained access control, we adopt the combination of ABE algorithm and RBAC model. In the RBAC
model, in order to achieve automatic granting between users and roles and more fine-grained access control, we adopt the combination of Abe algorithm and RBAC model. In order to implement data encryption using Abe in current RBAC model, an effective method is provided to transform RBAC model into Abe based model. Based on this idea, Abe can be used to encrypt data and then store it in the cloud. Create a framework of RBAC compliant Abe system, in which users can use the existing RBAC system to access the microservice resources, and the access process is completely transparent to users. At the same time, with Abe encryption, all data in the system can be stored and shared. In order to make up for the difference between RBAC and Abe, administrators need to establish a transition from RBAC to Abe. Each user's terminal needs to deploy an RBAC to ABE module to realize the above transformation.

On the one hand, the user's private key is associated with a set of attributes composed of any number of describable attributes. On the other hand, when the data owner encrypts the plaintext, he assigns the access structure for decryption to the encrypted plaintext. Therefore, the standard of decrypting ciphertext is that the set of attributes in the user's private key must satisfy the access control strategy in the ciphertext, otherwise it can not be decrypted.

Combining ABE algorithm with RBAC model: The overall framework flow and calculation formula of ABE algorithm are basically unchanged, and several concepts are replaced according to RBAC model. Here the data owner is the access control system of cloud storage platform, plaintext M is the role document R corresponding to each role, and the content of the document can be the authority corresponding to the role. The access structure T is the role's access structure. User, attribute set I and generated user private key SK are consistent with the original algorithm. In this way, when the user tries to decrypt the encrypted role document with his own private key, if the set of user attributes meets the requirements of the role access structure, the user decrypts successfully and automatically obtains the rights contained in the role document.

Firstly, attribute/trust management module is added to the RBAC model, which adds attribute sets to users and access structure to roles respectively. Whether the user can own the role is determined by whether the user's attribute sets match the role access structure. In the ABE algorithm, whether the set of attributes in the user's private key matches the access control strategy in the ciphertext determines whether the user can decrypt the plaintext or not.

Then, the combination of ABE algorithm and RBAC model can automatically grant users and roles, and improve the confidentiality and security of data resources in micro-service environment. ABE algorithm encrypts the roles in RBAC model. In the process of encrypting, roles are embedded in the access structure, and users are given the private key associated with the set of attributes. In the subsequent access authorization process, the grant between users and roles can be automatically accomplished by encryption and decryption; the role is encrypted, that is, the corresponding permissions of roles are encrypted, which improves the confidentiality and security of data resources in the micro-service environment. Finally, the combination of ABE algorithm and RBAC model can achieve more fine-grained access control. Combining ABE algorithm, the concept of attributes is introduced into RBAC model, which makes the RBAC model access control granularity finer.

4. CONCLUDING
This paper presents an access control optimization model based on RBAC. By improving ABE to support RBAC model, existing RBAC users can directly access ABE encrypted data in microservices. Compared with the traditional RBAC model, the optimization model achieves dynamic access control authorization, automatic authorization of privileges and more fine-grained access control, improves the expression ability of access policies, reduces computing overhead to a certain extent, and improves the security and operational efficiency of micro-services.

REFERENCES
[1] Martin Fowler, James Lewis. Microservices[J]. 2014.
[2] Docker [EB/OL]. https://www.docker.com/what-docker, 2016.
[3] H. Shen and F. Hong, “A survey of access control models,” Computer application research, 2005, 22(6):9-11.

[4] J. Li, Q. Wang, C. Wang and K. Ren, “Enhancing attribute-based encryption with attribute hierarchy,” MONET, 16(5):553–561, 2011.

[5] M. Li and X. Yu, “Role based access control technology and its application,” Computer application research, 2000, 17(10):44-47.

[6] Bethencourt J, Sahai A, Waters B. Ciphertext-Policy Attribute-Based Encryption[C]//IEEE Symposium on Security& Privacy. IEEE Computer Society, 2007.