http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (20): 5553-5558, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.5553.5558
© 2013 Asian Network for Scientific Information

A Credible Usage Access Control Model in Cloud Computing

Fengying Wang, Caihong Li, Hui Zhao and Shushu Liu
College of Computer Science and technology,
Shandong University of Technology, Zibo,Shandong, 255049, China

Abstract: Because cloud computing has the characters of virtualization, open, multi-tenant and elastification, cloud users and cloud objects always are changing dynamically, thus access control in cloud is more complex than traditional access control. The paper proposed Credible Usage Control Model in Cloud Computing (CUCONC),and based on the model given CUCONC reference monitor. CUCONC possesses Process continuity and attribute variability. By introducing credibility, CUCONC simplifies authorization policy,can change dynamically authorized rights,easy to grant or revoke rights. At the same time, the model enhances the manageability, flexibility and actionability.

Key words: CUCONC, Cloud computing, Credibility, Reference monitor, Authorized policy

INTRODUCTION

Cloud computing links large amounts of store resources, computing resources and software resources together, forms a huge Shared virtual resource pool so that provides IT services for remote computer cloud users (Zhang and Wang, 2012), lead to save the cost of cloud users. The rapid development of cloud computing has brought changes in service mode, but at the same time also brought a lot of new security challenges. At present, cloud computing security problem focus mainly on access control and authorization, virtualization security, and Web security three aspects (Subashini and Kavitha, 2011).

Cloud computing has the characteristics of on-demand pay, expandability, multi-tenant, and elasticity etc. (Sean and Curran, 2011). In cloud computing environment, access control is one of the effective means to protect information security. Compared with traditional access control, access control in cloud computing is more complex, because cloud users, cloud user attributes, cloud object, cloud object attributes always are dynamically changing. Traditional access control model is not completely suitable for cloud computing environments, so it is necessary for the special cloud computing mode to design a kind of access control model, according with the characteristics of cloud computing.

UCON (usage control) model (Park and Sandhu, 2004; Zhang *et al*., 2005) needs diversification and high-precision requirement for information resource usage control. By usage decisions on authorization, obligations and conditions, the model realized dynamic control for use process to access object resources, realized the continuous control of process and dynamic update of attributes, thus laid a good foundation to research access control of object resource in open network environment.

Existing UCON model not involved in management, authorization process, application and implementation. Authorization process is still an accurate validation process. When a user request authorization, will check systematic all constraint rules one by one. If checking pass, then system authorize the user, if not reject authorization. But in practice, most time, demands flexible authorization according to a variety of relevant factors. UCON defines abstract, realize complexity and do not tend to management and application.

Zhang and Wang (2012) could not reflect the continuity and dynamics of access control. Di and Wang (2007) not established suitable model, although applied fuzzy logic to usage control. Lin *et al.* (2012) proposed access control security model based on the behavior to ensure the security and privacy of data in the cloud server, but the characteristics of model “up read and down write” lowered its availability. Tang *et al.* (2011) divided the user cloud environments into two categories, ordinary users and the resource owner and the resource owner authorized rights related to access corresponding resources for ordinary users, lead to increase the burden of resource owner authorization management.

In the practical application of cloud computing, many times, demands flexible authorization on the basis of a variety of relevant comprehensive factors. The paper proposed Credible Usage Access Control Model in Cloud

Corresponding Author: Caihong Li, College of Computer Scienceand Technology, Shandong University of Technology, Zibo, Shandong, 255049, China

Computing (CUCONC) based on fuzzy logic, by usage control strategy, combining credibility of the trust management. The main contributions are as follows:

- Established CUCONC model based on fuzzy logic in cloud computing environment and the model is flexible, manageable and implemented
- Simplified the authorization policy. By computing credibility for cloud users according to a variety of comprehensive relevant factors, can change dynamically the authorized rights according to the degree of meet credibility, grant or revoke conveniently rights, has dynamic flexibility
- The model well retained the advantages of using control: continuous control of process and dynamic updates of attributes

The remainder of this article is organized as follows: section 2 introduces the credibility calculation method to cloud users; section 3 establishes CUCONC model based on credibility in cloud computing environment; Section 4 presents the reference monitor of CUCONC model.

CLOUD USER'S CREDIBILITY COMPUTATION BASED ON FUZZY LOGIC

In cloud computing, cloud users (requestors of cloud object resource) may be partially satisfy authorization rules (including authorizations, obligations and conditions), thus the system should grant different levels of permissions according to the extent of satisfaction, so should fuzzify the performance of cloud users . Different cloud environment can have different considerations. For example, we can divide 4 different grades of credibility, which correspond to the four credible levels, as follows:

- Complete satisfaction responding to complete trust: its value of credibility is set to 1 in the system
- Most satisfaction responding to special trust: the value of credibility is set to 0.7 in the system
- Small party satisfaction responding to general trust: the value of credibility is set to 0.3 in the system
- Dissatisfaction responding to distrust: the value of credibility is set to 0 in the system

Trusted degree of Cloud users will not simply belong to one of the four grades; it represents a certain degree of fuzziness. In other words, the cloud user's credible level may be between two trusted degrees. Based on membership degree of fuzzy set theory, we use a real Numbers between 0 and 1 to measure the trusted degree of a cloud user in membership degree of each grade, thus form a trust vector.

For example, a trust vector $V = \{v_1, v_2, v_3, v_4\}$, v_k $(k = 1, 2, 3, 4)$ $(0 = v_k = 1)$, v_k represents cloud user's trusted degree belonging to the kst credible level.

Here, the principle of fuzzy transform is used to get the trust vectors of cloud subjects. Four factors about the computation credibility should be considered:

- Factor Set $E = \{e_i\}$ $(i = 1, ..., n)$.This factor set contains crucial factors which determine the value of credibility. The paper considers the authorizations, obligations and conditions and so on.
- Evaluation Set $D = \{d_j\}$ $(j = 1, ..., m)$. For example, will evaluate Set divide into four levels,Evaluation Set D $= \{d_1, d_2, d_3, d_4\}$ = {Complete satisfaction,most satisfaction,Small party satisfaction,Dissatisfaction}. This set is the evaluation of each factor in set E. In this set, divide four grades according to credible grades
- Factors Evaluation Matrix $R = (r_{ij})_{2\times4}$ $(0 = r_{ij} = 1)$, $(i = 1, 2; j = 1, 2, 3, 4)$. r_{ij} refers to the possibility of each factor e_i in set E belonging to grade d_j. For example, r_{11} is the possibility value of e1 (the factor of payment) falling into grade d1 (excellent). Here, r_{ij} is calculated through a trapezoidal membership function.
- Trapezoidal Membership Function $\mu(x)$: $\mu_A(x)$, $\mu_B(x)$, $\mu_C(x)$, $\mu_D(x)$. These are four membership functions denoting the possibility of each factor in set E belonging to each evaluation grade in set D. In the system, the payment scope: $U = (0,M]$(M is the upper limit of payment). For the sake of simplicity, M is set to 100 and points of 30, 40, 60, 80, 90 are marked. These numbers can also be changed according to the actual situation. Setting the "payment" factor, membership functions are as follows
- Weight distribution for each factor in set E $W = \{w_i\}$, $(0 = w_i = 1, i = 1, ..., n)$, w_i presents the relative importance of each factor in set E for evaluation, satisfying the equation:

$$\sum_{i=1}^{n} w_i = 1$$

In this system, Uses the variable weights synthesis and determines the weight of each factor according to expert advice, actual problem domain and needs, statistical method, etc.

$$V = \{v_j\} = \{w_i\} \circ (r_{ij})_{n*m}, \ (i = 1, ..., n, j = 1, ..., m)$$

Here, "∘" refers to the fuzzy transform:

$$v_j = \bigvee_{i=1}^{n} (w_i \wedge r_{ij})$$

$\wedge$ and $\vee$ denote the max operation and min operation (Liu and Cao, 2005; Wang and Wang, 2007).

After calculating the weighted average of every vector component in V and every trust grade, the final credibility value is obtained.

For certain category of cloud resource, different kinds of rights require different credibility limits for access.

Cloud users rely on their credibility to access to cloud object resources. The credibility value is one of the attributes of cloud users and can be changed according to the cloud user behavior. In addition, in the process of cloud object resource usage, cloud users satisfying the extent of process decision, will cause the increase or decrease of the cloud user's credibility.

CUCONC--AUTHORIZATION MODEL BASED ON CREDIBILITY

Usage control model has powerful function and extensive application, can solve some new problems on modern information system. However it did not fully embody user's credibility in the open cloud environment and implementation and management is very complex. Considering virtualization, multi-tenancy, expandability, elastification and credible management and applicability, etc., combining usage control and credibility, put forward authorization model CUCONC based on fuzzy logic in cloud computing, as shown in Fig. 1.

CUCONC model: CUCONC model consists of 11 core elements and three functions in Fig. 1. 11 core elements are rights , cloud services, cloud object owner, cloud users, cloud user attributes (including cloud user credibility), cloud object, cloud object attributes (including credibility threshold), credibility, authorizations, obligations and conditions, three functions are respectively authorization function, obligation function and condition function. the definition of these rights, authorizations, obligations, conditions, authorization function, obligation function, condition function are the same as UCON (Park and Sandhu, 2004); cloud users, cloud user attributes, cloud objects, cloud object attributes corresponds to subjects, subject attributes, objects, object attributes in UCON (Park and Sandhu, 2004) ; cloud service providers and cloud object owner are new elements; the credibility computation have been discussed in the Introduction.

Relevant factors in CUCONC model

The cloud service provider and cloud object owner: The cloud service provider is provider of store, computing, software and so on in cloud. It provides a platform for store, computing and software.

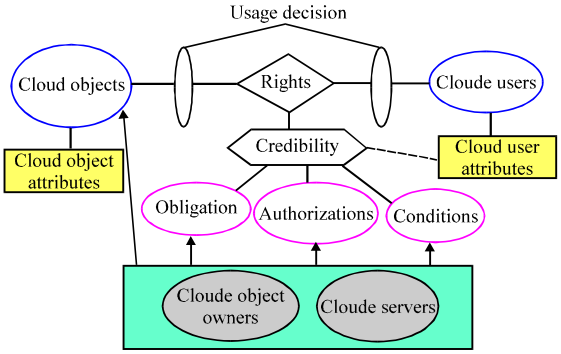

Fig. 1 : CUCONC model

The cloud object owner is provider of object resources in cloud.

Authorizations, obligations and conditions: Because the cloud object owner is cloud object resource owner, it has the rights to make authorizations, obligations and conditions. Authorizations, obligations as well as conditions may are made by cloud service providers or/and cloud object owners. Of course, a cloud object owner can also be fully authorized to cloud providers,thus the cloud service provider are in charge of authorizations, obligations and conditions. In most cases, the cloud service provider and the cloud object owner make joint authorizations, obligations and conditions.

Because authorizations, obligations and conditions can are very complex, so we use generally authorizations functions, obligation functions and condition functions describe authorizations, obligations and conditions.

The model refines authorizations, obligations and conditions into three pre-decisions and three process decisions. The three pre-decisions are pre-authorizations, pre-obligations and pre-conditions; they are the same as the meaning of literature (Park and Sandhu, 2004). Similarly, three process decisions are process authorizations, process obligations and process conditions; they are also the same as the meaning of literature (Park and Sandhu, 2004).

Credibility and credibility threshold: Last section has discussed credibility calculation way Based on fuzzy logic. The credibility is the credibility of a cloud user, the credibility is one of the cloud user attributes, The credibility represents the credible degree of the cloud user. Credibility threshold is one of the cloud object attributes.

The higher a cloud user possesses credibility, the more the user can access the cloud object resources, the bigger the user's rights is, otherwise, the smaller the user rights is.

Each cloud object corresponds to a number of permissions of use resources. The cloud service provider and the cloud object owner set a lower limit value of credibility for different usage permission. The lower limit value is a threshold corresponding to usage permission to can access the cloud object. Only the credibility of a cloud user is not lower than the threshold of correspond to some usage permission of a cloud object,the cloud user can has the usage permission of the cloud object.

According to a certain principle (such as security level of a cloud object, etc.), set a threshold of credibility for every different permission of a cloud object.

Combining variable attributes in CUCON model, when need to change the security level for cloud object resources, can directly modify its cloud object attributes. Credibility threshold can also consider expertise advice, actual need and so on.

Whether or not a cloud users are allowed to access the cloud object resources, can be made of 5 tuple (CO, P, COP_{RT}, CU, CU_R). CO represents a cloud object, P represents the a certain permission of a cloud object, COP_{RT} represents a credibility threshold of a certain permission P of a cloud object CO, CU_R represents the credibility of a cloud user CU.

In the model, by comparing the credibility of a cloud user with the credibility threshold of a certain permission P of a cloud object CO, Determine whether to grant. Only when the credibility CU_R is no less than the credibility threshold COP_{RT}, cloud user CU can gain access to the cloud object resources CO.

Initial cloud user credibility value is calculated by pre-authorizations, pre-obligations and pre-conditions (such as payments, meeting the demand, etc.). Whenever the cloud user object uses cloud resources, according to the cloud user credibility value, obtain initial access to cloud object resources. In entire use process of a cloud resources,the cloud user's credibility value is changing with process authorizations, process obligations and process conditions.

The reference monitor is a core concept that provides control mechanisms on access to cloud resources. Reference monitor associates decision policies and rules for control of access to digital objects. In the next section, we will research in detail reference monitor in CUCONC model. the reference monitor needs to calculate real-timely the credibility of cloud users who are access to cloud objects according to three process decision constraint:process authorizations, process obligation and process conditions, judge real-timely whether to satisfy the credibility thresholds, in order to make a decision to increase or reduce or cancel the rights.

Because the authorization policy based on credibility is found above three decision factors: authorizations, obligations and conditions, CUCONC model hold the advantages of usage control very well. At the same time, authorization systems must not judge decision-making factors respectively, so as to simplify the authorization policy. On the one hand, The CUCONC keep the extensive problem domain of UCON. On the other hand, by the credible management based cloud users, realize more security authorization mechanism.

CUCONC model analysis: CUCONC model is extension and supplement on UCON model. The objective is how to control the right of cloud users. In common they are:

- When a cloud user access to a cloud resource, must satisfy three factor constraints: authorizations, obligations and conditions
- The rights are consumable. The Cloud user may not have indefinitely permissions on cloud object. The cloud user's rights will exhaust gradually along with cloud users using cloud resource
- The cloud user access to the cloud object having process continuity and attribute variability. Reference monitor supervise real-timely access to the entire process. At the same time, the cloud user's properties can be changed according to the cloud user access behavior

The differences of two models in mechanism of permissions granted are:

In UCON, implements permission granted by the constraints of the three decision factors every once and considers separately the three factors. Application is flexible, but the implementation is difficult. However in CUCONC model, the authorization policy is based on the credibility of fuzzy theory, implements permission granted according the credibility of a cloud user and the threshold of a cloud object. By comparing the threshold and the credibility, Implements to grant or revoke access to the cloud object, thus the cloud object resources authorization is more flexible, simpler, easier to implement.

By above comparing on the similarities and the differences, UCON is of high security and dynamics, but did not fully embody credible relationships of cloud users in cloud computing environment and model implementation and management is more complex.

CUCONC model retains the main concepts and features of UCON, by introducing credibility authorization, improves the manageability and applicability.

REFERENCE MONITOR ON CUCONC MODEL

ISO has published a standard for access control framework [ISO/IEC 10181-3] that defined reference monitor and trusted computing base [ISO 96].

From an architectural point of view, the reference monitor is one of the key problems of performing authorization control. When cloud users access to cloud object resources, reference monitor coordinates and controls judgment execution of each decision module, achieve continuity control, attribute variability and dynamic authorization mechanism. CUCONC model reference monitor is as shown in Fig. 2.

CUCONC reference monitor is similar but different in some aspects from traditional reference monitor of ISO's access control framework. Figure 2 shows the conceptual structure of CUCONC reference monitor. CUCONC reference monitor consists of Decision Enforcement (ED) and Authorization Decision (AD). Each part includes several function modules. AD includes condition and obligation as well as authorization module.

Authorization module takes care of a process similar to traditional authorization process. It utilizes cloud user attribute--credibility and cloud object--credibility threshold and usage rules to compare whether the credibility is not less credibility threshold. It may return yes or no. Returning metadata information of authorized portion is used for customization of requested cloud objects by customization module of ED

Condition module decides the degree of conditional requirements satisfied by using usage rules and contextual information (e.g., current time, IP address, etc) for the authorized requests.

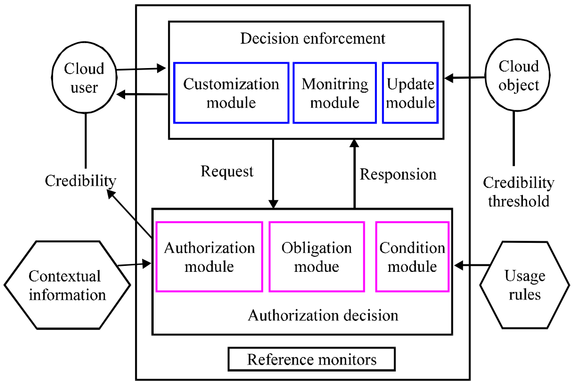

Fig. 2: Reference monitor of CUCONC model

Obligation module decides the degree of certain obligations performed before or during when requesting cloud objects use. The module must be monitored by monitoring module and the result has to be resolved by update module in ED.

CONCLUSIONS

Credible usage access control model --CUCONC proposed in this paper be appropriate for solving the problem of access control under virtualization, open, paid use and elastification cloud computing environment. The article studies only dabbled in some parts of it. Many aspects concerning about the model, such as the concurrency of dynamic update, delegation mechanism, the formalization description and so on, these works remains to be further research.

ACKNOWLEDGMENT

This research is supported by the Science and Technology Development Plan Program of Shandong Province under Grant 2013GGX10116 and by the Higher Educational Science and Technology Program of Shandong Province under Grant J13LN27 and by the Natural Science Foundation Program of Shandong Province under Grant ZR2013FM013.

REFERENCES

Di, W.Y. and X.M. Wang, 2007. Usage control model study based on fuzzy logic. Microelectron. Comput., 24: 116-119.

Lin, G.Y. and S. Huo et al., 2012. Cloud computing access control security model based on behavior. J. Commun., 3: 59-66.

Liu, Y.L. and Y. Cao, 2005. Subjective trust model research of distribution network environment. J. Beijing Polytech., 25: 504-508.

Park, J. and R. Sandhu, 2004. The UCON ABC usage control model. ACM Trans. Inform. Syst. Secur., 7: 128-174.

Sean, C. and K. Curran, 2011. Cloud computing security. Int. J. Ambient Comput. Intell., 3910: 14-19.

Subashini, S. and V. Kavitha, 2011. A survey on security issues in service delivery models of cloud computing. J. Network Comput. Appl., 34: 1-11.

Tang, Z., J. Wei and A. Sallam, 2011. A new RBAC based access control model for cloud computing. Int. J. Mordern Educ. Comput. Sci., 5: 279-288.

Wang, F. and F. Wang, 2007. The research and application of resource dissemination based on credibility and UCON. Proceedings of the International Conference on Computational Intelligence and Security, December 15-19, 2007, Harbin, China, pp: 584-588.

Zhang, X., F. Parisi-Presicce, R. Sandhu and J. Park, 2005. Formal model and policy specification of usage control. ACM Trans. Inform. Syst. Secur., 8: 351-387.

Zhang, Z.L. and C.F. Wang, 2012. Attribute-based distributed access control scheme in cloud. Comput. Eng., 38: 1-4.