Research on Trust-Role Access Control Model in Cloud Computing

Yuchen Wu
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, 710032, China
e-mail: 1127787176@qq.com

Pingping Liu
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, 710032, China
e-mail: 1341369601@qq.com

***Abstract*—In order to ensure the security of data in cloud computing, a trust-role-based hybrid cloud computing access control model is proposed based on the combination of role-based and trust-based access control models. The model introduces the calculation of trust based on the role-based access control, that is, the user needs to verify the trust value in order to obtain the permission to access the data. Through the application in the local business system, it shows that the model can effectively solve the user's legitimate access to the data in the cloud, that is, to protect the security of the data in the cloud. The trust-based access control model has good advantages in terms of system throughput and storage space. As the number of user requests increases, both access control methods increase significantly in terms of throughput, but when the number of user requests reaches 10, the system throughput of both access control methods decreases, but based on trust - The role's access control method is always larger than the role-based access control method in terms of throughput, which roughly increases the total amount by about ten percent.**

Keywords-Cloud Computing Access Control; Data Security; Trust Value

I. INTRODUCTION

Cloud computing[1] is a commercial implementation of distributed processing, parallel processing, and grid computing development; its main features are large scale, virtualizable, high reliability, high scalability, and on-demand services. In a cloud environment, various resources are dynamically connected to the Internet, users can not only apply for services, but all participants in the cloud environment can dynamically join or quit[2]. However, with the popularization of cloud computing, cloud computing service security failures occur frequently, and the cloud security issues involved are increasingly prominent. For example, data stored in the cloud makes users have no absolute control over it, and cannot guarantee data integrity and confidentiality. Sex, and cloud service providers have some degree of untrustworthiness, etc., and this potential data security problem constrains cloud computing. Development in archival data management, and access control is one of the main means to solve data security problems.

By studying several traditional access control methods, this paper introduces the concept of subject trust in the role-based access control method, and proposes a hybrid access control method based on "trust-role". The experiment proves that the method is to a certain extent. It can improve the credibility of the system, reduce the probability of task execution failure and spoofing, effectively solve the access of illegal users to resources and the unauthorized access of legitimate users, and ensure the integrity and confidentiality of data in the cloud.

DOI: 10.21307/ijanmc-2019-050

II. TRADITIONAL ACCESS CONTROL

A. *Autonomous Access Control and Mandatory Access Control*

Autonomous access control[3] is an access control policy based on subject authorization. This method is autonomous, but it makes the authority of the subject too powerful and the security level of the system is low. In the mandatory access control, the system's main body and object are given certain security attributes by the system administrator, and the subject cannot modify its own security attributes. However, its lack of flexibility and lack of consideration for authorization management are generally not used in large distributed environment systems.

B. *Role-Based Access Control Method*

In the role-based access control (RBAC) model, the concept of “role” is introduced[4]. The main idea is to separate the subject from the object. The access rights are not directly directed to the subject and the object, but are assigned to the role. This “user-role-privilege” relationship makes the access control method more flexible. However, as the number of roles increases, the relationship between the roles becomes more complicated, which reduces the security of the system in the case of affecting system performance. Furthermore, this passive security model is not well suited for distributed environments[5].

III. HYBRID ACCESS CONTROL BASED ON "TRUST-ROLE" MODEL

A. *Introduction of Trust*

Trust[6] is an assessment of the identity and activity of the subject and the activity in the system, and is closely related to its own reliability and integrity. Based on the role-based access control model, the concept of “trust” is introduced. When the subject tries to access the object resources, not only the role verification but also the trust value is calculated. System data is made more secure by trust and role double-layer verification.

The acquisition of trust value[7] mainly has three aspects: direct trust degree, recommendation trust degree and historical operation trust degree. The direct trust degree is obtained through the subject's identity verification and user authority. The recommendation trust degree is mainly based on other subjects and object resources. The recommendation information is calculated, and the historical operation trust degree is the behavior record accumulated by the subject in the historical access to the object resource process.

B. *Basic Concept Description of the Model*

Definition 1 Entity User: Access data in a cloud computing environment. The subject of the resource, recorded as U;

Definition 2 Role: The role is equivalent to the employee in the actual enterprise Role, recorded as R;

Definition 3 Trust degree: Trust degree is the degree of trust of the subject to other subjects. In this model, the value of trust is [-1, 1]. The greater the trust value, the higher the access rights of the subject;

Definition 4 Access rights: The power of the subject to access the system data resources. Depending on the role assigned to the subject, the subject has different permissions;

Definition 5 Credibility threshold: The credibility threshold is a fixed value defined. When determining the trust value of an entity user, it needs to be compared with the minimum trust threshold. If the current trust value of the entity user is greater than the minimum trust threshold, then The next step can be accessed, otherwise, the access cannot be continued;

Definition 6 Session: A session is an event process that is triggered when an entity user activates a role they own. The real user can activate multiple roles in one session, denoted as S.

C. *Calculation of Trust Values*

In a cloud computing environment, when a principal user requests a resource access, the credibility management center shall calculate the credibility of the user. In the calculation, if the credibility is greater than a certain credibility threshold, the authorization center can assign the corresponding role to the user, and the user can access the object resource.

In this model, trust includes: direct trust recommended trust and historical operational trust.

1) Direct trust (DT)

The acquisition of direct trust is calculated based on the identity verification and user rights of the subject and the environment information; When the user logs in to the system for the first time, the system administrator must provide his or her identity information and environment information. The system administrator will calculate the direct trust of the user based on the information. The formula is:

$$\mathrm{DT} = \frac{\sum \mathrm{R(i,s)}\cdot\alpha + \mathrm{R(p,s)}\cdot\beta + \mathrm{R(e,s)}\cdot\gamma}{\alpha+\beta+\gamma} \tag{1}$$

Where R(i, s), R(p, s), R(e, s) are the correlations between the identity information, rights, environmental information and system security of the entity user determined by the security administrator, respectively, α, β, γ is the weight of identity information, authority, and environmental information in direct trust.

2) Historical operation trust (HT)

Historical operational trust is a record of behavior accumulated by the subject user during historical access to the guest resource. The access of the main user to the resource is divided into normal access and abnormal access. A normal access is an access request that meets a system security rule that is filed within a specified time period, while a non-normal access is an access request that violates a system security rule that is filed within a specified time. When the user is performing normal resource access request behavior then the user's historical operation trust is improved, and the historical operation trust is reduced. Its calculation formula:

$$\mathrm{HT(U)} = \frac{\sum_{i=1}^{n} \mathrm{H(m,i,t)}\cdot \mathrm{vi}}{n} \tag{2}$$

Where H(m,i,t) is the trust value of the access of the subject user m to the guest resourceiat time t . vi is the definition coefficient for this access.If it is a normal access, vi takes a positive value, and if it is an abnormal access, it takes a negative value.

3) Recommended trust (RT)

The recommended trust degree is the recommended trust degree of the main user to other main users. Generally, the recommendation trust degree of one user to another user can refer to the recommendation trust degree of other users. Its calculation formula:

$$\mathrm{RT(U)} = \frac{\sum_{i=1}^{n} \mathrm{S(m,q)}^{i}\cdot \mathrm{D(m,q)}^{i}}{n} \tag{3}$$

Where S(m,i)i is the degree of satisfaction of the entity m with respect to the entity n at the ith operation, and D(m,i)i is the score of the entity m for the entity n at the ith operation.

4) Calculation of final trust (FT)

The ultimate trust is the direct trust available based on previous calculations. The sum of the degree of trust in the historical operation and the recommended trust degree, the weights of the three trust degrees are WDT, WHT, WRT, and the sum of the three weights is equal to 1. The final trust is calculated as:

$$\mathrm{FT(U)} = \mathrm{W_{DT}DT(U)} + \mathrm{W_{HT}HT(U)} + \mathrm{W_{RT}RT(U)} \tag{4}$$

D. Trust-role-based access control algorithm

When the user makes a request to access the resource, the cloud computing authorization center creates a session S for the subject user by verifying the information of the subject user, establishes a trust relationship between the system and the subject user U, and calculates the trust degree of the subject user U, the subject user. U Select the role to be activated in this session. The system applies the credibility of the user U to the access rights of the role according to the trust constraint conditions, and obtains the current effective access rights of the subject user.

The specific algorithm steps are as follows:

1) When the entity user needs to access the resource, first submit the account and password that he has logged in and the data resource that needs to be requested to the cloud computing authorization center;

2) The cloud computing authorization center checks the information submitted by the entity user, determines whether to establish a session, and if so, establishes a session between the system and the user, and forwards the information submitted by the user to the cloud computing role database;

3) The cloud computing role database determines the role that the user needs according to the information sent by the authorization center, assigns the role to the user, and forwards the information to the cloud computing trust value database;

4) The cloud computing trust value database determines whether to grant the authority to the role assigned to the user according to the current trust value of the user. If the current trust value of the user is greater than a predetermined minimum threshold, the authority is given, otherwise Reject and return this information to the Cloud Computing Authorization Center;

5) After the cloud computing authorization center saves the information of the cloud computing trust value database, it will return an authorization success certificate to the user, and the user can carry the authorization success certificate to access the resource database. After the resource database is checked, the user can access the information. Data resources that need to be accessed;

6) After the conclusion of the meeting, users and sources shall evaluate the satisfaction of the parties and submit the results to the trust value database for calculation and update of the trust value.

IV. BASED ON THE "TRUST-ROLE" ACCESS CONTROL MODEL APPLICATION

Aiming at the security problem of cloud environment, this paper introduces the trusted mechanism into the traditional access control mode, proposes the access control model based on trust-role, and conducts experiments in the local business system.

The cloud platform is built through Hadoop architecture. Firstly, the local database is migrated to the distributed data base HBase, and then the access control model is applied in the local business system. In other words, the user's identity, credibility and other information are verified at the same time. Finally, the advantages of this model in system throughput and data storage cost are obtained through simulation experiments.

A. Construction of hadoop cloud platform

1) Install Linux virtual machine

Install the VMware Workstation10 and install the Linux virtual machine. The Linux system is ubun-tu12. 04.

2) Install JDK

Install the JDK - 6 u43 - Linux - i586. Bin, and set its environment variable.

3) Configure SSH password-free login

Installation command:$ sudo apt-get install ssh

4) Install hadoop, zookeeper and hbase

Take hadoop-1 separately. 2. 1. The tar. Gz, the zookeeper - 3. 4. 6. The tar. Gz, hbase - 0. 94. 26. The tar. Three files of gz are decompressed and put into the target document folder, then the environment variables of Hadoop are configured, and the configuration files of Hadoop, zookeeper and hbase are modified respectively.

B. Application of the model in local business systems

1) System flow chart shown in Figure 1

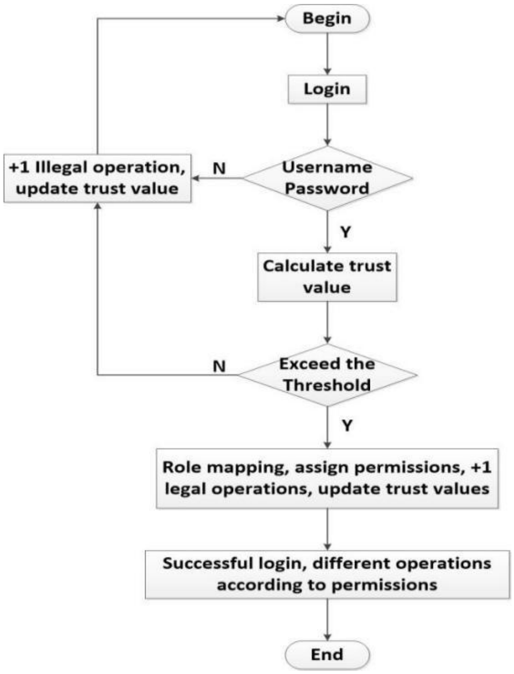
Begin
Login
Username Password
N
+1 Illegal operation, update trust value
Y
Calculate trust value
Exceed the Threshold
N
Y
Role mapping, assign permissions, +1 legal operations, update trust values
Successful login, different operations according to permissions
End

Figure 1. Business System Flowchart

2) System user login processing

The user to enter your login account and password, login request to the server, the server receives the request, after looking for value table with a table and trust, and find the attribute information, the user first line into the user name and password match, if the match is successful, by the trust of the user ID to find its corresponding value, through the three kinds of trust value calculated finally trust value, compared with the threshold of system setting, if not smaller than the threshold, through carries on the Angle of color reflected beam, root, according to the Angle of color not to grant to the users of different operating as xu can, And the number of interchanges will be increased by 1, the new user's trust value; If it fails, the user is unable to log in, and according to the user ID, the number of non-normal operations is increased by 1, and the new letter value is obtained. The user login interface is shown in figure 2.

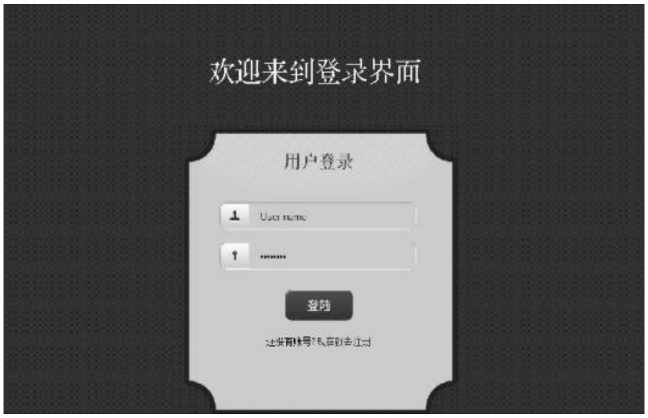

Figure 2. business system login interface

C. Simulation experiment

Simulation experiments mainly compare the access control model based on "trust-role" and the access control model based on role from the aspects of system throughput and data storage cost. See figure 3 and figure 4.

Figure 3 shows the storage space comparison required for the two access control methods to store access control information, indicating that the amount of storage space required for the trust-based access control method does not increase significantly as the number of users increases.

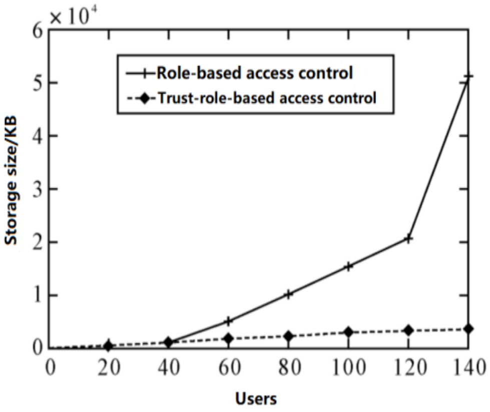

Figure 3. storage space comparison chart

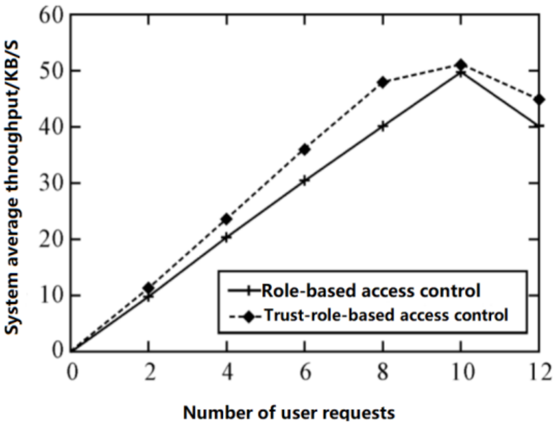

Figure 4. System throughput comparison chart

Figure 4 shows a comparison of the system throughput between the two access control methods, showing that both access control methods increase significantly in throughput as the number of user requests increases. However, when the number of user requests reaches 10, the system throughput of both access control methods is decreasing, but the trust-based access control method is always larger in throughput than the role-based access control method.

V. CONCLUSION

This paper adds the concept of credibility to the traditional role-based access control model, and proposes a hybrid-access-based hybrid access control model in cloud computing. This model makes up for the shortcomings of role-based access control methods. Experiments show that this model has great advantages in system user authentication, and the trust-based access control model has good advantages in system throughput and storage space.

ACKNOWLEDGMENT

New Network and Inspection and Control National Local Joint Engineering Lab. Fund Project (GSYSJ20170009)

http://www.ijanmc.org

REFERENCES

[1] Li Qiao, Zheng Xiao. Summary of the status quo of cloud computing research [J]. Computer Science, 2011, 38(4): 32-37.

[2] Chen Quan, Deng Qianni. Cloud computing and its key technologies [J]. computer application,2009, 29 (9): 2562-2567.

[3] Long Qin, Liu Peng, Pan Aimin. Role-based extension manageable access control model research and implementation [J]. Computer Research and Development, 2005, 42(5): 868-876.

[4] Luo Xueping, Zheng Yuli, Xu Guoding. An extended role-based access control model [J]. Computer Engineering, 2001, 27 (6): 106-107.

[5] Liao Junguo, Hong Fan, Xiao Haijun, et al. Fine-grained role-based access control model [J]. Computer Engineering and Applications, 2007, 43(34): 138-140.

[6] Deng Yong, Zhang Lin, Wang Weichuan, et al. Research on dynamic role access control based on trust degree in grid computing [J]. Computer Science, 2010, 37(1): 51-54.

[7] Lin Qingguo, Liu Yanbing. A trust-based dynamic access control strategy [J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2010, 22(4): 478-482.