Fine-grained AR-UCON Model Based on Time Constraints under Cloud Computing Environment

Sun Yuejiang[1, a *], Qi Chunxia[2,b]

[1]Department of Information Engineering, Qingdao Institute of technology, Qingdao,266300, China

[2]Department of Information Management, Shandong Foreign Trade Vocational College, Qingdao,266071, China

[a]116339822@qq.com, [b]qichunxiasdut@163.com

Keywords: usage control; authorization; time constraint; role ; fine-grained

Abstract. Traditional access control technologies are not well adapted to cloud computing environments. Usage Control (UCON) model is featured with attribute variability and decision-making continuity, which means advantageous in the new environment. But UCON model is highly abstract and difficult to apply. For better solutions, this model was improved in this paper. Roles and time constraints was added to UCON model. So, the model was extended to a new model: AR-UCON model, which was proved to achieve a fine-grained access to resources under cloud computing environment.

Introduction

In nearly 50 years of development history, some access control model like discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC) have been greatly developed and applied. These access control models have mainly focused on unused data authorization protection in the closed system, but not well adapted to the current open system environment or achieve dynamical authorization [1]. Compared with traditional environment, cloud computing environment require higher level for fine-grained access control and massive user dynamic extension. The access control problem is particularly prominent.

Usage Control model

In 2002, Park.J and Sundhu.R proposed the usage control(UCON) model and in 2004, they gave the model's complete formal definition and the core model named $UCON_{ABC}$. The model is mainly composed by subject, object, authorization, obligation and conditions etc... Sandhu et al proposed $UCON_{ABC}$ model on the basis of UCON, which has eight core components with subject, subject attribute, object, object attribute, right, authorization, obligation and conditions [2,3]. The model is as shown in Fig. 1.

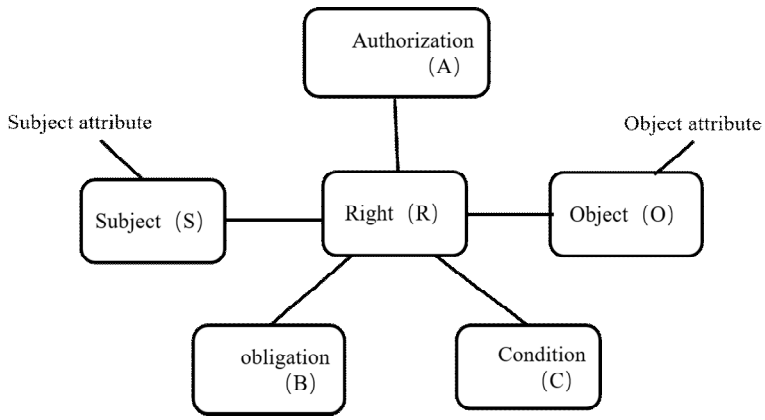

Fig. 1 $UCON_{ABC}$ Model

$UCON_{ABC}$ model has many advantages [4]. It contains traditional access control model, has wider range of applications as well as meet the needs of different access control systems and achieve a variety authorization management. When it's used for the cloud computing environment, the main advantage of UCON model is the authorization continuity and attribute variability. As shown in Fig. 2.

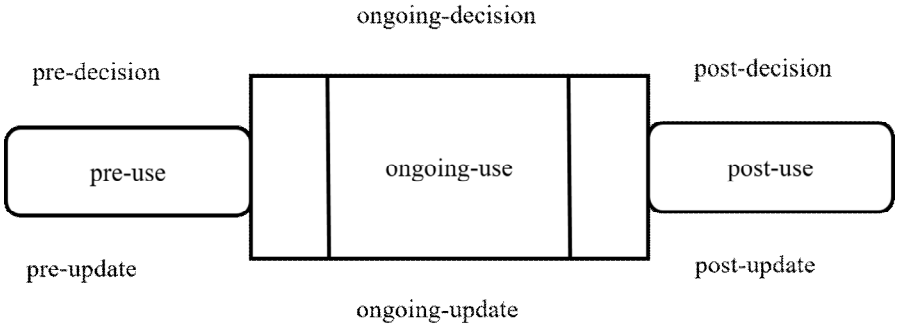

Fig. 2 Variable attributes and continuous control

Cloud computing usage control mode Based on attributes(AR-UCON)

Attribute-based access control model can describe RBAC roles with attributes. Meanwhile, the role can be a new attribute added to the usage control model. UCON takes in the extended attributes as model factors, achieving dynamic management and user privileges allocation. The model stands on the traditional model with factors of authorization, conditions and obligations, and then considers a new decision factor, the role of a delegate. The rights of the role are restrained by access control rule and conditions. The subject achieves the appropriate authorization rules by obtaining the corresponding role in hierarchy structure.

By changing the attributes of subject and object, the authorization rules would be affected. The model could achieve assigning roles and dynamic changes of authorizing. As shown in Fig. 3.

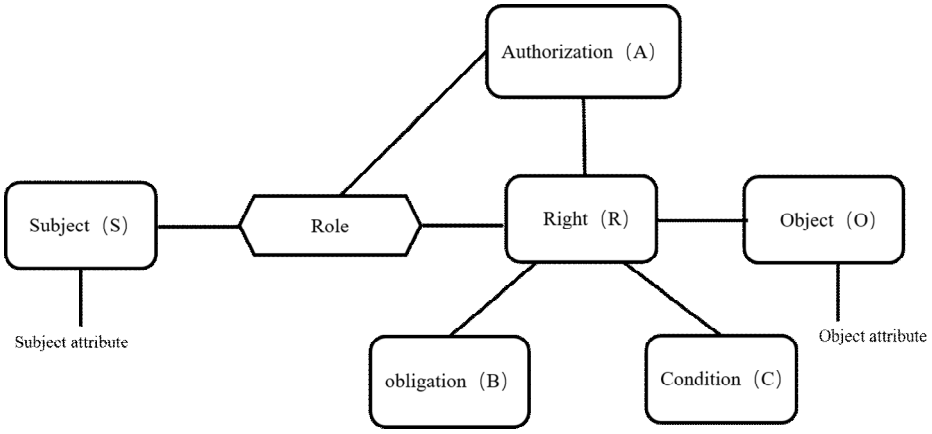

Fig.3 UCON Model with role attributes

In this model, authorization is not only related with subject, object, authorization rules, conditions and obligations, but also dynamically related with the roles. Firstly, the subject got the role and perform access control operations. The rights of role are activated. Then, when the access control was operated, the properties of subject and object would be dynamically updated accompanying with the changing of authorization rules and roles assignment.

The traditional $UCON_{ABC}$ model could be divided into 16 child models depending on the determinants and attribute update period. By combining the various sub-models, the UCON model can achieve a variety of different control mechanisms [5]. In our AR-UCON model, the addition of the role hierarchy and delegate element contributed to the extension of two child models. The elements of authorization, obligations and conditions are still included same as the original model. But two fine-grained models were added based on delegate elements. So the model was extended by

pre-delegate attribute updating model (AR-UCONpre) and ongoing-delegate attribute updating model (AR-UCONon).

Formal Description of AR-UCONpre

Basic definition: Subject set is symbolled with S; Object set is symbolled with O; Subject attribute is symbolled with SA; Object attribute is symbolled with OA; Role is symbolled with R; privilege is symbolled with P; Delegate attribute is symbolled with D; The delegate role is symbolled with DR. The description "authorize (r, p) -> {true, false}" determine whether permission P was granted to role R; The description "grant (rs) {true, false}" would determine whether the subject S has a role R.

Delegate Description: The description "PRE GA (SA, G, OA, P)" is used to describe whether to grant the commission after receiving other subject's attribute delegate. The description "pre GR (R, RD, OA, P)" is used to determine whether to grant the permissions after receiving other subject's role delegate.

In the delegate model, the delegate attribute as well as the role are the two basic factors for prior authorization decisions.

The description "Allowed (s, o, r) => contain (s) ≧ pre (o, r)" [6], represents if the subject request the commission meeting pre-delegate function and have role contains permissions, the authorization to objects can be granted.

The description "Update (D, SA)" expresses the updating function for the main attribute after attribute were delegated and "Update (R, SA)" expresses the updating function for the main attribute after the role was delegated.

Formal Description of AR-UCONon

AR-UCONon is the on-going delegation model. That is, when the subject access to the resources, it gets the commission. The grant is judged in the course of the visit. If the ongoing access operation is no longer meet the corresponding commission, the system will recover the subject's permissions. The formal description is similar to AR-UCONpre. Here, due to space limitation, not repeat them.

UCON Model With Time Constraint

Under cloud computing environment, there is a more important constraint attributes: time. Bertino [7] had proposed an access control model based on temporal characteristics, which added temporal constraints to the RBAC model. Wang XM and Zhao ZT [8] proposed embed the model with elements and temporal constraints, which means the dynamic role-based access control could be achieved by defining new temporal inheritance mechanism. The model can effectively reduce the number of the rules in the rule library, improve the efficiency of access control, but not suitable for large-scale distributed computing.

Time billing is a typical billing plan in cloud computing. Time constraint is everywhere. Sometimes, some users would have a specific role in a specific period of time, it is necessary to control the user's access to data with time constraint. Associating the main attributes with the time constraints would help to extend AR-UCON model and then further enhance the skills and versatility of the model.

Typical time constraint categories

A typical time constraint could be divided into the following three categories:

The time length constraint. The constraint is mainly used to set the length of activation time for a fixed user or role. It is mainly used in the case to protect sensitive information, such as online banking, e-payment platform etc. This constraint could prevent information disclosure in case the landing time is too long.

The time limit. The constraint is mainly used to set the active period of a fixed user or role. For example, in the school's student grads management system, teachers are only allowed to log in during normal working hours to edit data in the system.

The time length constraints for fixed period. The constraint is mainly used for setting the time length constraints of a fixed time period. For example, in the school's student grads management system, if the teacher had not completed inputting students' grads within 60 minutes, the teacher would be prohibited landing the system. So, some kind data protection could be guaranteed.

The improved UCON model based on time constraints

After introducing time constraints to UCON model, the time element can be added to the authorization decision. Therefore, authorization and time constraints completely achieve a better correlation. Thus, when the system tries to authorize the user, it can directly assign the role with the time characteristics to the user.

Control logic steps of the decision-making model are as follows:

Step 1: The user requests permission. These requests must have object information to be accessed and the specific operational requirements;

Step 2: The execution point obtains the relevant attribute in the repository based on user requests;

Step 3: The attribute information requested by user will be sent to a policy decision point;

Step 4: The policy decision point obtains the appropriate policy from the Policy Library based on the information received;

Step 5: Policy decision point return the received policy to the point of execution;

Step 6: The policy enforcement point decides whether to authorize based on the results returned.

Conclusion

In order to study the adaption and application of UCON under cloud computing environment, we introduced the role factors and time constraints to UCON model and proposed a new improved UCON model, AR-UCON, which has rights authorization and time constraints. The new model enhanced the decision continuity and authorization flexibility. So, it's better to achieve a fine-grained access to resources.

Acknowledgement

The paper was sponsored by a project of Shandong Province High Educational Science and Technology Program (No.J13LN76).

References

[1] Chen mingjie, Fan kefeng, Zhang subbing, A new DRM usage control model, J. Application Research of Computers,2010,27(8): 3073-3077，3080．

[2] Chen yue, Security of Database, Beijing: National Defend Industry Press,2011．

[3] Park J, Sandhu R, Towards Usage Control Models: Beyond Traditional Access Control, Proceedings of the 7th ACM Symposium on Ac-cess Control Models and Technologies． SACMAT02． Monterey，California，USA: ACM，2002: 57-64．

[4] Xia qishou, Fan xunli,Yin xiaoling, RBAC delegation model based on time, J. Journal of Northwest University(Natural Science Edition) 2009, 38(6): 932-936.

[5] Park J, Sandhu R, The UCON ABC usage control model , J. ACM Transactions on Information and System Security (TISSEC), 2004, 7(1): 128-174.

[6] Sun yuejiang, Application of UCON in electronic commerce system, J. Information Security and Technology.2012.6.60-62.

[7] Bertino E, Bonatti P, Ferrari E, TRBAC: A temporal role-based access control model, ACM Trans. on Information and System. Security, 2001,4(3):191-223.

[8] Wang XM, Zhao ZT, Role-Based access control model of temporal object, Acta Electronica Sinica, 2005,33(9):1634-1638．