Hindawi Publishing Corporation
Journal of Electrical and Computer Engineering
Volume 2016, Article ID 9820590, 8 pages
http://dx.doi.org/10.1155/2016/9820590

Research Article

Cloud Multidomain Access Control Model Based on Role and Trust-Degree

Lixia Xie and Chong Wang

School of Computer Science and Technology, Civil Aviation University of China, No. 2898, Jinbei Road, Tianjin 300300, China

Correspondence should be addressed to Lixia Xie; lxxie@126.com

Received 10 November 2015; Accepted 22 February 2016

Academic Editor: Hui Cheng

In order to solve the problem of access control among different security domains in cloud networks, this paper presents an access control model based on role and trust-degree. The model combines role-based access control and trust-based access control. The role assessment weights are defined based on the user's role classes, and the trust-degree is calculated according to the role assessment weights and the role's behavior. In order to increase the accuracy of access control, the model gives the concept and calculation methods of feedback trust-degree. To achieve fine-grained access control, the model introduces direct trust-degree, recommendation trust-degree, and feedback trust-degree, all of which participate in comprehensive trust-degree by adjusting their weights. A simulation experiment was conducted in the LAN environment, and a web system was used to construct an access control model with multisecurity domains in the experiment. The experimental results demonstrate that our model has higher security, expansibility, and flexibility.

1. Introduction

With the rapid development of network technology and cloud computing, attacks and interactions are becoming more and more frequent; complex network security situation will be more serious. By controlling the access permission of the key resources, access control achieves the protection of system resources, ensuring that all of the main direct entrances to the object are authorized and preventing legitimate users from using illegal access to system resources at the same time. Access control policy is one of the main strategies of network security and the main method to realize data confidentiality and integrity [1]; it has become the important subject in the area of network security.

At present the commonly used access control policy includes discretionary access control, mandatory access control, and role-based access control [1]. Due to the arbitrariness in users' privileges transfer, discretionary access control is unable to ensure the security of the system, and it is not conducive to achieving a unified global access control. In addition, it is easy for the protected information to leak, and it can not resist the Trojan horse attacks in this access control policy [2]. However, the mandatory access control is no interference access control. Due to its reinforcement in access restrictions, the system flexibility declines, and the application is limited. At present, this policy is mainly used in military and the field which has obvious hierarchies and the high security requirement. Role-based access control is different from the above two kinds of access control policy and develops rapidly. It combined with existing security technologies. A variety of access control models emerged. Reference [3] proposed a C/S structure of trust decentralized access control (TDAC) framework: through the client's temporary monitors and server-side assessment of the primary monitor application access request in the subject context-aware access control to protect private data. The defects of this method are increasing the burden to clients and servers. When error occurs in the clients, the servers will not easily detect and repair it. Reference [4] proposed a flexible access control strategy, and the strategy ensures that when users are offline, independent user groups still have the right to perform critical tasks, but the performance of this strategy should be improved. Reference [5] proposed a comprehensive encryption-based access control framework for the content

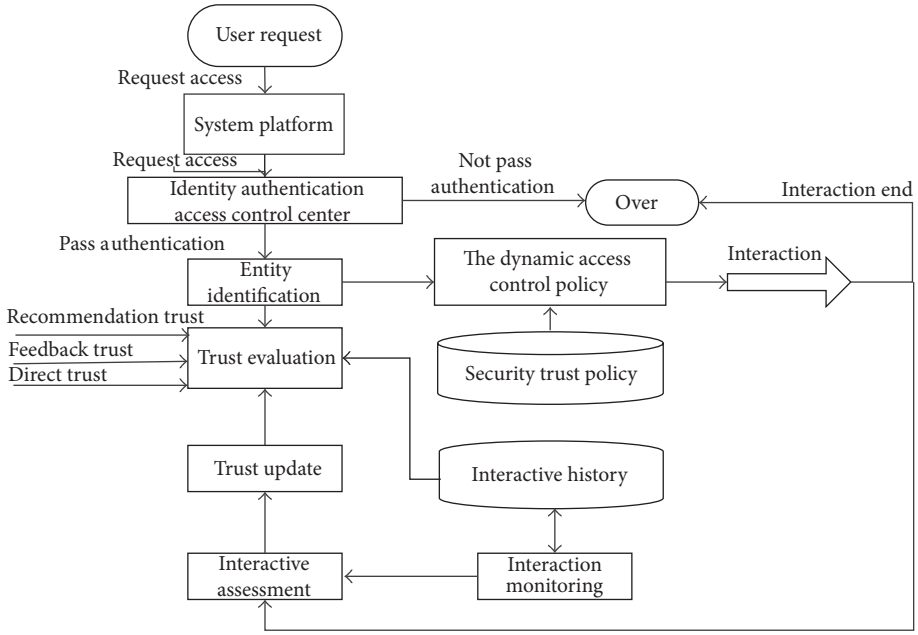

Figure 1: Framework of role and trust-based access control.

centric network; it was also extensible and flexible. The design of the framework mostly relied on secure content objects' concept. It also implemented two access control schemes, group-based access control and broadcast access control, to demonstrate the flexibility. Reference [5] proposed a hybrid access control model. It combined the advantage of both type enforcement model and role-based access control. It enabled unified access control and authorization for IaaS clouds and the permission transition framework was also provided to dynamically assign permission to virtual machines. This paper puts forward the access control that is based on roles and trust method, the concept of feedback credibility, and the role of trust evaluation weight. It also combined with direct trust and recommended trust to evaluate the user's access behaviors [6]. It realizes the dynamic fine-grained access control.

2. Model Framework

The framework which is based on role and trust entity access control is shown in Figure 1. It describes the relationship of each component. The framework mainly includes the entity recognition and trust management. The following paragraphs will give instructions about the two parts.

2.1. Entity Recognition. The framework of the entity recognition [6] is mainly used to identify the login entity components (user) level, so as to obtain the trust evaluation weights used in the subsequent fine-grained trust evaluation. Entity recognition features include the foreign entity visit and entity mapping, in the process, if the entity for anonymous entity will not affect the interaction with other entities.

If the anonymous entity has the identity of the lowest level, conforming to the resource access trust threshold can also be carried out in accordance with the established process interaction. The anonymous entity in the process of the session by the trust through the above framework participates in the trust evaluation; in order to avoid malicious slander, anonymous users' trust evaluation will not be involved. Entity recognition process is shown in Figure 2.

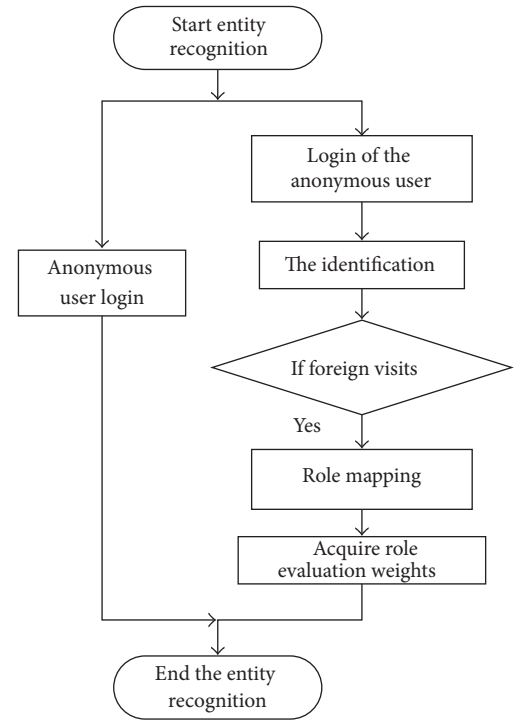

Figure 2: Entity recognition process.

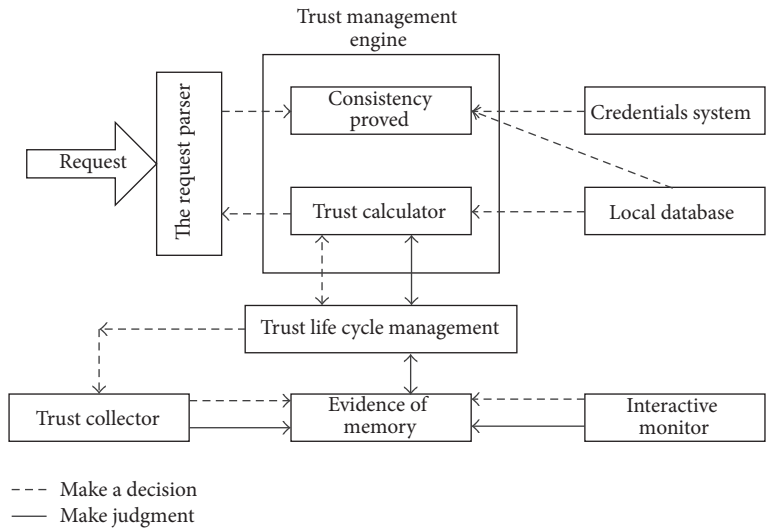

Figure 3: Trust management model structures.

2.2. Trust Management. Trust management include computing, collecting, and updating the trust. Trust management model structure is shown in Figure 3. Trust computation can be divided into three parts: interactive entity directly trusted computing, feedback trust computation, and other entities in the recommendation trust computing network. In the process of the above calculation, it gives three kinds of calculation results of different weight coefficient.

If interactive entities are new members of the network, we give an initial trust value and assign certain access permissions through a third-party authority. The entities that are out of the system also can use anonymous entity. The system automatically assigned a smaller trust value and the role of a minimal operation.

At present the commonly used access control models mainly include discretionary access control, mandatory access control, and role-based access control. Due to discretionary access control permissions to users with the transfer of the arbitrariness result in the decrease of the safety of the system. This is not conducive to achieving a unified global access control. The information leaks easily. It can not resist the Trojan horse attacks in the access control model. However the mandatory access control has no interference of access control, due to its access restrictions for the reinforcement, thus affecting the flexibility of the system. Role-based access control is different from the above two kinds of model. It obtained a rapid development and combined with some existing security technologies derived from a variety of access control model.

3. Role and Trust

Principal component analysis (PCA) is a mathematical transformation method [3], and it is used to reduce data dimension. It can switch the multidimensional data into several major dimensional data. The main problems that need to be solved in the role management include the role mapping, the strategy of role adding and deleting, and role conflict resolution strategy. Set up the weight of participation trust-degree evaluation according to the level and this is role evaluation weight:

(1) Role mapping: when two equivalent security domains visit each other's resources, each should map the role in this domain to target resources domain's role. In access control model system proposed in this paper, the distrust security domain and trust security domain take different role mapping strategies.

(2) Adding the role: upon adding new roles, new role mapping's strategy is automatically generated according to the model's mapping strategy.

(3) Deleting the role: upon deleting a domain role, the mapping will be replaced until mapping this role to its subrole.

(4) Role conflict resolution: in this paper, the solution of role conflict of access control is to allow the outland role to have the right of the highest conversion role mapping.

(5) The role of trust evaluation: set up different roles according to the user in the access control security domain model and the role of the various security domains, each role assigned different weights of evaluation, and the higher weights reflect the higher user level permissions.

Table 1 is a sample which is set in the simulation experiments depending on the set role rank and role evaluation weight values, in a real environment, according to the need to set more user levels and evaluation weights which are fit for the level.

According to literature [4], the time t node n_i direct trust-degree is defined as $D(n_i, n_j, t)$. A direct trust table is distributed to the network nodes. Each cell in the table is the node for direct interaction. According to the direct trust table of all nodes to build a two-dimensional direct trust

Table 1: Example of rolegrade and role weight evaluation.

Role level	Role description	Evaluation weights
1	Total access control center administrator	1.00
2	Access control security domain administrator	0.95
3	Security component user	0.90
4	Anonymous users or components	none

relationship matrix [3], defining it as M_1, nodes n_i to node n_j direct trust is represented by $M_1(n_i, n_j)$.

At time t, if nodes n_i and n_j have an interaction, the direct trust $D(n_i, n_j, t)$ is

$$D\left(n_i, n_j, t\right) = M_1\left(n_i, n_j\right) e^{-(t-t_{ij})}, \quad t - t_{ij} \geq 0, \tag{1}$$

where $e^{-(t-t_{ij})}$ is time decay function. It describes the case that direct trust declines with time passing by.

If nodes n_i and nodes n_j have had interactions many times at time t, the direct trust is shown by mean value

$$D\left(n_i, n_j, t\right) = \frac{\sum_{k=1}^{I(k)} S\left(n_i, n_j, t_k\right) e^{-(t-t_k)}}{I\left(k\right)}, \quad t - t_k \geq 0, \tag{2}$$

where $\sum_{k=1}^{I(k)} S(n_i, n_j, t_k) e^{-(t-t_k)}$ is interaction evaluation expectations of nodes n_i and n_j after every interaction evaluation, $I(k)$ represents the times when nodes n_i and n_j have interactions frequency in time t. Based on literature [5], define recommendation trust $R(n_i, n_j, t)$ at time t of node n_i to node n_j:

$$R\left(n_i, n_j, t\right) = W_i \times D\left(n_i, n_j, t\right). \tag{3}$$

Recommendation trust of node n_j is given by recommended node n_i's evaluation of n_j. Trust evaluation weight is represented by w_i, defined as follows:

$$W_i = e^{-1/\sum_{k=1}^{I(k)} S(n_i, n_j, t_k) e^{-(t-t_k)}}. \tag{4}$$

On the basis of direct trust, this paper puts forward the concept of feedback trust and gives the calculation method of feedback credibility. Different from direct trust and recommendation trust, feedback trust is the evaluation which represents the feedback of their own behaviors. The feedback helps users adjust trust behavior quickly.

Definition 1. Feedback trust is a kind of excitation mechanism that users are responsible for their access behavior [6]. According to regulations, users can use information resources in the system safely and reliably; this will improve their trust and have permissions of enjoying more safe and reliable services.

In the access control model proposed in this paper, for every node n_i establish a two-dimensional feedback trust matrix. It records all the feedback trust between all nodes. The feedback trust of node n_i to node n_j is represented by $M_2(n_i, n_j)$.

At time t, the feedback trust of node n_i to node n_j is defined as $F(n_i, n_j, t)$:

$$F\left(n_i, n_j, t\right) = M_2\left(n_i, n_j\right) e^{-(t-t_{ij})}, \quad t - t_{ij} \geq 0, \tag{5}$$

where $e^{-(t-t_{ij})}$ is time decay function.

Formula (5) is considering that the interaction time is only once. If nodes n_i and n_j interact many times, the users' operations feedback trust computing takes interaction average:

$$F\left(n_i, n_j, t\right) = \frac{\sum_{k=1}^{I(k)} X\left(n_i, n_j, t_k\right) e^{-(t-t_k)}}{I\left(k\right)}, \quad t - t_k \geq 0. \tag{6}$$

$X(n_i, n_j, t_k)$ represent moment t_k and node n_i feedback operation evaluation to n_j, taking value interval as $[0, 1]$. In formula (6), $\sum_{k=1}^{I(k)} X(n_i, n_j, t_k) e^{-(t-t_k)}$ is the evaluation of each interaction expectation after nodes n_i and n_j interaction evaluation and attenuation. $I(k)$ represent node n_j and n_i interactions times within the time t. Direct trust, recommendation trust, and feedback trust describe the user's trust from different views [7]. All are defined as comprehensive trust. It can describe user trust comprehensively and accurately. For arbitrary nodes n_i and n_j, then

$$T\left(n_i, n_j, t\right) = D\left(n_i, n_j, t\right) + R\left(n_i, n_j, t\right) + F\left(n_i, n_j, t\right), \tag{7}$$

where the comprehensive trust of node n_i to node n_j is represented by $T(n_i, n_j, t)$ at time t. When there are third-party authentication institutions to participate in the trust evaluation, nodes n_i, n_j formula of comprehensive trust at time t can be expressed as

$$\begin{aligned} &T\left(n_i, n_j, t\right) \\ &\quad = \text{status}\left(n_i, n_j, t\right) \\ &\qquad \wedge \left[D\left(n_i, n_j, t\right) + R\left(n_i, n_j, t\right) + F\left(n_i, n_j, t\right)\right], \end{aligned} \tag{8}$$

where status(n_i, n_j, t) is a state function, representing the allowance of n_i to n_j at time t. status(n_i, n_j, t)'s value is 0 representing identity permission, 1 indicating identity is not allowed. If the interaction time is too long, the trust declines with time. The status of the current network node can not reflect trust by direct trust $D(n_i, n_j, t)$, and recommendation trust $R(n_i, n_j, t)$ and feedback credibility $F(n_i, n_j, t)$ can accurately reflect the current state of the node [8]. After calculating the direct trust $D(n_i, n_j, t)$, recommendation trust $R(n_i, n_j, t)$, and feedback credibility $F(n_i, n_j, t)$, comprehensive trust is calculated:

$$\begin{aligned} &T\left(n_i, n_j, t\right) \\ &\quad = \text{status}\left(n_i, n_j, t\right) \\ &\qquad \wedge \left[\alpha D\left(n_i, n_j, t\right) + \beta R\left(n_i, n_j, t\right) + \gamma F\left(n_i, n_j, t\right)\right], \end{aligned} \tag{9}$$

where $\alpha + \beta + \gamma = 1$, $\alpha \geq 0$, $\beta \geq 0$, $\gamma \geq 0$.

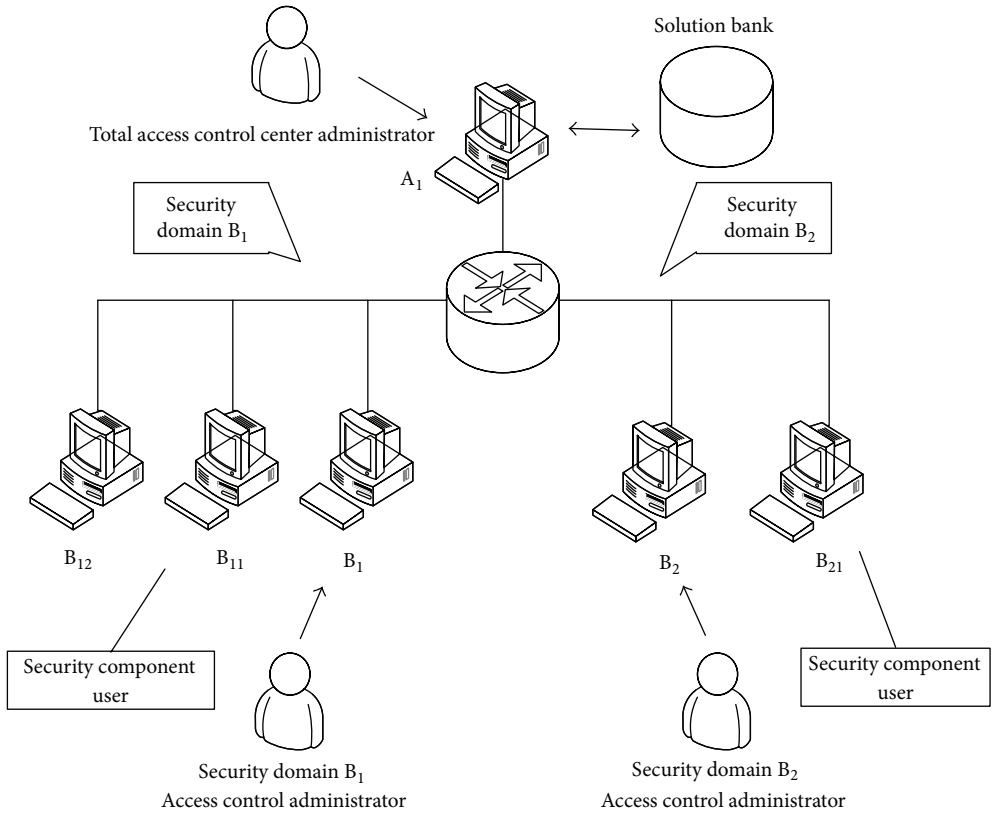

Figure 4: Simulation model structures.

If the security component is the service provider, it does not have feedback trust in practical situation [9]. Under this condition, the comprehensive trust is

$$T\left(n_i, n_j, t\right) = \text{status}\left(n_i, n_j, t\right) \wedge \left[\alpha D\left(n_i, n_j, t\right) + \beta R\left(n_i, n_j, t\right)\right], \tag{10}$$

where $\alpha + \beta = 1$, $\alpha \geq 0$, $\beta \geq 0$. Similarly, if a certain security component does not provide services and resources, it does not have direct trust [10]. Under this condition the trust is

$$T\left(n_i, n_j, t\right) = \text{status}\left(n_i, n_j, t\right) \wedge \left[\beta R\left(n_i, n_j, t\right) + \gamma F\left(n_i, n_j, t\right)\right]. \tag{11}$$

Among them, $\beta + \gamma = 1$, $\beta \geq 0$, $\gamma \geq 0$.

4. Experiments

The experiments are done in the laboratory's LAN environment. A server is the general access control center, two PC represent two different domain management centers, and the other three PC represent the security components of different domains. Simulation model structure is shown as in Figure 4. In Figure 4, A_1 is model access control center which is responsible for user management and providing safe trust policy, dynamic access control, interactive assessment, and trust evaluation. B_1 and B_2 are the domain management centers which manage their security domain. B_{11}, B_{12}, and B_{21} belong to the security domain security components of security domains B_1 and B_2.

Simulation model is using B/S structure, so the B_{11}, B_{12}, and B_{21} do not need to deploy any function module, simply by IE login and connecting to the corresponding access control center module and interacting with other security components.

In the process of simulation experiment, by different user login access control system and other security components interaction access and access control center do corresponding actions in the process of access control. In order to achieve the legitimate users access to legal resources, illegal user cannot access resources, and the legal user cannot access illegal resources.

5. Experimental Process and Results

In the simulation model, userb_{12} and userb_{11} were two security components in security domain B_1. In the process of creating security component of model, users were given 0.7 as initial recommendation trust.

Different user roles grading to ascertain the weight of character evaluation values is according to Table 1 and, in the initial stages, defined on the relationship between the credibility and trust, as shown in Table 2.

At this time the direct trust and feedback trust were 0. In the model the user creates immediate access to the test,

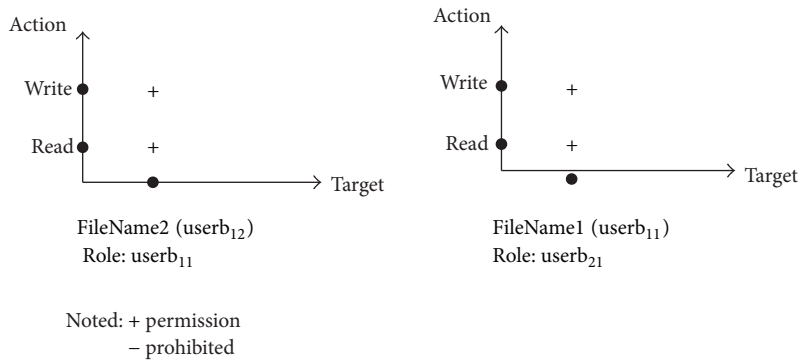

Figure 5: Access policies of userb_{11} and userb_{12}.

Table 2: Definition of trust status.

Trust *value t*	Trust situation
$0 \le t < 0.5$	Do not *trust*
$0.5 \le t < 1$	Relative *trust*
$t = 1$	Total *trust*

Table 3: Weights of the three trust degrees.

Right to direct *trust value* α	Recommendation trust weights β	Feedback trust weights γ
0.35	0.3	0.35
0.6	0.4	0.0
0.0	0.5	0.5
0.0	1.0	0.0

so at this time of attenuation it is negligible (the results approximately equal 0.7), so the first degree of trust visits is

$$T\left(n_i, n_j, t\right) = \alpha D\left(n_i, n_j, t\right) + \beta R\left(n_i, n_j, t\right) + \gamma F\left(n_i, n_j, t\right), \tag{12}$$

where $\alpha + \beta + \gamma = 1$, $a \ge 0$, $\beta \ge 0$, $\gamma \ge 0$.

Calculated by formula (1)–(11) $T(\text{userb}_{11}, \text{userb}_{12}, t_0) = T(\text{userb}_{12}, \text{userb}_{11}, t_0) \approx 0.7$; that is, at time t_0, component userb_{11} access to components userb_{12} trust is 0.7; at the same time userb_{12} access to userb_{11} trust was 0.7. Based on the model set userb_{11} resources "document 1" literacy reading and writing trust-degree threshold were 0.5 and 0.7. userb_{12} have the read and write permissions to "document 1."

Userb_{11} is used for designing experiment of userb_{12} access control policy as shown in Figure 5. Ordinate Action represents access Action, including two operations which are write and read. Abscissa represents the Target resources.

userb_{11}, for resources "document 2" after the read operation, calculated userb_{12} providing services for direct trust evaluation of 0.9, according to type (12) to calculate the trust at this time $T(\text{userb}_{11}, \text{userb}_{12}, t_1) = 0.788$. According to "document 1" userb_{11} setting threshold, userb_{12} still have permissions to read and write. If userb_{12} provides the unsafe service, on a visit to "document 2" again, after access to direct trust evaluation is set to 0.5, according to type (10) one gets $T(\text{userb}_{11}, \text{userb}_{12}, t_2) = 0.644$. At this point, according to userb_{11} access to resources "document 1" trust threshold setting, userb_{12} has only permissions to read and lost permissions to write, and it is through this mechanism that users are motivated to provide more safe and reliable service. If userb_{12} has access components provided by certain standard judged to be extremely dangerous, relevant access components or the administrator can delimit userb_{12} directly into the blacklist, causing its loss of the appropriate minimum component resources access.

userb_{11} to userb_{12} resources for access to the direct trust evaluation are calculated; at the same time, userb_{12} feedback on userb_{11} for trust evaluation is calculated by formula (9) trust and synchronous update in the database. Through this mechanism they can exercise the power of their own incentive component, safer permissions to read and write, and so forth.

The detailed testing results of all kinds of trust weight value are shown in Table 3. For different access requirements of the system, the setting of the weight of all kinds of trusts is also different. It reflects the flexibility of the model. Based on the definition of various types of trust, the following conclusion can be drawn.

The test results can be seen from Table 3; when evaluating trust gradually reduced, the trust declined. On the contrary, when a user provided good service and safe and reliable resources or used their legal rights, it had the higher credibility evaluation. Thus the total trust increased. The experimental results showed the feasibility and effectiveness of the proposed access control mode.

Experiments of all kinds of trust weight value settings are shown in Table 3. For different access requirements of the system, the setting of the weight of all kinds of trust also is different; it also reflects the flexibility of the model. Based on the definition of various types of trust one can draw the following conclusion. When direct trust weight value is bigger, the user's comprehensive trust continued volatility may occur; for example, for some security component trust evaluation is more matching and for other components trust is completely opposite. When the recommendation trust

Table 4: Test result.

Users	Comprehensive trust	Target resource	Operation	Result	Trust evaluation/role level
$Userb_{11}$	0.7000	Document 2	Read	0: action succeeded	0.90/1, 0.90/3
$Userb_{12}$	0.8200	Document 1	Read	0: action succeeded	0.85/1, 0.85/3
$Userb_{11}$	0.8225	Document 2	Write	0: action succeeded	0.80/1, 0.80/3
$Userb_{12}$	0.8050	Document 1	Write	0: action succeeded	0.75/1, 0.75/3
$Userb_{11}$	0.7875	Document 2	Read	0: action succeeded	0.70/1, 0.70/3
$Userb_{12}$	0.7452	Document 1	Read	0: action succeeded	0.65/1, 0.65/3
$Userb_{11}$	0.6378	Document 2	Write	1: action is not allowed	0.60/1, 0.60/3
$Userb_{12}$	0.5968	Document 1	Write	1: action is not allowed	0.55/1, 0.55/3
$Userb_{11}$	0.4968	Document 2	Read	1: action is not allowed	0.50/1, 0.50/3
$Userb_{12}$	0.4658	Document 1	Read	1: action is not allowed	0.45/1, 0.45/3
$Userb_{11}$	0.3847	document 2	Write	1: action is not allowed	0.40/1, 0.40/3

weight value is bigger, the user's comprehensive trust value is relatively stable.

When feedback trust weight value is larger, comprehensive trust users access to the current user behavior is more sensitive and can quickly reflect the current access behavior trust situation. In general according to the different requirements of different systems all kinds of trust weight value can be set. This also can make all kinds of trust weight values roughly equal. The weights of three kinds of trust assignment are shown in Table 3.

In Table 3, the first line says three types of trust are the weights of evaluation. The second line indicates only direct trust and recommendation trust weights. The third line showed only recommendation trust and feedback trust weights. In the fourth row only recommendation trust weights are shown. Recommendation trust in the building of a role is given, so it is inevitable.

Detailed test results are shown in Table 4. Initial conditions are as follows: system building role given recommended trust being 0.7, the name of documents 1 and 2, and speaking, reading, and writing trust threshold being 0.5 and 0.7. Detailed test of read and write operations alternates, initial interaction evaluation value is 0.9; read and write interactive evaluation is reduced to 0.05.

6. Conclusions

This paper puts forward a kind of access control method based on the character and credibility. It also puts forward the concept of feedback credibility and the role of trust evaluation weight, combined with direct trust and recommendation trust. Direct trust and recommendation trust all evaluate the user's access comprehensive action. The effectiveness of the proposed model is verified by simulation.

The test results can be seen from Table 4; when evaluating trust gradually reduced, the trust will drop. On the other hand, when a user provides good service and safe and reliable resources or exercises their GeFaQuan period, it will get higher credibility evaluation; thus the total trust will be increased.

Design of access control model in this paper is through such mechanism incentive component users with better service and more safe and reliable resources and more effective exercise of their rights and increase of their trust, so as to enjoy a higher authority. Based on user roles we set different weights of evaluation and give the weight of different trust to achieve fine-grained trust evaluation and credibility in order to achieve the fair and reasonable evaluation purpose. The test results of Table 4 show that the access control model proposed in this paper is feasible and effective.

Competing Interests

The authors declare that they have no financial and personal relationships with other people or organizations that can inappropriately influence their work, and there is no professional or other personal interest of any nature or kind in any product, service, and/or company that could be construed as influencing the position presented in, or the review of, this paper.

References

[1] G. Jun, *Research on the Hierarchical Authorization Management of Role-Based Access Control*, Xidian University, Xi'an, China, 2012.

[2] S. Barker, M. J. Sergot, and D. Wijesekera, "Status-based access control," *ACM Transactions on Information and System Security*, vol. 12, no. 1, pp. 1–47, 2008.

[3] W. Han, M. Xu, W. Zhao, and G. Li, "A trusted decentralized access control framework for the client/server architecture," *Journal of Network and Computer Applications*, vol. 33, no. 2, pp. 76–83, 2010.

[4] N.-H. Li, M. V. Tripunitara, and Q.-H. Wang, "Resiliency policies in access control," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 113–123, ACM Press, 2009.

[5] J. Kuriharay, E. Uzun, and C. A. Wood, "An encryption-based access control framework for content-centric networking," in *Proceedings of the 14th IFIP Networking Conference*, pp. 1–9, IEEE, Toulouse, France, May 2015.

[6] C. Zhou and B. Li, "iHAC: a hybrid access control framework for IaaS clouds," in *Proceedings of the IEEE/ACM 7th International Conference on Utilty and Cloud Computing (UCC '14)*, pp. 853–858, London, UK, December 2014.

[7] W. Tolone, G. J. Ahn, and T. Pai, "Access system," *Journal of ACM Computing Surveys*, vol. 37, no. 1, pp. 29–41, 2005.

[8] S. Barker, M. J. Sergot, and D. Wijesekera, "Status-based access control," *ACM Transactions on Information and System Security*, vol. 12, no. 1, article 1, 2008.

[9] W. Liang and G. Ya-Jun, "Reputation-based on trust evaluation mechanism for P2P system," *Computer Engineering and Applications*, vol. 45, no. 15, pp. 136–138, 2009.

[10] S. Ma, J. He, and F. Gao, "An access control model based on multi-factors trust," *Journal of Networks*, vol. 7, no. 1, pp. 173–178, 2012.