Chapter 300
Improved Access Control Model Under Cloud Computing Environment

Yongsheng Zhang, Jiashun Zou, Yan Gao and Bo Li

Abstract With the development of cloud computing, cloud security problem has become a hot topic. Some scholars put forward the role access control based on mapping, which is used to solve the leakage problem of data storing in the cloud. This paper briefly describes the cloud computing and traditional access control model based on the latest research. Then the paper sums up the work and puts forward a new kind of access control model based on the hop named HBAC. It is based on the role access control that based on mapping. It is used to control the length of path to access the data in outer domain. At last, the paper gives the concrete steps to describe the principle of its operation in detail. And this paper makes a comparison with other related researches. Then this paper summarizes the advantages and disadvantages of HBAC.

Keywords Cloud security · Access control · RBAC · HBAC

Y. Zhang · J. Zou (✉) · Y. Gao
School of Information Science and Engineering, Shandong Normal University, Shandong Provincial Key Laboratory for Novel Distributed Computer Software Technology, Jinan 250014, China
e-mail: 1010336028@qq.com

Y. Zhang
e-mail: zhangys@sdnu.edu.cn

Y. Gao
e-mail: 15553109740@163.com

B. Li
Academic Affairs Office, Shandong Polytechnic, Jinan 250104, China
e-mail: 24874890@qq.com

S. Li et al. (eds.), *Frontier and Future Development of Information Technology in Medicine and Education*, Lecture Notes in Electrical Engineering 269,
DOI: 10.1007/978-94-007-7618-0_300, © Springer Science+Business Media Dordrecht 2014

300.1 Cloud Computing

300.1.1 Concept of Cloud Computing

The cloud computing has not been clearly defined up to now. Although the exact meaning of cloud computing has not yet been fully understood, everywhere is various related service. The understanding of this paper is: Cloud computing is a kind of service used for data storage and applications through the Internet and remote service center [1].

300.1.2 Cloud Security Issues

Under the cloud computing environment, users will not store their information data in their hard drives, but in the remote server data center [2]. Because of the change of data center from the client to the server, the data security of the server is very important. Therefore trusted cloud security technology is also developing rapidly. Many scholars have done research on the aspects of destruction and protection of data, such as the proposed Dissolver system [3].

300.2 Traditional Access Control Model

ISO, the international organization for standard proposed the hierarchical security architecture in the design standard of the security of network system (ISO7498-2), and defined five security services: authentication service, access control, data confidentiality, data integrity, non-repudiation service. As one of the five services, access control service plays an irreplaceable role in network security system [4]. Traditional access control models mainly include four types: access control matrix, Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role Based Access Control (RBAC) [5].

1. DAC increases the characteristic of “independent” based on access control matrix. Authorized subjects can give authority to other subjects. So it has strong flexibility.
2. MAC is mainly used in military application of multi-level security level. It defines the trust level as user proposed a request or access to the system. The system carries out the comparison, to determine if the access is legitimate.
3. RBAC introduces the concept of the role between subject and object [6]. A user associates with one or more roles, and the role associates with one or more permissions. The users can activate the corresponding role by logging on system to get the corresponding permissions.

At present, RBAC has been widely studied, the experts have put forward some models. For example, the RBAC96 and ARBAC97 put forward by George Mason university of America [7].

300.3 Improved Access Control Model

300.3.1 Division of Logical Domain

Under the environment of cloud computing, users' information are stored in the cloud server, including some private and confidential data. Therefore under multi-tenant environment, data security issues are very important. Here, the paper divides data center under computing environment into different security domains. Resource belongs to different companies or enterprise will be divided into different security domains, which we call the logical domain [8].

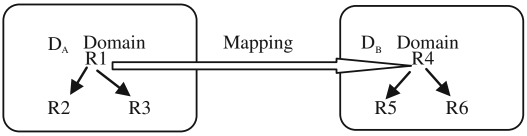
300.3.2 Hop-Based Role Access Control

In each logic domain, we use role-based access control model. But to establish the role, this paper adopts a Hop-Based Access Control (HBAC), to make the access in different logical domain a fine-grained limit. It will be described in detail below. For the roles in the logical domain, we record them as three byte R = {(Role, Domain, Hop)}.

300.3.3 The Mapping of Role Between Domains

Under the multi-domain environment, a subject of a security domain has no access to another security domain unless it can pass the permission check of the resource-requested domain. Only when it is cognized by the access control system and it has appropriate permission, the subject can have access to the resource in the foreign domain [9]. We use the role access control based on the mapping as the strategy to visit from one domain to another. The example is Fig. 300.1.

Fig. 300.1 Mapping diagram



300.4 The Defects and Improvements of Role Mapping

300.4.1 A Brief Introduction to the HBAC

To solve the problem of permeation of authority, the paper puts forward a kind of access control based on hop count (HBAC). Assuming the existence of A, B, C, D four security domain, four domain resources are expressed as O = {(Object, Domain)}.The roles are denoted as R = {(Role, Domain, Hop)}. And all the initial value of hop in four domains is set by 0. If B assuming that there is role mapping relation between B and C. Then there is role mapping relationship between C and D. When we want to establish mapping relationship between A and B, we can have fine-grained access control through the 'Hop' fields. Each value of hop should minus 1 if the role wants to visit resources in foreign domains. If its hop = 0, the access is rejected. Else, the value of hop will minus 1, and the visit will be permitted. So, it can prevent problem of penetration of authority.

300.4.2 The Disadvantages and Solution in the HBAC

Although the HBAC mechanism has fine-grained access control, there is also such a situation that when the value for the hop field of the role in A is assigned, we assuming it equals 2, the user have two choices at the moment. One is to continue visiting domain C which has mapping relationship with ask B domain. The other choice is that the user may withdraw from the B domain, and then visit B domain again. In all the situations, the Hop's value will minus 2. But users in the second case (we call it the inverse domain access) cannot visit the resources in C, which is contrary to our original intention. In addition, if different users need different hop value, the same role not be authorized to different users. Therefore, the HBAC mechanism requires strict restrictions on these problems. The solution is as follows:

1. All the initial values of hop are set by 0.
2. Establish a Mapping Hop (MH), table. The table only records the information of the roles which have mapping relationship. Common role won't be recorded into the table.
3. In the process of mapping of role (the role is visiting the resources in foreign domain), the access control system will check the hop's value in the MH table. If the user doesn't exist or the hop's value of the role is 0, then the visit will be turn down, and error will be returned. Otherwise the corresponding hop's value will minus 1, allowing the role mapping.
4. The users' information will be automatically deleted when the access is over. Users should be reauthorized if they want to visit again. We will cancel the users' information in the MH table once the user finishes his visit to the resource in foreign domain and return his own domain.

5. MH table needs to be established by the reliable system which is safe. It is effective only when the identity-authentications of both the cooperation units are given. And once the MH table is set up, it cannot be modified by the provider of cloud service himself.

300.4.3 The Process of HBAC

Access process:

Step 1: As the users in secure domain D_A, P and S want to obtain the authorization of RB_2 in D_B. We need to make restrictions that the user P can only visit the resources in D_A and D_B but not in D_C. The user S can visit the resources in D_B and D_C. When the P and S are authorized with role, we should modify the MH table. Create Row S(S, RA_1, 2); Create Row P(P, RA, 1);

Step 2: When S or P want to visit the resources in D_B, the access system will check them: if (S∧S→hop!=0){S→hop–;visit();}else{return ERROR;}

Step 3: After having visited the resources in the D_B, the result in MH table is as follows: Row S(S, RA_1, 1); Row P(P, $RA_{1,}$ 0);

Step 4: If P and S want more visits to the resources in D_C, then the S will have the access, the result being Row S(S, RA_1, 0) while the P will be turn down.

300.4.4 Advantages of HBAC Mechanism

The advantages of HBAC mechanism include fine-grained restrictions in access, avoidance of penetration of authority, saving more space compared with establishing the mirror role mapping to prevent penetration of authority, because the MH only records the information of users who has mapping relationship. So the needed space is very small. Secondly, the MH table is updated at dynamic runtime, which reduces the consumption.

300.5 Conclusions

Cloud computing can provide us with reliable and custom service and maximum utilization of resources. Cloud computing service will become popular in the future with its On-demand concept of service. The paper puts forward an improved mechanism based on the analysis about access control model. We believe that the cloud computing service will improve step by step. In the end, it will become a kind of service without any menace from the “rear”.

Acknowledgments This research was supported by Natural Science Foundation of Shandong Province of China under Grant No. ZR2011FM019 and Postgraduate Education Innovation Projects of Shandong Province of China under Grant No. SDYY11117. It was also supported by the Project of Shandong Province Higher Educational Science and Technology Program under Grant No. J12LN61. In addition, the authors would like to thank the reviewers for their valuable comments and suggestions.

References

1. Fauzi AAC, Noraziah A, Herawan T, Zin NM (2012) On cloud computing security issues. In: Pan J-S, Chen S-M, Nguyen NT (eds.) Paper presented at the 4th asian conference on intelligent information and database systems. Berlin, Heidelberg
2. Zou J-S (2012) Security problems and its countermeasures in the cloud computing environment. CD Comp Softw Applicat 35–37
3. Zhang F-J, Chen J, Chen H-B, Zang B-Y (2011) Data privacy protection and self destruct in cloud computing. Compute Res Develop, 1155–1167
4. Li H, Li H (2010) Trusted cloud security key technologies and realization. People's Posts and Telecommunications Press, Beijing
5. Han D-J, Gao J,Huo H-L, Li L (2010) Progress of access control model research. Compute Sci, 29–33
6. Sandhu R, Coyne EJ (1996) Role based access control models. IEEE Compute, 38–47
7. Zou X (2006) Analysis and implementation of role-based access control model. Info Microcompute 108–111
8. Tan X (2011) Cloud computing environment access control model. Beijing Jiaotong University, Beijing
9. Zhang D-Y, Liu L-Z (2008) Multi-domain access control model. Compute Applicat, 633–637