A Security Architecture Research Based on Roles

Linbo Tao[1,*], Jianjing Shen[1], Bo Liu[2]and Zhenyu Zhou[1]

[1]School of Arts and sciences, Information Engineering University, Zhengzhou 450001, China
[2]Shenyang NanChang High School, Shenyang 110002, China
[*]Corresponding author: taotlb@126.com

Abstract. Security has always been the top issue against the cloud computing, scientific security architecture is the foundation of other security technologies. Comparing existed cloud computing security architectures and traditional security architectures, there are some common ground and new problems. In cloud computing environment, different users need different security requirements, so if we can assign them reasonable authority, there will be great efficiency improvement for data security and system efficiency. Role is an authority division and management method, it gains very good effect for its classification to user and data operations. Inspired by this, a security cloud computing architecture based on role has been designed, the security of the architecture has been evaluated at last.

1 Introduction

Cloud computing is a type of service that service vendors provide different types of services by a cluster of servers through networking, such as online software services, hardware rental, data storage, calculation etc [1]. These resources or services are supplied as the way of water or electricity which only to be paid according to the amount you actually used [2].

The biggest advantage of cloud computing is the elasticity of supply and low cost, the biggest obstacle is data security[3]. The security issues include the risk of privacy leakage and data abuse led by remote data storage, data tampering, lacking of censorship on the service provider, imperfect verification mechanism on user login check. For the data actually controlled by service providers, users have no rights to develop specifications on data management and security measures. So the cloud services providers and academia have designed a variety of security cloud computing infrastructure to maximize the security. These architectures should consider the practicality and scalability besides security.

Role is a collection of certain number of privileges. It refers to a collection including resources accessing and appropriate operating permission to complete a task. As an agent layer between user and authority, role is expressed as the relationship between authority and users. All authorities should be given to roles rather than directly to a user or group.

So a security cloud computing architecture based on roles is supposed on the following. The architecture will compares existing cloud computing security architectures first, then analyzes characters of roles, including authority division, security requirements division, the security of the architecture will be evaluated at last.

2 Security Model and Architecture

Cloud computing is the integration results of distributed computing, parallel computing, utility computing, network storage, virtualization, load balancing, hot standby redundancy and other traditional computer and network technologies[4]. It has a hierarchical structure, each level involving a wide range of properties and security issues.

Santos et al has proposed and designed a trusted cloud computing platform, TCCP, including a series of trusted nodes (N), trust coordinator (TC), untrusted cloud manager (CM) and external trust entity (ETE) etc. Wherein TC is maintained by a specific external trust entity (ETE) [7]. TCCP secures guest virtual machine by providing a closed box operating environment, it also allows users to test and verify the security.

The advantage of this architecture is to fundamentally solve the security issues of cloud computing architecture, the disadvantage is the excessive dependence on hardware which is contradictory with compatibility and cheapness of cloud computing. Another security architecture is based on isolation which can achieve data and operation isolation from hardware and software, it isolates multi-tenants data efficiently to a certain extent and has certain maneuverability.

Currently Cisco, VMware and other software, hardware providers have put forward their own isolation scheme, the core idea is to achieve logical space and level division through appropriate technologies which can isolate services provided to users. But this scenario is still high dependence on hardware and high cost.

Security as a service based SOA draws lessons from concept of SOA, it takes and packages security as services, different user can choose different services according to their needs. The classical SOA security architectures are IBM , EasySaaS security architectures.

3 Security Architecture Based on Roles

Sharing property of cloud infrastructure always give users the illusion that data is easier to lose when they are stored in the cloud. In fact, the overall technical architecture of cloud computing provides centralized management by security experts can achieve more security objectives[8] than the decentralized management of individual and non-professional management .

It is different from traditional security architecture who emphasizes border protection. The cloud computing divides logic isolation instead of physical border protection when different users applying their services[9]. But there are similarities between the two architectures on corresponding levels. Fig.1 has shows the comparison between cloud security architecture and traditional security architecture.

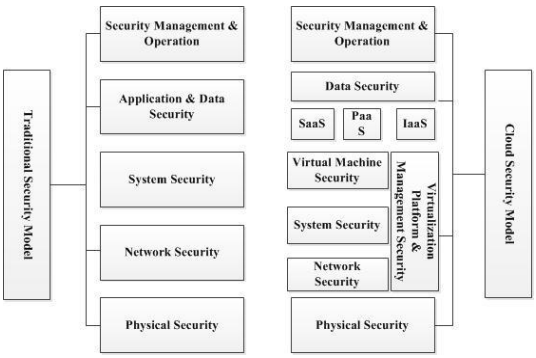

Fig.1. Comparison between cloud security and traditional security

The results show that cloud computing has introduced virtualization technology who change the service model, but not overturn the traditional security model. Cloud computing security and traditional security have the same security objectives, system resource type, basic security technologies. The cloud computing has its own specific security issues, including virtualization security and security issues about cloud computing sub-service model[10]. Generally speaking, cloud security is the inheritance and development of traditional security in a cloud computing environment. They are substantially similar in the level of security classification.

In cloud computing environment, cloud computing need to incorporate virtualization security precautions, due to the introduction of virtualization technology. In the basic level, sophisticated traditional security technologies can still provide security [11].

3.1 Security Architecture Design

Trusted security architecture and isolation architecture have good security, but poor extension. SOA architecture is flexible, but lack of clear secure margin [12], its level of responsibility is not clear enough.

In order to find a secure cloud computing management structure with both flexibility and security, user management and rights assignment should be the key. The concept of role has many good applies in rights management. Such as roles management in database are much successful in categorizing users, unifying licenses and unifying management. The concept of group in windows operating system is a role management too. Roles represent a class of users with same rights. Certain role has a set of certain rights.

The advantage role management is that designers can focus more attention on division of authority without concerning for someone specific. When the members of role changed, the content of role can still remain unchanged. In the cloud computing environment, the main bodies include cloud service providers, users, distributed hardware and software applications. The cloud service providers are responsible for providing hardware and software services to users and ensuring their data security. Users pay for their actual amount of consumption and storage.This mode allows data separated from the control of their owners, so its the actual reason why users would not save their data in the cloud.

In order to help users actually control their data, we must think more on rights assignment. If rights of cloud service providers and users are clear, they will get their own role, users will trust cloud computing more for their actual control of their data[13].

Here we divide the roles according to storage, data management, data ownership and cloud service providers. Combining with the cloud computing security architectures above and comparing with the traditional security models, a cloud computing security architecture based on roles has been proposed. as figure 2

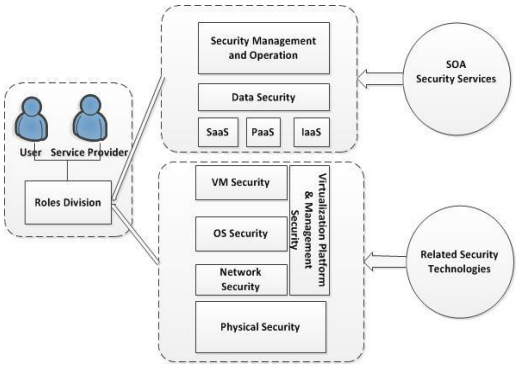

Fig.2. Security Cloud computing architecture based on roles

From the perspective of roles, cloud service providers are only the role that data kept in them, they are not the data owners and managers. The data owners are the only manager of their data who have all rights to their data management. Other users must be authorized by the user if they want to access his data. Any other users can not grasp the actual content of his data without his authorization, so data owner is the only administrator of his data.

3.2. Roles Division and Rights Assignment

Here roles are divided into four types including service provider, data administrator, inspector and user. The relationship among the four types are service providers build cloud environments and provide services, accept service requests, save

data, recycle resources, user apply services and manage his own data, he is only the administrator of his own data, but users to others.

Let any user is u_i, his corresponding data set is D_i, rights set is F, $F = \{f_1, f_2, \cdots f_n\} \to \{\text{copy}, \text{delete}, \cdots\}$, each f_i corresponds a operating authority, such as moving, delete, encryption, copying etc. $f_i = 0$ represents illegal operation, $f_i = 1$ represents legal operation. The four types of roles above are the subset of F, let them as F_p, F_a, F_i, F_u.

Let user u_i and u_j get the F_a role to their own datasets D_i, D_j after they apply cloud services successfully. To each $f_a \in F_a$ there is

$$u_i(D_i) \xrightarrow{f_a} true \tag{1}$$

$$u_j(D_j) \xrightarrow{f_a} true \tag{2}$$

$$u_i(D_j) \xrightarrow{f_a} false \tag{3}$$

$$u_j(D_i) \xrightarrow{f_a} false \tag{4}$$

That is only the user itself has the F_a role to his data, other users do not have the role. To the service provider, role p_i and inspector role s_i, they do not have the F_a role, so they don't have rights to operate users' data, that is $F_p \cap F_a \cap F_i = \phi$.

Because of the openness of the cloud, the user can not only operate their own data, they need to share other users' data or share their data with others. But the sharing degree depends on the authority degree they get or give. The user get authority having the role F_u, they can get part or all rights of administrator, this depends on the authority degree by the administrator, so F_u is the subset of F_a. To any data d_i, $d_i \in D_i$ of user u_i, the operation authority relationships is shown as table1.

the relationship of roles and authorities

Table 1. Roles and Authority

roles \ authorities	F_p	F_a	F_i	F_u
Service provider	1	0	0	0
administrator	0	1	0	1
inspector	0	0	1	0
user	0	e	0	1

From table1, we can see the roles have no operating authority overlapping except administrator and user, this approach is more conducive to ensure the security of data. For data those role F_u has rights to operate, the role F_a certainly have rights to operate them. In turn, the data operated by role F_a do not mean they can be operated by the role F_u unless they get the authority by role F_a. So the role value of F_u is e, $e \in \{0,1\}$, when the role get the operating authority $e=1$,else $e=0$.

In order to ensure the authenticity and legality of the operation among administrators, authorized users and service providers, a trusted third party as an inspector is needed to monitor the operation of the other three roles. The content of monitoring is the authenticity check and operation rights test. The role of inspector has no operating authority to data, but they has the rights to limit some unusual or dangerous operation operated by administrator or user, then give user a warning or terminate the dangerous operation.

The authenticity check is judged by the integrity and the user's operation records. If the user's identification information is incomplete, no logical association with the identification information or the reservation information is incorrect. When the unauthorized operation or dangerous operating application appearing, the role F_i will strictly control the user's service request and give a risk warning to the corresponding role F_a timely. Each broken access trying of roles F_p, F_a, and F_u will be recorded so that to facilitate judging the safety level of this operation trying by tracking their operating locus. The relationship among the four roles are shown as figure 3.

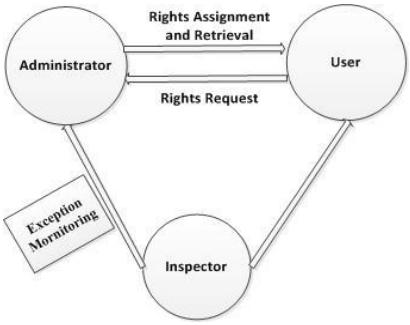

Fig.3. Relationship between roles and authority

4 Security analysis

Considering the complexity and cost of evaluation, the mathematical analysis is undoubtedly the most convenient and efficient methods[14]. The following is the security analysis procedure of cloud computing security architecture based role division.

Comparing to the previous architectures, the security architecture based role division has more clearer levels and responsibilities [15]. So we compare them from the angle of having roles division and without roles division. The architecture with roles division has the four roles F_p, F_a, F_i, F_u, and F_u is the subset of F_a. We can regard sets F_p, F_a, F_i as three vector spaces. Respectively take any sequence $A=\alpha_1\alpha_2\cdots\alpha_n$,

$B=\beta_1\beta_2\cdots\beta_n$, $C=\gamma_1\gamma_2\cdots\gamma_n$ from the three vector spaces, there are $\vec{A}\bullet\vec{B}=0$, $\vec{A}\bullet\vec{C}=0$, $\vec{B}\bullet\vec{C}=0$,

This shows the three spaces are orthogonal, so the vectors correspond to a series of authorities, the orthogonal vectors means the their vector spaces have no crossover authorities. But to any two operating series $\Gamma=\delta_1\delta_2\cdots\delta_m,(\delta_i\in F)$, $\mathrm{X}=\chi_1\chi_2\cdots\chi_m,(\chi_j\in F)$, in the architecture without roles division, there are not always $\Gamma\bullet\mathrm{X}=0$, so there are the danger to users that they may face operation without authority.

Through the analysis above, two objects u_i,u_j both have the role F_a, they will be closed to their data operation, so the Cartesian product constituted by different users and their data are orthogonal, that is $(F_a\times D_i)\perp(F_a\times D_j)$,the unauthorized probability is $P(f_i\times d_j)=0$.

In the architecture without roles division, any data $d_i, d_i\in D_i$, its owner is u_i, but d_i is stored in the remote place, so the service provider p_i becomes to the actual administrator of d_i, if p_i is untrusted, the dangerous probability to d_i is $P(d_i)\geq\frac{1}{2}$, because the architecture is lack of role F_i, user u_i can not get unauthorized operation of d_i or unauthorized operation can not be terminated timely.

If p_i is trusted, but without roles division, p_i is the actual administrator of d_i, so there are probability that p_i authorize the operating authority of d_i to other users. So the worst unauthorized operating probability of d_i is $P(d_i)=\frac{1}{2}P(u_j)$, $P(u_j)\leq\frac{1}{2}$, $P(u_j)$ is the probability of p_i authorize other users to operate d_i without the permission of u_i. The probability under the condition with roles division will be $P'(d_i)\leq\frac{|D_i|}{\left|\sum_{i=0}^{n}D_i\right|}$, and $P'(d_i)$ will be smaller along with increasing of data scale.

From the analysis above we can see architectures without roles division would likely to be confusion on authorization between data owners and those sharing the data or the condition that attackers get the authority of service providers. The attackers can do illegal operation and further damage penetration after they illegally obtain the service providers authority. But under the architecture with roles division, the attackers can only get one role, so they can't do more harm to others data. It shows that the architecture with roles division can bring higher security.

5 Conclusion

Existing cloud computing architecture and security model have been summarized and compared to the traditional security structures in this thesis. A cloud computing security architecture based on roles division has been proposed, the architecture combines the common characteristics with other cloud computing security architectures, divides their security levels more clearly, against the different authorities of different roles and their cooperation with each other, the data security and efficiency can work better.

References

1. Ashutosh Kumar Singh, Dr. Ramapati Mishra, Fuzail Ahmad, et al. A Review of Cloud Computing Open Architecture and Its Security Issues. International Journal of Scientific & Technology Research, Vol.6, No.1, 65-67 (2012)
2. Fei Hu, Meikang Qiu, Jiayin Li, et al. A Review of Cloud Computing:Design Challenges in Architecture and Security. Journal of Computing and Information Technology, Vol.1, No.19, 25-55 (2011)
3. Chen Ke-you, The Research On Data Security And Privacy Issues In Hybrid Cloud Computer. NanChang, JiangXi Normal University (2013)
4. Chi Li-ying. Research on Security Architecture of Cloud Computing and Its Key Technologies. Computer Development & Applications,Vol.6, No25, 20-22 (2012)
5. Zhang tao. The Cloud Computing Security Architecture Research Status Analysis Domestic and Foreign. Safety Broadcasting & Monitoring, No.11, 123-127 (2011)
6. JerichoForum. Cloud Cube Model:Selecting Cloud Formations for Secure Collaboration. Version1.0. www.JerichoForum.org (2009)
7. Lin Chuang, Su WenBo, Meng Kun,Liu Qu, Liu WeiDong. Cloud Computing Security:Architecture, Mechanism and Modeling. Chinese Journal of Computers,Vol.9, No.36, 1765-1781 (2013)
8. Sanjaya Dahal. Security Architecture for Cloud Computing Platform. Stockholm,Sweden:Master of Science Thesis (2012)
9. Muthu Ramachandran. Component-Based Development for Cloud Computing Architectures. Computer Communications and Networks,No.10, 91-114 (2011)
10. Masayuki Okuhara, Tetsuo Shiozaki, Takuya Suzuki. Security Architecture for Cloud Computing.Fujitsu Sci. Tech. J,Vol.4, No.46, 397-402 (2010)
11. Vic (J.R.) Winkler. Securing the Cloud:Cloud Computer Security Techniques and Tactics. Edition 1, Publisher: Syngress (2011)
12. Chen Chi,Yu Jing. Cloud computing security system. Edition 1, Science Press (2014)
13. Zhang Wei, Dong Qunfeng. Design and implementation of cloud security comprehensive analysis system. Computer Engineering and Applications, Vol.19, No.50, 89-94 (2014)
14. Dan Gonzales, Zeremy Caplan, Evan Saltzman, et al. Cloud-trust-a Security Assessment Model for Infrastructure as a Service(IaaS) Clouds. .IEEE Transactions on Cloud Computing. PP(99), 1-14 (2015)
15. Jinag Zheng-wei, Zhao Wen-rui, Liu Yu. Model for Cloud Computing Security Assessment Based on Classified Protection. Computer Science,Vol.8, No.40, 151-156 (2013)