Trust Based Access Control Policy in Multi-domain of Cloud Computing

Guoyuan Lin
School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, China
State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, China
Email: lingy@cumt.edu.cn

Yuyu Bie
School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, China
Email: bieyuyu@126.com

Min Lei
Information Security Center, Beijing University of Posts and Telecommunications, Beijing, China
National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing, China
Email: leimin@bupt.edu.cn

***Abstract*—Cloud computing is a new paradigm which enables users to reduce their costs and is advantageous to both the serving and served organizations. However, security issue is a major concern in the adoption of cloud computing. The most effective way of protecting cloud computing services, resources and users is access control. This paper intends to provide a trust-based access control mechanism for cloud computing considering its multi-domain aspects. Firstly, trust is introduced into cloud computing environment and trust relationships between users and cloud platform are built. It also analyzes the difference between intra-domain trust and inter-domain trust. Furthermore, a role-based access control framework combined with trust degree in multi-domain is given from this paper. Access control in local domain directly applies RBAC model combined with trust degree, whereas in multi-domain it contains the conception of role translation. The simulation results show that the proposed method is more suitable to cloud environment and definitely can improve the reliability and validity of the system.**

***Index Terms*—cloud computing, trust, access control, multi-domain, role translation**

I. INTRODUCTION

In recent years, cloud computing with its advantages of super large-scale, virtualization and high reliability lead to changes in computer networks. However, cloud computing is faced with serious security problems [1]. 'Cloud' is like a pool of shared and virtualized resources which assembles large-scale resources in the network, such as computing resources, software resources and storage resources [2]. Hence, cloud computing is for sharing computation. In order to implement the resource-sharing feature, access control problems shall be resolved. Traditional access control is an identity-based authentication technology and it only works within the scope of a united security domain [3]. Cloud computing provides services via the virtualized resource pool throughout the network which often covers a wide range and resource owners usually do not belong to the same security domain. So cloud computing is cross-domain and dynamic. While the traditional identity-based access control technology has apparently cannot satisfy the security requirements of cloud computing. At present the most effective way is to make improvement on the basis of traditional access control policy and consequently adapt to the new security requirements of cloud computing. How to improve the traditional access control technology and solve the security problems of cloud platform are the hottest focuses of current research.

Access control technology can not only ensure normal access requests of valid users, prevent invasions of unauthorized users, but it also can solve security problems caused by valid users' misoperation. In cloud computing, researchers are more concerned about how to implement access control by using unconventional methods. IAM (Identity and Access Management) is the main access control technology in cloud computing, but it cannot ideally solve cross-domain access control problems. Cross-domain access control has become an important direction of scientific research and trust is the core issue of cloud computing access control. In 1996, Blaze M proposed the concept of trust management and for the first time applied trust mechanism in human society to the technical field, providing a new way of solving the security problems in cloud computing environment. Based on trust management, trust mechanism will be introduced into access control area, which will be redefined and calculated. Finally this developed access control model will be implanted in cloud computing platform for research. In order to ensure

doi:10.4304/jcp.8.5.1357-1365

the credibility of cloud computing in distributed multi-domain environment, trust model will be built and trust computation and updating mechanisms will be included. The major difficulty will be trust computation due to the dynamic features of trust.

In this paper, cloud computing security issues will be analyzed and then trust management and RBAC model will be discussed. In addition, the paper introduces trust degree into access control model and finally proposes trust-based access control model of multi-domain in cloud computing environment. Trust computation methods are given in local domain and multi-domain, respectively. The establishment of trust relationship and multi-domain access control policy are better realized.

The rest of this paper is organized as follows, section II analyses related works on trust and access control method of cloud computing. Section III gives a new trust computation model in cloud computing environment. Section IV presents the trust based access control policy in multi-domain environment including access control in local domain and cross-domain. Section V addresses the simulation environment, parameters and performance evaluation of the proposed trust based access control model. Finally, conclusion is given in Section VI.

II. Related Work

As a new information service mode, cloud computing has brought new security risks and challenges. However there is no essential difference between cloud computing services and traditional IT services in terms of security requirements. And the key technology to meet the security requirements is access control technology. Reference [4] analyzed the dynamic requirements of access control in cloud computing, and introduced role-based access control (RBAC) model into cloud computing environment. RBAC model combined with advantages of cloud computing had realized dynamic management and increased maintainability of access control.

RBAC model is enclosed and based on identification, so its access control mechanism only applies to enclosed networks, which does not suitable for large-scale, distributed networks. It's unable to meet the security needs of the multi-domain environment in cloud computing either. Hence authorization of multi-domain is the main problem to be solved of access control in cloud computing. Besides, when a role is assigned to a user in RBAC model, it only verifies authenticity of user's identity without taking trust of user's behavior into account. Meanwhile, roles are pre-assigned in access control authorization and it does not regulate and control in the process of practical application. Consequently, once malicious operations of users have been found, the system must have been violated. To solve these problems, some researchers think they can integrate trust mechanism into the traditional access control model [6-8]. Reference [6] suggested improvements against deficiencies of RBAC model based on Blaze's trust management. Trust was introduced into access control mechanism and finally a trust-based access control model TRBAC (Trust Role Based Access Control Model) was proposed. TRBAC, starting from users' specific requirements for permissions, calculated varieties of user's trust features and implemented the fine-grained, flexible authorization mechanism and thereby a much more secure and reasonable distribution of permissions for users. Reference [7] and [8] also developed RBAC against its deficiencies and presented a dynamic trust-based RBAC model in cloud computing environment. Reference [7] gave a detailed calculation process of trust degree and permission assignments according to user's role and trust degree. And this method could reduce risks of communication and improve the safety. While Reference [8] only presented theoretical analysis and did not present details of trust calculation method. However, studies mentioned above hadn't considered the multi-domain aspects of cloud computing.

Nowadays, integrating Trusted Computing into cloud environment and making it as a reliable way to provide cloud services is a hot topic in cloud security. Santos [9] proposed a trusted cloud computing platform (TCCP) on which IaaS providers could offer a closed box-type execution environment to users and ensure the confidentiality of guest virtual machine. In addition, it allowed the user to checkout whether the service provided by IaaS providers was security or not before starting the virtual machine. Sadeghi believed that Trusted Computing could provide trusted software, hardware and demonstrated mechanism of its own behavior, which could be used to solve the confidentiality and integrity issues of outsourcing data. Meanwhile a trusted software token binding to a security functional testing module had been designed and performed various functional operations on encrypted data under the premise that no information disclosure [10]. However, studies above are expected to guarantee data safety by trusted cloud computing platform without considering the credibility of cloud users.

Cloud computing is a multi-domain environment and its security domain could be divided into three grades. According to its safety needs, there're firewalls between security domains performing security isolation and ensuring that data transmission comply with the corresponding access control policy. However, existing access control models cannot meet the multi-domain requirements. Reference [11] proposed a trust-based cross-domain access control model which could both achieve local domain and cross-domain access control strategy in grid environment. In this paper, combined with the idea of cross-domain access control in Reference [11], we developed RBAC model and put forward a multi-domain access control policy in cloud computing environment.

III. Trust Computation in Cloud Computing

Human society is a complex system in which interactions between entities are depended on their trust relationships. Therefore some people think that trust mechanism in human society can be introduced into

cloud computing. Reference [12] proposed the general concept of trust for the first time. Trust represents an entity's ability to work safely and reliably in a particular environment. The paper also gave some relevant properties of trust relationships. Trust relationship always exists between two entities and is characterized by its being dynamic, transitive, specific, fuzzy and uncertain. Soon afterwards, researches of trust in computer network have been widely applied to fields of P2P networks, e-commerce, grid computing, cloud computing, etc.

Trust in real life is a subjective concept, depending on one's experiences. We can hardly describe or calculate trust using accurate models or algorithms after applying trust to computer networks. Trust is the assessment of an entity's identity trust and behavior trust. Trust is related to reliability, integrity and performance of this entity [13].

According to the concepts above, trust can be divided into identity trust and behavior trust. Identity trust is used to indicate the identity of an entity and the traditional access control technology only considers identity trust, such as identity verification. After identity verification the trusted entity can access the appropriate resources. However, in network environment it cannot ensure behaviors of users who pass the identity authentication are legal, so behavior trust should be taken into account. Hence, this article is on the basis of behavior trust to implement access control policies.

Trust in cloud computing can be considered as the ability of the entity to ensure safe and reliable cloud computing services. Although this method is able to describe trust very clearly, it cannot figure out the values of trust degree. Trust is an objective reality. In the field of access control, trust can make a more clear definition of security policy and make different security policies depending on trust values.

There are some related researches at home and abroad about the expressions of trust and typical trust expressing and reasoning models are proposed, such as Beth model [14] and Jϕsang model [15]. Beth model introduced the concept of experience to describe and measure trust relationships, and gave calculation equations of recommended trust. Trust in this model was composed of direct trust and indirect trust. Direct trust is a trust relationship between entities through direct interactions, while indirect trust is a trust relationship recommended by the intermediate entity between two entities that had never been interacted before. This classification of trust is adopted by lots of subsequent models. According to the classification, the establishment of trust relationships can be divided into two kinds: ①Direct establishment: if there are interactive experiences between two entities, trust relations can be directly established based on the result of their interactions; ② Recommended establishment: if there's no interaction experience between two entities before, trust relations can be established based on the recommendation of the third party (an intermediate entity). This method of classification is applied to trust model proposed in this paper. Based on the probability theory, Jϕsang put forward the concepts of evidence space and concept space and described trust relations. Although there's no clear distinction between direct trust and recommended trust, it provided the recommended operator for the derivation of trust. Jϕsang model as well as Beth model cannot effectively eliminate the influence of malicious recommendations.

On the basis of Beth model, we proposed a trust-based multi-domain access control model. Entities would be respectively assigned different weights of direct trust and recommended trust according to trust policies. For example, some entities believe the experience of their direct interaction; so direct trust will be given a higher weight. While others do not interact directly and believe the recommendation of the intermediate entity, so they give recommended trust a larger proportion.

A. Trust Relations in Local Domain

When visiting is happening in the same security domain, cross-domain access control can be ignored. Therefore, it can make security operations simply by introducing trust into traditional access control model. Based on RBAC model, trust relations and trust degree between users and resources in local domain shall be established and evaluated.

Suppose A is a security domain in cloud computing environment and it contains multiple entities marked as n. When interaction occurs in domain A, it calculates trust degree between the interacted entities and implements access control policy of local domain. In local domain, trust consists of intra-domain direct trust and recommended trust.

Definition 1(Intra-domain Evaluation): In local domain, an evaluation value will be given when an entity complete interaction with another entity, represented by the symbol E, which $-1 \le E \le 1$. Negative value indicates not satisfied and it will reduce the trust degree, while positive value expresses satisfaction and it will increase the trust degree. After the k-th interaction, entity n_j will give entity n_i an evaluation value, which can be formalized as $E(n_i, n_j)^k$.

Definition 2(Service Satisfaction): In local domain, a service satisfaction value will be given when an entity complete multiple interactions with another entity, represented by the symbol *S*. After k times of interactions, entity n_j will give entity n_i a service satisfaction value, which can be formalized as follows:

$$S(n_i, n_j)^k = \beta \times S(n_i, n_j)^{k-1} + (1-\beta) \times E(n_i, n_j)^k \quad (1)$$

Definition 3(Direct Trust Degree): An entity's intra-domain direct trust degree is related to its intra-domain evaluation value. Direct trust degree can be represented by DTD. The value of DTD is usually initialized to zero. In domain A, after the k-th interaction, direct trust degree between entity n_i and n_j is as follows:

$$DTD(n_i, n_j)^k = \alpha \times DTD(n_i, n_j)^{k-1} + (1-\alpha) \times E(n_i, n_j)^k \quad (2)$$

Definition 4(Reputation): An entity's reputation in local domain can be calculated by the satisfaction values obtained after interactions with all the other entities in the same domain. This reputation can be represented by Rp . The reputation of entity n_i in domain A can be expressed as $Rp(n_i, A)$, and the concrete calculation formula is as follows:

$$Rp(n_i, A) = \frac{\sum_{j=1, j\neq i}^{k} S(n_i, n_j) \times Rp(n_j, A)}{k} \quad (3)$$

Definition 5(Intra-domain Trust Degree): An entity's intra-domain trust degree refers to the credibility of the entity and it consists of direct trust degree and reputation. Intra-domain trust degree can be represented by the symbol TD. Trust degree of the i-th entity n_i in domain A can be formulized as $TD(n_i, A)$, and the calculation formula is as follows:

$$TD(n_i, A) = \gamma \times \frac{\sum_{j=1, j\neq i}^{k} DTD(n_i, n_j)^j}{k} + (1-\gamma) \times Rp(n_i, A) \quad (4)$$

Where $\alpha, \beta, \gamma > 0$. The values of these weight parameters are relevant to local domain security policies and stored in local domain authentication and authorization center.

B. Trust Relations Cross-Domain

Although trust evaluation among different security domains differs from that in single domain, the impact of inter-domain trust is relevant to trust degree of some entity and the behavior of every entity in the domain. Meanwhile, the traditional RBAC model is no longer applicable in access control of multi-domain environment. If you want to apply RBAC model to multi-domain environment of cloud computing, you need to carry out role association and dynamic role translation. Role translation in multi-domain circumstance will be introduced in the following text.

Suppose domain A and B represent two different security domains in cloud computing, m_i is an entity of domain B. It calculates the trust degree when interactions occur between two entities respectively from domain A and domain B and implement cross-domain access control policies.

Definition 6(Direct Trust Degree Cross-Domain): Direct trust degree between two domains is related to the direct trust between one domain's entities and the other domain. $DTD(A, B)$ represents the direct trust degree from domain B to domain A. As time changes, the results change constantly. The calculation formula is as follows:

$$DTD(A, B) = \frac{\sum_{j=1}^{k} DTD(m_j, A)^j}{k} \quad (5)$$

Definition 7(Reputation Cross-Domain): The reputation of entity m_i in domain A is represented by $Rpa(m_i, A)$. $Rp(A, B)$ represents cross-domain reputation from domain B to domain A. The calculation formula is as follows:

$$Rp(A, B) = \sum_{j=1}^{k} \theta_j \times S(m_j, A)^j \times Rpa(m_j, A), \sum_{j=1}^{k} \theta_j = 1, \theta_j > 0 \quad (6)$$

The weight factor θ_j in (6) corresponds to the direct trust degree of entity m_j in domain B.

Definition 8(Trust Degree Cross-Domain): $TD(A, B)$ represents the comprehensive cross-domain trust degree from domain B to domain A and it contains two parts, cross-domain direct trust degree and reputation which would be assigned to different weights by the security management center. The calculation formula is as follows:

$$TD(A, B) = \delta \times DTD(A, B) + (1-\delta) \times Rp(A, B) \quad (7)$$

IV. TRUST BASED ACCESS CONTROL POLICY IN MULTI-DOMAIN ENVIRONMENT

Trust relations between users and cloud computing platform will be established according to user's behavior and trust degrees will be calculated by the trust model. Combined with RBAC technology, dynamic access control in cloud computing environment will be implemented. In accordance with the multi-domain character, this paper introduced trust into access control model and established a trust based multi-domain access control model in cloud computing environment. The main difference between trust based multi-domain access control and the traditional access control mechanism is that users visit local domain and cross-domain respectively by means of two different kinds of access control policies. In trust based multi-domain access control model, when a user logs in, the system shall verify user's identity first. If the identity is trusted, the user's identity will be authorized. Trust levels reflect users' behavior trust in this model. Authorization is no longer a static mechanism based on identity trust, but a dynamic mechanism combined with identity trust and behavior trust. Therefore, this model realized the combination of user's identity trust and behavior trust. The overall framework of trust based multi-domain access control model is shown in Fig.1.

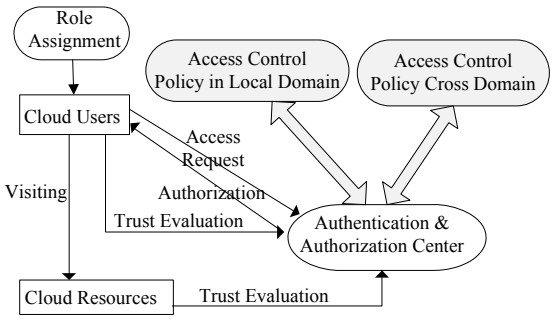

Figure 1. Overall framework of trust based multi-domain access control

The cloud user will be assigned the appropriate role by role management center and then interacts with the authentication and authorization center. The user first submits its requests including ID, password, role information and requested resources, and then applies for permission to access. If the user requests local domain resources, then use local domain access control policy. Else if the requested resources are in another domain, then use cross-domain access control policy and implement permissions distribution and management.

A. Access Control Policy in Local Domain

The main method of introducing trust into RBAC model is taking trust degree as the basic property of cloud users and cloud services and resources. The authentication and authorization Center (AAC) is in charge of access control authentication, authorization and trust management in local domain. While in cross domain, access control and trust management are the responsibility of both master authentication and authorization center (MAAC) and AAC.

In local domain, every time when cloud users request access to cloud services or resources, AAC would see user's trust degree to ensure that the user's trust degree meet the trust threshold. If it is so, the user's request would be allowed. The structure of access control in local domain is shown in Fig.2.

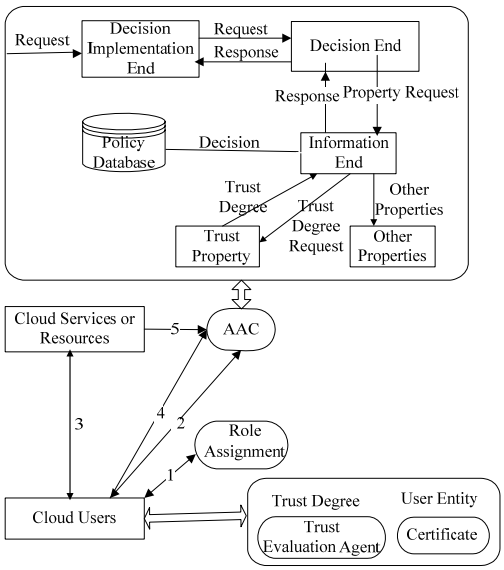

Figure 2. Access control structure in local domain

The access control process in local domain is as follows:

(1).In RBAC, cloud user will request to role assignment before it sends an access request and obtains the corresponding access rights indirectly. While in our model, users can only obtain access rights through their roles, but they do not have the permission to use these rights. It also needs further measures such as trust management to decide whether a user can use their access rights.

(2).The cloud user sends an access request including user ID, password and ID of the requested resources or services to AAC. AAC authenticates the user's identity first and then authorizes the user based on its trust degree obtained from trust management. Authorization process is as follows:

①The decision database initializes security policy in local domain;

②The decision implementation end delivers user's request to the decision end;

③The decision end delivers the request to the information end;

④The information end obtains information of user's trust degree and other properties and returns it to the decision end;

⑤The decision end makes an access control decision according to user's information and current security policy;

⑥The decision implementation end returns the result to the user entity.

If the user's access request is permitted, then provide the user a certificate, so that the user obtains the permission to use the access rights corresponding to its roles.

(3).The cloud user executes its access control privileges and visit cloud services or resources.

(4).In the end, the user evaluates the performance of cloud services or resources. The trust evaluation agency would compute a new trust degree and send it to AAC.

(5).The cloud service or resource provider also gives an evaluation of the cloud user and returns it to AAC.

B. Access Control Policy Cross-Domain

As users usually need to access cloud services or resources of different security domains, a safe and effective access control method is necessary. Research about cross-domain access control problems in cloud computing environment is not much, but it cannot be ignored. RBAC applies to the closed network environment and is unable to meet the security requirements of the multi-domain environment. Therefore, role association is required. Role association means converting roles of one domain into roles of another domain. The structure of trust based access control in cross-domain is shown in Fig.3.

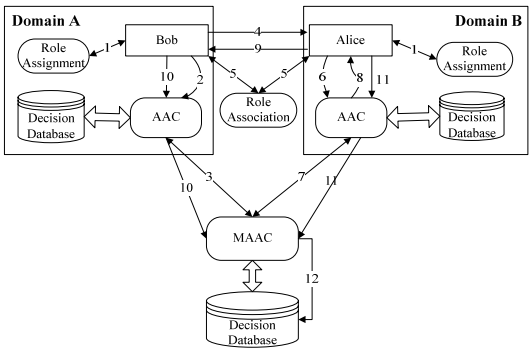

Figure 3. Structure of access control in cross-domain

Cross-domain access control process is as follows:

(1).Bob's role in domain A will be assigned by role assignment center of A, so that Bob can obtain his role in domain A. Alice's role in domain B will be assigned similarly by role assignment center of B.

(2).Bob sends a request to AAC of domain A. AAC figures out Bob's trust degree and judges whether Bob has the permission of visiting the target domain according to local security policy.

(3).AAC of domain A sends the request to MAAC. MAAC looks up trust relations between domain A and domain B and then checks if access should be allowed. If it is allowed, AAC will provide Bob a certificate.

(4).Bob sends Alice his access request, certificate and his role in domain A.

(5).After receiving Bob's access request, Alice first converts Bob's role in domain A into an understandable role of domain B through role association and then checks whether this role has the permission of visiting Alice's resource. If it has the permission, then turn to step (6); If it doesn't have the permission, then refuse Bob's access request directly.

(6).Alice passes the certificate to AAC of domain B.

(7).AAC of domain B contacts with MAAC. MAAC completes the connection between the two domains and the certificate transmission according to trust degree and role mappings between domain A and domain B. MAAC figures out Bob's trust degree in domain B, then returns the result to AAC of domain B.

(8).AAC of domain B compares Bob's security properties with local security policy, and then returns the result to Alice.

(9).Alice returns the result of authorization to Bob. If the request is permitted, Alice would allow Bob to use her resource; if not, Alice would refuse Bob's request.

(10).Bob evaluates the performance of the requested resource and sends the value to AAC of domain A. Then AAC passes it to MAAC.

(11).Alice evaluates Bob and sends the evaluation value to AAC of domain B. Then AAC passes it to MAAC.

(12).MAAC calculates and updates the mutual trust degrees between domain A and domain B according to the evaluations of the above.

C. *Inter-Domain Role Translation*

There are multiple security domains in cloud computing environment, so security interoperability of two domains shall be considered. IRBAC2000 model [16] proposed the concept of cross-domain access control and complemented security interoperability between different security domains by dynamic role translation. The management domain is administrated by a single management authority including a collection of multiple hosts, routers, and Internet. In this paper, our trust based access control model continues to use RBAC model for reference. Every user in the cloud would be assigned with a role that represents the permission of the user to use the rights. If domain A and domain B are intended to interoperate securely, a security context between A and B need to be established. The security context is a security session between two entities under the security policy management of a certain domain. In order to establish the security context, the two domains must reach an consensus on the security policy. A basic method is that two domains establish a default security policy providing basic security. But that does not meet the requirements of high security and reliability in multi-domain cloud computing environments. For example, in Fig.3, Bob of domain A want to establish a security context with the target object, Alice of domain B. It must rely on the underlying security mechanism to establish the security context. In order to obtain a higher degree of flexibility, Bob and the target object, Alice must know each other's identity. The same situation is very common in a single domain. However, because Bob and Alice are in different domains, they usually do not know each other and their identities. In order to solve this problem, a strategic framework can be used to simplify the security interoperability between two or more domains. The framework operated by establishing a set of associations of role hierarchy between local domain and another domain. These associations constitute a combination of role hierarchies, and the role hierarchy is still a partial order.

The definition of role a associate with role b is that role a of outer domain would be converted to role b of local domain and make a in local domain have the permission of b. It is represented symbolically by $a_{R_1} \mapsto b_{R_0}$, or simplified as (a,b). R_1R_0 Represents the set of all associations from R_1 to R_0, getting $R_1R_0 \subseteq R_1 \times R_0$. Define $x > y$ as a type of relations between role x and role y. $x > y$ Means that x is higher than y in role hierarchy, in other words, x is the ancestor of y.

Association is divided into two types, one is transitive association, and the other is intransitive association.

(1) Transitive association

Suppose there is an association $a_{R_1} \mapsto b_{R_0}$, if $\forall x \in R_1, x_{R_1} > a_{R_1}$ implies $x_{R_1} > b_{R_0}$;

$\forall y \in R_0, b_{R_0} > y_{R_0}$ implies $a_{R_1} > y_{R_0}$, then this kind of association is called a transitive association.

(2) Intransitive association

Suppose there is an association $a_{R_1} \mapsto b_{R_0}$, and the ancestors of a_{R_1} (roles of higher level than a_{R_1}) are not allowed to inherit this association. This kind of association is called intransitive association, symbolized as $a_{R_1} \mapsto_{NT} b_{R_0}$ or $(a,b)_{NT} \in R_1 R_0$.

Role association is converting roles in outer domain into understandable roles in local domain. When associations established, all the outer domain roles would be dynamically translated into local roles.

In role hierarchy between the outer domain and local domain, a combination of partial order relations shall be established by means of transitive association and intransitive association and define some kind of security policies. These policies can be divided into the following three types:

(1) Default policy

This policy is to establish a minimum number of associations $g_{1R_1} \mapsto g_{0R_0}$ between role set of outer domain and role $g_{0R_1}(Guest)$ (the minimum role in local domain) which makes $\forall x \in R_1$, $if\ x_{R_1} > g_{1R_1}$, $then\ x_{R_1} > g_{0R_0}$.

(2) Clear policy

The security officer will clearly have each role of outer domain map to a local domain role.

(3) Partial clear policy

A mapping, if is not a clear policy and exits one or more associations except the default policy, is called a partial clear policy. This strategy reflects a real sense of flexibility of dynamic role translation. In the partial order hierarchy, roles without clear association in outer domain can still realize a logical association by means of partial clear policy.

Associations (label 1, 2 and 3) in Fig.4 can illustrate this policy. H_0 represents the role hierarchy of domain D_0 and H_1 of domain D_1. The arrow from role x to role y means that x is the father node of y and the level of x is higher than y in the role hierarchy. Although the hierarchical structure of the role in H_0 and H_1 are very similar, but their semantics are different. If an object with the role of "Manager" from the outer domain intends to interoperate with an application in local domain, while the application usually only allows local role "Professor" access. Therefore, it should convert the outer domain role "Manager" into local role "Professor" (see label 1). The association (label 2) is an intransitive association. There are roles of "Guest" in both two domains shown in Fig.4. If a role in outer domain cannot be understood by local domain, it can define such a simple policy: regarding all the roles of outer domain as role "Guest" in local domain, that is the association from GuestH_1 to GuestH_0 (label 3). However, since all of the roles in outer domain are regarded as the same kind of role ("Guest"), this method is obviously not flexible enough.

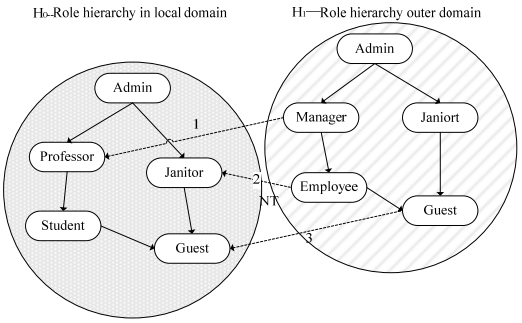

Figure 4. Associations between role hierarchies

In this framework a combination of partial order relations are developed by adding a series of associations between the two role hierarchies. By this mechanism, you can easily manage the access level of a role in foreign domain. Each role in foreign domain regards the maximum role that is allowed as the converted role in local role hierarchy.

Implementation process is as follows:

(1) Security officer in local domain establishes associations by means of role editor.

(2) The strategy server traverses all of the associations and constructs a list of all the entry points of local roles.

(3) Subject in foreign domain provides local strategy server with its certificate.

(4) The server will add the entry list of the subject to the certificate of roles in outer domain and then finish the role translation.

V. SIMULATIONS AND PERFORMANCE ANALYSIS

In order to evaluate the efficiency and performance of the cross-domain access control model in cloud computing proposed in this paper, a simulation experiment using a cloud computing simulation software CloudSim is designed. The simulation environment consists of two cloud computing domains: computer cluster (including 32 nodes) and a local area network (including 20 personal computers). The purpose of the experiment is to validate the relative advantages of the trust based access control model across domain in contrast with the traditional access control models and measure the rationality of trust evaluation. The experiment is divided into two parts:

A. The Comparison of Trust-based Access Control and Role-based Access Control

In this experiment, it will compare the trust-based access control model proposed in this paper with RBAC model. The user entity sends resource access requests simultaneously to trust-based access control system and RBAC system. And the two systems authorize the user according to their access control rules. Relevant parameters of trust based access control model are shown in table I. As time goes on, the numbers of accessible

resources change in the two systems. The result obtained by the experiment is shown in Fig.5. It is shown that the number of accessible resources of the user entity is constant in RBAC system, while in trust-based access control system that number changes along with trust degree. Hence, the trust-based model proposed in this paper has fine granularity.

TABLE I

RELEVANT PARAMETERS

Descriptions	Parameters	Values
Weight of direct trust in k-1 times interactions	α	0.5
Weight of service satisfaction value	β	0.45
Weight of direct trust in k times interactions	γ	0.5
Direct trust between n_i and n_j.	$DTD(n_i, n_j)$	0.3

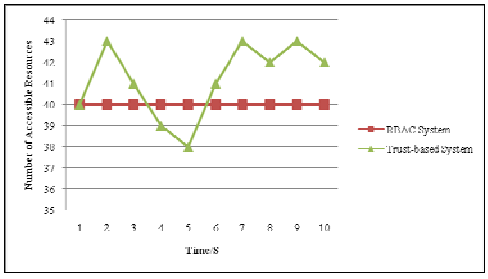

Figure 5. The numbers of accessible resources in different systems

B. The Comparison of Trust Evaluation and Other Methods

The superiority of trust evaluation algorithm in this paper and other calculation method are compared through success rate of cloud computing services. The success rate of cloud computing services means the proportions of successful times of the total number of cloud services. It is shown in Fig.6 that the success rate of traditional access control method decreases as time goes on, while success rate of trust evaluation method is higher and changes dynamically. Entities with a higher trust degree have a larger number of accessible resources and a higher success rate of cloud services.

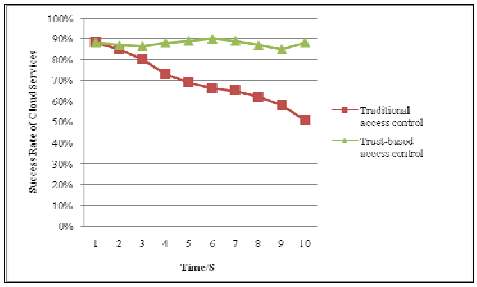

Figure 6. Success rate of cloud services

VI. CONCLUSION

In conclusion, this paper discussed access control in cloud computing environment and proposed a trust-based access control model in multi-domain, which combined with RBAC mechanism. The author discussed access control policies in local domain and cross-domain, respectively. In local domain, access control policy includes role assignment, trust management, authentication and authorization. Besides, access control cross-domain involved as well as role translation. The author converted roles of outer domain into roles of local domain by means of role association. Moreover, it performed trust management, authentication and authorization. In cloud computing, the application of trust-based access control and the consideration of the features of multi-domain can be more intuitive and effective in protecting the security of cloud users and cloud computing platform.

ACKNOWLEDGEMENTS

This paper is supported by the Opening Project of State Key Laboratory for Novel Software Technology of Nanjing University of China under Grant No.KFKT2012B25), and Youth Foundation by Beijing University of Posts and Telecommunications under Grant No.2013RC0308.

REFERENCES

[1] Jiyi Wu, Qianli Shen, Tong Wang, "Recent advances in cloud security," *Journal of Computers*, vol. 6, no. 10, 2011.

[2] Dengguo Feng, Min Zhang, Yan Zhang, "Study on cloud computing security," *Chinese Journal of Software*, vol. 22, no. 1, pp. 71-83, 2011.

[3] Xuri Chen, Weimin Xu, Wenfeng Shen, "Trustworthiness-based dynamic access control for grid application," *Journal of Hunan University (Natural Sciences)*, vol. 35, no. 7, pp. 85-89, Jul. 2008.

[4] Chen Jincui, Jiang Liqun, "Role-based access control model of cloud computing," *Energy Procedia 13*, pp. 1056-1061, 2011.

[5] Bo Lang, "Access control oriented quantified trust degree representation model for distributed systems," *Journal on Communications*, Dec. 2010.

[6] Wu Liu, Haixin Duan, Hong Zhang, "TRBAC: trust based access control model," *Journal of Computer Research and Development*, Aug. 2011.

[7] Zhanjiang Tan, Zhuo Tang, Renfa Li, Ahmed Sallam, Liu Yang, "Research on trust-based access control model in cloud computing," *Proceedings of 6th ICPCA*, 2011.

[8] Wenhui Wang, Jing Han, Meina Song, Xiaohui Wang, "The design of a trust and role based access control model in cloud computing," *Information Technology and Artificial Intelligence Conference (ITAIC)*, 2011 6th IEEE Joint International.

[9] Santos N, Gummadi KP, Rodrigues R. "Towards trusted cloud computing," *In: Sahu S, ed, USENIX Association Proc. of the Workshop on Hot Topics in Cloud Computing 2009. San Diego*, 2009. http://www.usenix.org/events/hotcloud09/tech/full_papers/santos.pdf

[10] Sadeghi AR, Schneider T, Winandy M. "Token-based cloud computing: secure outsourcing of data and arbitrary computations with lower latency," *In: Proc. Of the 3rd Int'1 Conf. on Trust and Trustworthy Computing. Berlin: Springer-Verlag*, pp. 417-429, 2010.
[11] Junzhou Luo, Xudong Ni, Jianming Yong, "A trust degree based access control in grid environments," *Information Sciences*, pp. 2618–2628, 2009.
[12] T. Grandison, M. Sloman, "A survey of trust in Internet applications," *IEEE Communications Surveys and Tutorials*, 2000.
[13] Junchang Song, Cheng Su, "Using trust in access control mechanism," *Computer Engineering and Design*, Oct. 2007.
[14] Beth T., Borcherding M., Klein B. "Valuation of trust in open networks," *Proceedings of the Third European Symposium on Research in Computer Security*, *Brighton: Springer-Verlag*, pp. 3-18, 1994.
[15] Jϕsang A. "A logic for uncertain probabilities," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 9, no. 3, pp. 279-311, 2001.
[16] Apu Kapadia, Jalal Al-Muhtadi, R. Campbell, et al. "IRBAC 2000: secure interoperability using dynamic role translation," *University of Illinois, Technical Report: U I-UCDCS-R-2000-2162*, 2000.
[17] Liangmin Guo, Yonglong Luo, Zhengzhen Zhou, Meijing Ji, "A recommendation trust method based on fuzzy clustering in P2P networks," *Journal of Software*, vol. 8, no. 2, pp. 357-360, Feb. 2013.
[18] Weiliang Zhao, Varadharajan V, Bryan G. "General methodology for analysis and modeling of trust relationships in distributed computing. *Journal of Computers*, vol. 1, no. 2, pp. 42-53, 2006.
[19] Dongyan Jia, Fuzhi Zhang, Sai Liu, "A robust collaborative filtering recommendation algorithm based on multidimensional trust model," *Journal of Software*, vol. 8, no. 1, pp. 11-18, Jan. 2013.

Guoyuan Lin was born in Shandong, China in the year of 1975. He is now an associate professor at China University of Mining and Technology. He obtained his Ph.D. from Nanjing University in 2011. His research interests are information security and intrusion detection.

He works in China University of Mining and Technology for nearly 15 years since 1997. With the first author or instruction graduate student announce thesis more than 20 articles, among them abroad magazine's announcing to combine be registered a thesis 1 by the SCI and 11 by the EI. He published three books including: Computer Operating System(Beijing, China: Tsinghua University Press, 2011). His current research interests are information and network security, cloud computing security.

Yuyu Bie is now a postgraduate at China University of Mining and Technology, Xuzhou, China. She was born in 1990, Shandong, China. She received the B.Eng. in School of Computer Science and Technology at China University of Mining and Technology in 2011. Her main research interests include information system security, access control and cloud computing.