Evaluation and Analysis on Security Framework Model of Cloud Computing

Zhao Li[1, a]

[1]Wuhan Donghu University，School of computer Science,Wuhan, Hubei,420000,China

[a]lizhao0920@163.com

Keywords: cloud computing, security framework, trust model, structure

Abstract. as for the trust model in the past neglects trust fuzziness and dynamic and it can not precisely reflect trust relations, this paper relies on idea of fuzzy logic and it puts forward evaluation model of cloud computing based on fuzzy trust, uses fuzzy comprehensive judgment method to calculate trust rank of fuzzy, establishes fuzzy control rule and authorizes cloud users corresponding authority by fuzzy decision. It introduces into time factor on calculating trust rank, which enables it better satisfy requirement of access control in the cloud computing environment. It effectively enhances security of cloud computing platform by establishing double trust and evaluation.

Introduction

Cloud computing is another new calculation model after distributed computing[1], grid computing[2] and peer to peer computing[3] , it uses resources lease, application hosting and service outsourcing as core, which quickly becomes to be the hot point in computer technology development. Under cloud computing environment, the idea of service according to one's needs in IT field obtains real indication, cloud computing can meet customized requirements of users by integrating distributed resources and establishing calculation environment of dealing with plenty of service requirements, which can realize decoupling of system management and maintenance as well as service and application. How to use relevant outcome of cloud computing to promote development in national economy and the people's livelihood has become to be the important part for development strategy of China.

As for the security danger caused by characteristics such as dynamic, multiple-leaser and higher extendibility etc in the cloud computing environment, this paper put forward evaluation model TBFEM of cloud computing based on fuzzy trust by relying on idea of fuzzy logic, it applies fuzzy comprehensive judgment method to calculate trust degree of cloud service, meanwhile cloud service supplier establishes fuzzy control rule and authorizes cloud users corresponding authority by fuzzy judgment, it introduces into time factor on calculating trust degree, which can enable it better meet requirement on dynamic access control under cloud computing environment. It effectively enhances security of cloud computing platform by establishing double trust mechanism.

Evaluation model of cloud computing based on fuzzy trust

Fuzzy evaluation model based on trust

Because of autonomy of resources distribution, different security regions have big difference in choosing access control strategy and security mechanism, state of cloud computing has necessary to establish one universal trust strategy set among every trust field. So as for cloud computing and evaluation model based on fuzzy trust, cloud computing platform has strong demand on security solutions plan based on trust.

By relying on idea of fuzzy logic, this paper puts forward TBFEM, it applies fuzzy comprehensive judgment method to calculate trust rank of cloud service, meanwhile cloud service supplier establishes rules for fuzzy control and authorizes trust rank to cloud service by fuzzy judgment, which can make it better meet requirements of access control in dynamic cloud computing environment. It

© 2015. The authors - Published by Atlantis Press

can effectively enhance security of cloud computing environment by establishing double trust and evaluation.

The elements of TBFEM model:

（1） $CSP = \{csp_1, csp_2, \ldots, csp_n\}$ is the set of cloud service supplier

（2） $US = \{us_1, us_2, \ldots, us_n\}$ is the set of cloud users

（3）One group pf certification server CA = {C A $_0$, CA_1} trusted by cloud users and cloud service supplier, here there are 2 kinds of servers, CA verification requests user identity of cloud service and keeps evaluation information corresponds tp cloud users, that is trust value, once users pass by ID verification, they can check trust value of them or other users on cloud service.

Suppose in CSP set, cloud service supplier belongs to one Dom. In the beginning stage, the cloud service supplier newly joined in Dom firstly submits information to carry out registration, the registration information includes service category, charge situation, privacy protection, the adopted security strategy, uses what kind of way to monitor system, time ratio of normal operation for service, the management strategy and standard that observe etc. Cloud users also need to choose certification server CA_0 to make registration before submitting application service to cloud service in Dom, it is mainly to submit some ID prove. The model indication of TBFEM is indicated by diagram 1.

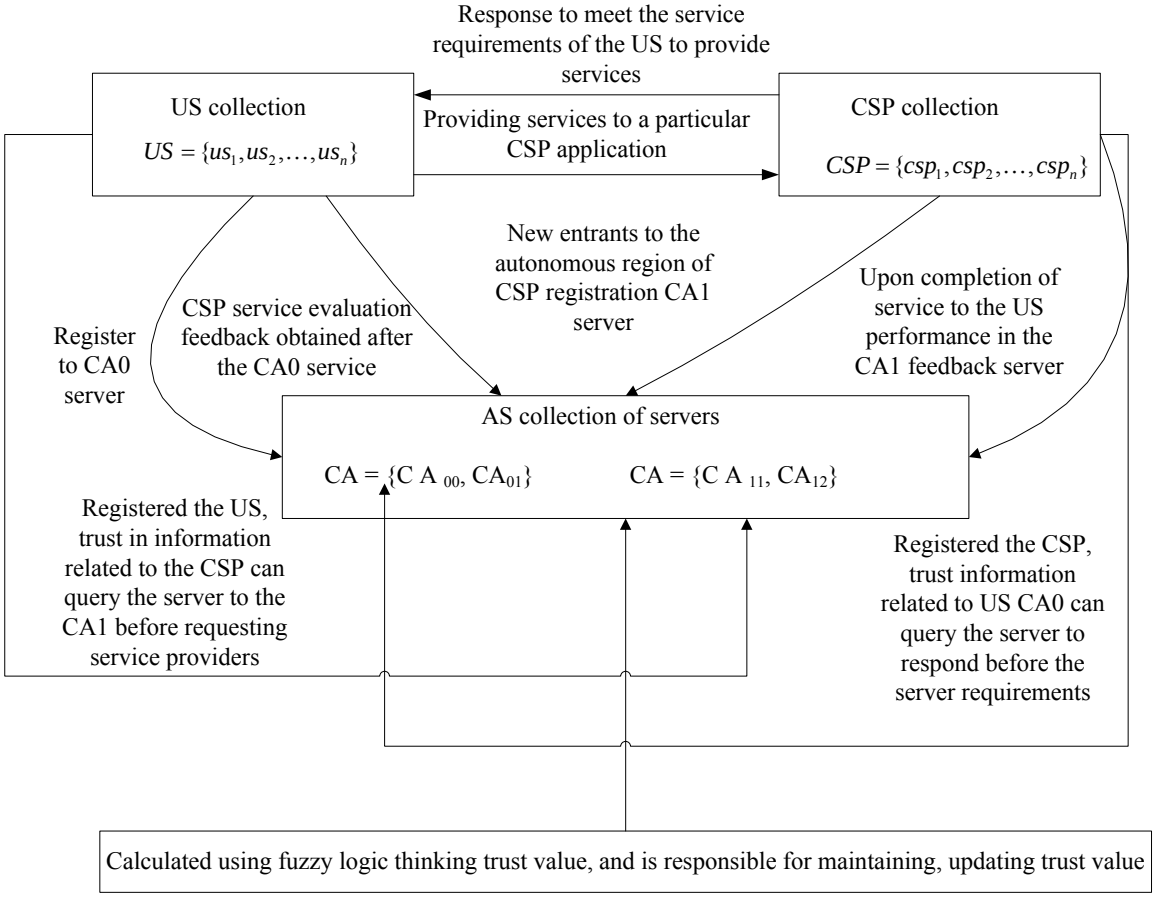

Diagram 1 TBFEM model

Cloud users and cloud service supplier need to give each other one corresponding evaluation and membership of nature trust vector after transaction is completed, these information is stored in the certification server that trusted by Dom. Of which, membership function has stronger subjectivity, it needs to make careful consideration on option, it can refer to the transaction time, transaction times and obtained authority during transaction process of the following factors.

Evaluation of cloud users on cloud service

In the Dom, CA0 also undertakes certification work of trust, it needs maintain several pieces of trust tables, of which, direct trust relations table is the information needs to feed back after cloud users using service supplied by cloud service supplier, including nature satisfaction, overall trust evaluation,

transaction background(detailed transaction project), transaction time, transaction times(except for the first time is written by users, system will add 1 according to user updating table) up to this transaction of every nature, ID information of users.

After the CSP transaction between cloud user CSU_0 and cloud service supplier is completed, it will give evaluation vector $R_{ab}=[r_1,r_2,\ldots r_n]$ of trust degree for CSP_1, which is membership vector of nature. In real condition, ever user has different satisfaction in nature of cloud service, for example, some users are concerning reliability of the whole operation process, and some users pay attention to whether extendibility of cloud service is better or not, there are also users emphasize at the fees charged for transaction for once. Here we introduce into weight vector and allow different cloud users to give higher weight values of nature that they concern, which increases the flexibility of trust evaluation.

Trust is continually and dynamically changing, it also has attenuation property, here we add attenuation function $\phi(t)$, the trust degree of cloud users CSU0 for cloud service supplier CSP 1 in certain period.

$$\varphi_{ab}(t)=R_{ab}W_t\varphi(t_i) \qquad (1)$$

Of which, W_t indicates the caring degree of users for different evaluation factors in time t, trust has attenuation property, so it adds attenuation function $\phi(t)$ on calculating trust value, its value range is from 0 to 1.

After adding attenuation function of time, the latest trust evaluation information, weight value should set higher, and vice versa. The calculation formula of time attenuation factor is as follows:

$$\varphi(t_i)=\begin{cases}1 & t=0\\ \dfrac{1}{e^{t_i}} & t\neq 0\end{cases} \qquad (2)$$

t_i indicates the time interval between current interaction time of cloud service supplier CSP 1 for cloud users CSU0 and the i interaction. With the enlargement of time internal between each other, trust degree of both is gradually becoming smaller. When time internal reaches certain degree, the trust value has already closed to zero. This kind of change trend conforms to dynamic and attenuation of trust. In the real application, certification server will automatically delete the information like trust value when it reaches certain time interval. After procession, it can enable system to obtain promotion and effective application in storage space.

Suppose there are n cloud users have transaction with cloud service supplier k in one cloud service Dom, that it has n service evaluation for k. So the credibiliy of k can be defined as follows:

$$\phi(k,t)=\sum_{i=1,i\neq k}[\varphi_{ik}(t)\lambda(i)] \qquad (3)$$

The comprehensive trust degree of cloud users a on cloud service supplier b is composed of direct trust degree of cloud users a for cloud service supplier b and recommendation of other cloud users for b, that is credibility of b is as follows:

$$\prod(a,b,t)=u\varphi_{ab}(t)+\eta\phi_{ab}(t) \qquad (4)$$

Of which, μ an d η are respectively weight, the value range of μ and η is from 0 to 1, allowing cloud users to adjust weight value by themselves. If cloud users have direct exchange with cloud service supplier, then $\mu > \eta$, so under normal condition, people are rather trust themselves, if cloud users are people are hardly to trust other people, they can also command $\mu = 1$, $\eta = 0$. Under the special condition, if cloud users have no direct transaction or no direct exchange with cloud service supplier, so cloud users can only rely on commendation and trust of other users, then it can command $\mu = 0, \eta = 1$.

Trust relations model and evaluation

As it is indicated by diagram 2, it is the trust model of cloud users to request in process of cloud service under cloud computing environment.

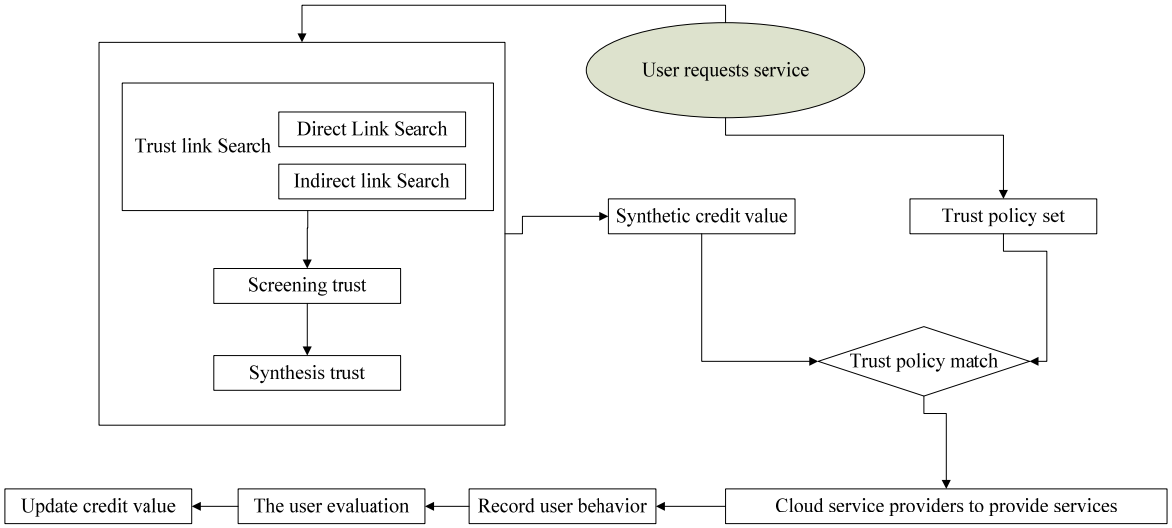

Diagram 2 Trust model of cloud users request in the cloud service process

Cloud calculation platform centralizes a large number of software and hardware resources as well as user data resources, once they are attacked by malicious users, the consequence is very serious. So it is necessary to make trust evaluation for behavior of cloud users, it should refuse to provide service for users with low credibility. The relevant definitions are as follows:

(1) Set S is the set of object trust degree, S = {S0 , S1}， S0 indicates refusing service request, S 1 indicates accept service request.

(2) Set P is fuzzy evaluation vector, P={p1 , p2,... , pn}p indicates evaluation project, it can be regarded that whether it has false operation during cloud users accept service and whether it has timely paid fees etc after service is completed.

The evaluation process of cloud service for trust degree evaluation of users is as follows: (suppose user A wants to use service provided by cloud service supplier M):

Step1 In the beginning stage, after certification server verifying user identity, it will distribute one initial trust value, it will guarantee users can at least obtain one cloud service.

Step2 M and A has exchange experience: the direct trust degree of M towards applier A of certification server is marked as dtru. If dtru $\geqslant \lambda$(λ is the lowest trust degree value of provided service set by M), then M accepts service request of A, if dtru $< \lambda$， then M refuses to provide service to A.

Step3 M and A has no transaction experience: cloud computing server M consults trust evaluation value of other servers on A. It uses certain algorithm and strategy to comprehensively calculate out indirect trust degree of A. If rtru $\geqslant \lambda$, M responses to service request of A, otherwise it refuses to provide service for A.

Step4 After service is provided and completed, server M has to make monitor on action in the whole process of user A, prevent static higher trust degree, but it makes false operation in the action process.

Simulation test in security framework model of cloud computing

The test operation of this paper is in Map/Reduce platform of Hadoop, in order to demonstrate the effectiveness of cloud users and cloud service terminal and get change relations of mutual trust degree with action and time, the test environment using close to real random and real condition of complicated network as target, it sets the following test network environment and identity interaction scene. It respectively simulates network environment composed of 100 to 700 nods in lab, it is used to

compare trust evaluation model of cloud users and cloud service terminal as well as interaction success rate of TACS model and anti-attack ability. In addition, the parameter setting in ant colony algorithm has bigger influence on capacity of algorithm; the test chooses the optimal parameter setting of ant-week model, that is $\alpha = 1, \beta = 5, \rho = 0.5$.

As it is indicated by table 1, it is the direct trust adjacent matrix and trust degree adjacent matrix of each node changes with time.

Table 1 Change relations of trust element of A and B with time and interaction times

Time t	1	2	3	4	5	6	7	8	9	10
Tp_{AB1}	0.5	0.25	0.125	0.063	0.032	0.01563	0.00781	0.00391	0.00195	0.00098
Tp_{AB2}	0.5	0.724	0.823	0.865	0.886	0.89433	0.89806	0.89969	0.90042	0.90073

The simulation test in cloud computing platform respectively observes change rule of trust degree, that is the change rule of trust degree with time factor and interaction times, by taking A and B for example, it calculates change relations of trust degree of node A and B with time and interaction times. As it is indicated by diagram 3, the blue line describes change relations of trust information element of node A and B purely change with time. In the actual operation process, trust relation of users and every service node are affected by time factor and interaction times, therefore, this paper comprehensively considers these 2 kinds of factors, the red line describes change relations of trust information element of node A and B mutually affected by time and interaction events (suppose A and B has one interaction in each unit time).

The initialization of trust and information element between A and B is 0.5, when trust and information element of 2 entities are only affected by time factor, trust and information element will decrease after every unit time until after the 8^{th} unit time, trust information element of A and B is nearly 0. This indicates that time factor has big influence on trust degree among entities, once 2 entities can not make interaction for long time, the trust degree of both can be deleted. When 2 entities make one interaction every unit time, trust information element will increase, and the increase amount is larger than attenuation amount of information element with time, therefore, the red line presents increase trend. But due to value range of trust information element is [0,1], therefore, the maximum value of trust information element should not exceed 1.

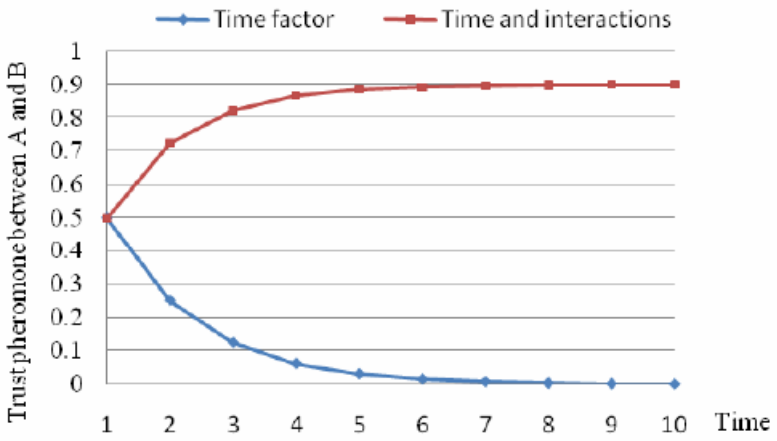

Diagram 3 Change relations of trust information element with time and interaction event between A and B

From diagram 4 we can see that in the beginning stage, the interaction success rate of TACS is lower than interaction success rate of TBFEM, the cause lies in that under cloud computing environment, the number of node in network is in the dynamic change process, the interaction success

rate of TACS in static network can reach above 96%, the interaction success rate in dynamic network is relatively lower than TBFEM model. But with increase in interaction times, TBFEM model and TACS model can all pass ant colony algorithm and gradually choose node interaction with higher trust degree, so that it can increase its interaction success rate. The general trust model can inevitably have malicious recommendation problem, TACS model has made no consideration on malicious recommendation, while TBFEM model fully considers the trust degree of medium entity and it chooses entity with higher trust degree as recommendation entity, so that it reduces times of being attacked.

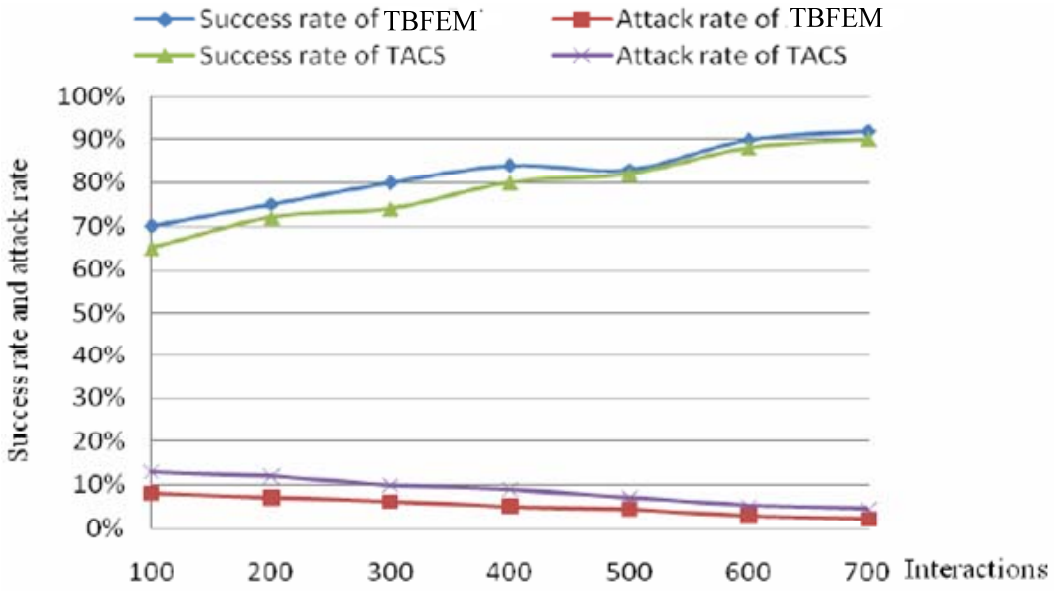

Diagram 3 Performance comparisons between TBFEM model and TACS model

Summary

In the cloud computing environment, access control strategy is the effective measure of guaranteeing cloud users as well as cloud computing service and resources interaction security, trust management is one of the core technology to solve security problem of cloud computing, therefore, as for supplier of cloud service, demonstrating whether user identity of its resources is reliable or nor is the first step to protect internal resources. The traditional network security technology can not well adapt to characteristics of cloud environment, which neglects fuzziness and dynamic of trust as for the past trust model, it can not correctly reflect trust relations, it puts forward cloud computing evaluation model based on fuzzy trust by relying on idea of fuzzy logic, applies fuzzy comprehensive judgment method to calculate trust degree of cloud service, establishes fuzzy control rule, authorizes cloud users corresponding authority by fuzzy judgment, it introduces into time factor on calculating trust degree, which can make it better meet requirements on access control in the cloud computing environment. It effectively enhances security of cloud computing platform by establishing double trust mechanism.

References

[1] Feng Dengguo，Zhang Min，Zhang Yan etc. Research on Cloud Computing. Software Journal，2011, Vol 22，p71-82.

[2] Lin Guoyuan etc. Security Model on Access Control of Cloud Computing Based on Action [J]. Communication Journal，2012,Vol 33(3)，p59-66.

[3] Hyukho Kim, Hana Lee, Woongsup Kim, et al. A Trust Evaluation Model for Cloud Computing[M]. International Conference on Grid and Distributed Computing. Springer Berlin Heidelberg, 2009，p184-192..

[4] Greenberg A, Hamilton JR, Jain N. VL2: A scalable and flexible data center network. In: Proc. of theSIGCOMM 2009[C]. 2009，p51-62.

[5]Xiong Runqun, Luo Junzhou. Replica Selection Strategy of QoS Preference Feeling and Perception under Cloud Computing Environment. Communication Journal, 2011,Vol 32(7)，p93-102.

[6] Wang Shurong. Research on Security and Trust Model Based on Cloud Computing Platform. Nanjing University of Posts and Telecommunications，2011.2. .

[7] Liu Wu，Duan Haixin，Zhang Hong etc. TRBAC：Access Control Model Based on Trust. Computer Resaerch and Development，2011, Vol 48(8),p 1414-1420.. .

[8] Wenhui Wang, Jing Han, Meina Song, et al. The Design of a Trust and Role Based Access Control Model in Cloud Computing[C]. Information Technology and Artificial Intelligence Conference (ITAIC), 2011 6th International Conference on. IEEE, 2011, p330-334.

[9] Li Xiaoyong. Resarch on Dynamic Trust Model under Large-scale Distributed Environment. Software Journal, 2007 ,Vol 18(6),p1510−1521.

[10] Hu Jianli，Zhou Bin，Wu Quanyuan. Research on Trust Management with Encouragement Mechanism in P2P Network. Communication Journal，2011,Vol 32(5),p22-32..