Trusted Access Control Based on FCE of User Behavior in Cloud Environment

LEIYUE YAO
Information College,
Jiangxi University of Technology,
Higher Education Parks in Yao Lake, Nanchang, Jiangxi Province,
CHINA
Email: special8212@sohu.com

Abstract: - In a complex dynamic cloud computing environment, both analyses of abnormal behavior of users and confirming incredible users are effective security measures. Fuzzy mathematics is used to reflect the ambiguous judgment of experts, and AHP method is used to compute the weight for each attribute of network users' behavior. So a comprehensive way is used to evaluate user's trust value based on FCE in this study. Experimental results show that the trust in different types of users can be evaluated effectively, service rejection rate for malicious nodes is improved, and success rate of service interactions is also improved for integrity users. So the evaluation method helps to quantitative analysis of dynamic trust-based security controls, and provides a reliable evidence for service providers in response to user's request.

Key-Words: - cloud platform, user behavior, access control, Fuzzy Comprehensive Evaluation, trust evaluation.

1 Introduction

With the rapid development of cloud technology, people enjoy the lower operating costs, improved operational efficiency and various conveniences. The interface provided by network enables users directly use or operate software, operating systems, even programming environment and network infrastructure in cloud. As promising as it is, this paradigm also brings forth many new challenges to data security and access control when users save sensitive data for sharing on cloud servers [1]. The massive important user data in cloud systems has a greater temptation to an attacker. It is obviously that the destruction to cloud resources is much more serious than current use of the Internet for resource sharing [2]. Therefore, the authentic identity and the confirming of trustworthy behavior for end-user who access to cloud resources, is important to ensure the security of cloud computing. The trust of users also includes two aspects, the end-user's identity and behavior. Authentic identity can determine whether the user is accurately. The trustworthy behavior refers to whether the behavior of end user is credible [3].

Trust management has become an important challenging issue in the emerging cloud computing area. Several trust management issues have been mostly neglected and need to be addressed before cloud computing can be fully embraced, such as identification, privacy, personalization, integration, security, scalability, etc.. [4]. Over the past few years, different techniques have been proposed in many studies to address trust management issues. For example, Ryan believes consumers are aware that, "trust" issue is very important in this context of cloud environment [5]; Abbadi believes that the establishment of cloud trust model is important, although complexity and dynamic nature of cloud infrastructure makes it difficult to solve. He proposed a trust framework for IaaS cloud type and cloud user [6]. The behavior trust is more specific, and is a dynamic form of trust. Therefore, in a cloud computing environment, it is not enough to only solve the problem of identity trust [7]. We have to combine the user's behavior to address the issue of evaluating users' trust problems to service providers. Dewangan discusses evaluation importance of user behavior trust and evaluation strategy in his paper, including trust object analysis, principle on evaluating user behavior trust, basic idea of evaluating user behavior trust, and evaluation strategy of behavior trust for each access in the cloud computing [8]. Wu proposed a cloud computing environment of trust evaluation model based on DS evidence theory and the sliding window approach. Direct evidence of the trust entity in DS evidence theory is calculated based on the interaction of recommended trust through transitive trust fusion from user's experience [9]. Ray believes that users need to acquire different permissions from

different administrative domains based on the services in cloud computing environment. His research specified that how authorization occurs based on user's credibility in the proposed model [10]. Zhang also proposes a reference model for access control management in the cloud computing. A model based on trust grade of behaviors to achieve role control is built; it focuses on the entity behaviors, or the results of entity's behaviors, and integrates a credible value to change the entity of role and authority in cloud system [11]. But the article merely researches the overall structure from a macro point on user behavior and management mechanism. However, the problem of how to build the behavior trust model also attracts attention. For example, Guo proposed Fuzzy Analytic Hierarchy Process (FAHP) to compute weight of each attribute of user behavior, and made more objective evaluation results. But the Analytic Hierarchy Process (AHP) cannot reflect evidence relationship of each attribute well [12]. Siddiqui also presented a technique for calculating the trust based on the rule of fuzzy logic. Three parameters, reliability, capability, and user satisfaction are taken as the input values and trust factors are the output [13]. Bee took the user behavior as a core in trusted network, and proposed architecture for trust assessment oriented to user behavior in trusted network. It used Bayesian network for users to predict the future behavior of the trust [14]. But neither of them takes the user's historical behavior into account, and the evaluation of main consideration is to analyze the real-time behavior.

In comparison, the traditional authorization and authentication are mainly to solve the issue of the user's identity, while fail to deal with the dynamic users. Even though some are trust models proposed for evaluating end users, they often are based on transitive or real-time behavior, and have signal evidence. They don't fully consider the end user behavior rules, fail to solve the problem of user behavior trust in history, and have no dynamic evolution of trust mechanism. In this paper, we not only consider the history behavior, but also take into account the time decay, trust updating strategy. We use the FCE (Fuzzy Comprehensive Evaluation) method and AHP, which is recognized as a valid method to calculate the weight. The combining method can overcome subjective arbitrariness of using AHP alone, thus improving the objectivity and effectiveness for assessment of user behavior trust. The experiments show that it can also improve service rejection rate for malicious node and success rate of service interactions for integrity users. The rest of the paper is organized as follows. Section 2 is a description of the access control model in cloud based on trust. In this section, the detail attribute of behavior trust and the process of access control are are analyzed. Section 3 constructs the user trust evaluation model based on FCE. In this section, the trust model takes the time decay into account, calculates weight value of each attribute by AHP method, and builds fuzzy membership of the trust evidence by trapezoidal fuzzy function. In section 4, we test three types of user's trust value, and also verify the value of the model by Service Rejected Rate and Service Request Success Rate. Finally in section 5, we make a conclusion of the paper and point out the significance of behavior trust research in cloud. So the main contribution of this paper is that it proposed a dynamic, personalized trust model in a comprehensive evaluation by behavior rules of users. The service providers who adopt strategy based on this method can assess the credibility of end users more objectively, and improve service efficiency in cloud.

2 Trusted Access Control on Behavior in Cloud

2.1 Trust Model of the Cloud User

Trust refers to a belief on reliability, security, dependability and ability of an entity that acts in particular environment. The ultimate goal of trust evaluation in the network is not completely eliminate incredibility, but rather to help system administrators to balance "providing services" and "credible assurance". It is an active testing before the attack. Creation and updating of trust for cloud users are based on the evidence of various acts directly or indirectly. User behavior is the basic evidence used to quantitatively assess the trust value. The service provider may obtain objective evidence directly from the hardware.

For example, in order to stop the occurrence of these untrustworthy behaviors, Database providers take punitive measures for different users according to the severity degree of adverse behavior. The database provider predicts the trust level of user based on user history after each visit and records these predictable results in database. When a user accesses the database, the database provider adopts different control and early warning depending on the level of trust. The trust of user U is evaluated

from three trust attributes, including performance attribute of *PA*, the safety attribute of *SA* and reliability attribute of *RA*. Each attribute is composited by different evidence. According to the cloud user behavior characteristics, evidence is shown as Table 1.

Table 1. Trust model of behavior

Target Level	Attribute level	Evidence level
Behavior Trust of user	Performance attribute (*PA*)	Data transfer rate Service response time Transmission delay CPU utilization
	Reliability attribute (*RA*)	Can report the error rate Error response rate Transmission rate Is the data jitter
	Safety attribute (*SA*)	The integrity of the data Abnormal behavior Illegal scan important port Data encryption authentication

Table 2. Basic evidence of security

Evidence	Basic meaning of trust
The integrity of the data	whether the integrity of data provided is lower than the trust threshold range
Abnormal behavior	Whether occur specified abnormal behavior
Illegal scan important port	Whether the number of scanning port is more than trust threshold
Data encryption authentication	Whether the number of verify the encrypted data is more than trust threshold

Security property describes whether the user behavior is in line with requirements; whether caused destruction and attacks on access to databases. In these properties, security is the most important and basic attributes of trust property. Other trust properties are based on security. Performance is to describe the user connectivity performance, and reliability is to describe the user connection reliability. Use *PA* to explain the evidence, each basic meaning of trust evidence is listed as Table 2.

2.2 Access Control Process by User Behavior

The cloud service provider can refuse to provide services for untrustworthy users to prevent unauthorized users from misuse or destruction of resources in cloud. Service providers also take punishment for these users, for example, blacklisting. For users who have a certain level of trust, cloud service providers can take access policies to limit them. For example, cloud service providers only give a very low privilege to users; only let them take limited operation and take no impact on providers; and warn users to avoid continue to take mistrust behavior. Therefore, the purpose of dividing the trust into different level is to use different measures for different users. Trust value feedback on the user, can guide the user to take a more trustworthy behavior, and to improve the safety awareness of terminal user. Fig. 1 shows a control flowchart of the process.

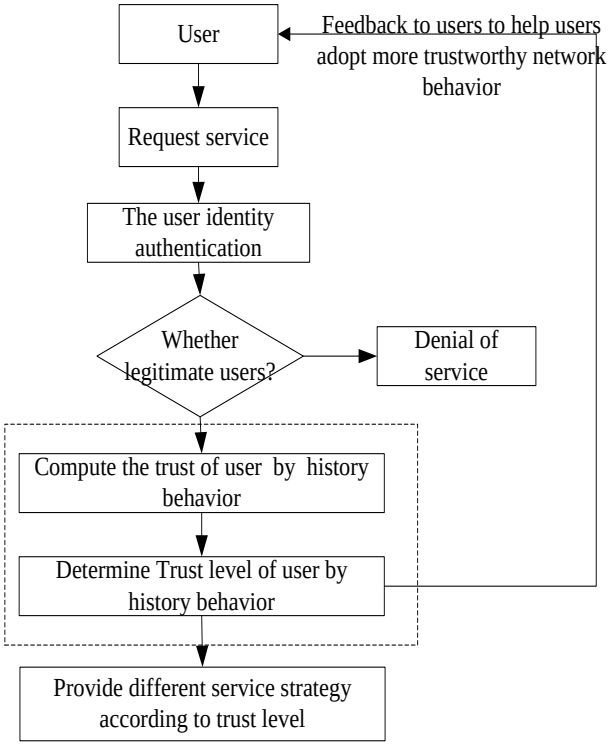

Fig. 1. The access method based on trust mechanism

3 Trust Evaluation of User by FCE

3.1 Comprehensive Trust Model

Fuzzy theory is used to analyze various factors due to their ambiguity. Firstly, factors set of trust $\{a_1, a_2, \ldots a_n\}$ is constructed, and n is the amount of factors. There are three factors here from the above model: Performance attributes (*PA*), reliability properties (*RA*), security attributes (*SA*), so $n = 3$. It should establish the weight of the characteristics before the trust calculation. The value for behavioral evidence has been obtained for each element, so the trust value can be calculated by assessment value and weight value of each factor. AHP method is used here. 10 surveyed users were invited to give judgment on these factors, and a "judgment matrix" is constituted through the mean value of judgment, as shown in Table 3. The consistency checking of "Judgment Matrix" in the pairwise comparison matrix $CR = 0.0007 << 0.1$, which indicates the acceptance of consistency of the judgment matrix. The weight for the three factors of *PA*, *RA*, *SA* is $\{W_P, W_R, W_S\} = \{0.19, 0.16, 0.65\}$, where the maximum weight value is *SA*. It is obviously that user security is generally considered the most important factor in trust calculation.

The comprehensive trust model is:

$$T = w_p \cdot PA + w_R \cdot RA + w_S \cdot SA \quad (1)$$

Table 3. Comparison Matrix

Factor	*A*	*A*	*A*
P			
A		.13	.27
R			
A	.88		.26
S			
A	.7	.85	

3.2 Fuzzy Membership Values of Trust Evidence

Build evaluation set of various factors: evaluation set includes three different items $B = \{b_1, b_2, \ldots b_m\}$, where m is the number of elements of evidence in evaluation set. It is divided into three grades in qualitative way, so $m = 3$, as shown in Table 4.

Table 4. Explanation of Evaluation Set

Symbol	Level	Explanation
b_{e1}	satisfied	Interaction evidence to establish high trust
b_{e2}	medium	Interaction evidence to establish medium trust
b_{e3}	unsatisfied	Interaction evidence to establish low trust

Establishment of trust ambiguity functions for secondary indicators: The difference between the evidence and reference threshold reflects the level of user's satisfaction. The evidence value of behavior below the threshold brings a higher satisfaction. According to expert's experience and data characteristics, we divide several different intervals by the value of evidence, and establish a trapezoidal membership functions as Fig. 2.

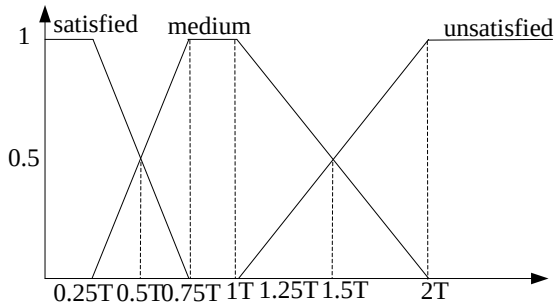

Fig. 2. Fuzzy function of membership

The corresponding function is expressed as follow:

1) Satisfied: $\mu(x) = \begin{cases} 1, & x \le 0.25T \\ -2x + 1.5, & 0.25 \le x \le 0.75 \end{cases}$

2) Medium: $\mu(x) = \begin{cases} 2x - 0.5, & 0.25 \le x \le 0.75 \\ 1, & 0.75 \le x \le 1 \\ -x + 2, & 1 \le x \le 2 \end{cases}$

3) Unsatisfied: $\mu(x) = \begin{cases} x - 1, & 1 \le x \le 2 \\ 1, & x \ge 2 \end{cases}$

Primary evaluation of evidence: For each evidence parameter of attributes, membership matrix P can be calculated in accordance with the rules of membership. Performance indicators are used for example.

$$P_e = \begin{bmatrix} p_{a1} & p_{a2} & p_{a3} \\ p_{b1} & p_{b2} & p_{b3} \\ p_{c1} & p_{c2} & p_{c3} \end{bmatrix}$$

Where p_a, p_b, p_c respectively express the membership value of evaluation set $\{b_{e1}, b_{e2}, b_{e3}\}$. Reset the same weight for the three parameters, then the weight vector Ve = [0.33 0.33 0.33]. The

attributes membership vector *Re* of trust obtained from evidence performance is = *Ve* × *Pe*.

Second level of fuzzy comprehensive evaluation: Make the second level of fuzzy comprehensive evaluation on performance attributes, reliability attributes and security attributes. Construct credible factor matrix *R* through their membership vector W_p, W_r, W_s. Vector *W* is the value of each factor's weight. Finally, the comprehensive credibility membership vector $S = W \times R$ is obtained.

Table 5. Grade range of possibilities events

Trust level	Low	Medium	High
P	$0 \le p \le 20\%$	$20\% \le p \le 80\%$	$80\% \le p \le 100\%$

Referring to the range of event occurrence probability in GB/T20984-2007, which is called "Information security risk assessment norms of Information security techniques", a trust range grading is set as Table 5. When the evaluation goal falls into a certain level, it determines the probability of an event occurring range.

Probability vector is obtained from the middle value, *E* = {10%, 50%, 90%}. Thus the specific trust value of most possibility is calculated: *RV* = *S*•*E*, and the evaluation in accordance with the value of the trust level is performed.

3.3 Time Decay

Evidence decays with time. If there is no any interaction between service provider and the user for a long time, the effectiveness of evidence will be reduced gradually. In other words, the trustworthy node may convert to an untrustworthy one, and the node needs to re-establish trust. So the introduction of time decay factor $\psi(t)$ is to represent this feature, where $t = t_{cur} - t_{ave}$; t_{cur} is currently interaction time; t_{ave} is the average time before the current interaction. The method of trust over time decay is as the Eq. 2.

$$et_{new} = et_{old} \times y(t_{cur} - t_{ave}) \quad (2)$$

Value of ψ(t) can be set according to practical use. Use $y(t) = 0.9^{t/30}$ as an example, the result of it is as Table 6.

Table 6. Example of Time decay

IT	One month	Three month	Half a year	One year
0.9	0.81	0.66	0.48	0.28

3.4 Update the Evidence of User Behavior

The old evidence need to be updated into new one as Table 7. Every updating for evidence is according to the old one. The original evidence trust value can be set by threshold value Theo. Use the evidence value bring by new interactions to update the old evidence. If some items lack of new evidence, then updated with the old evidence attenuated by time.

Table 7. Updating of evidence

	Number of login failed	Number of scan the port	Response time	…
Old evidence	et_{old1}	et_{old2}	et_{old3}	…
New evidence	et_{new1}	et_{new2}	et_{new3}	

If evidence value obtained from an interaction is et_c, then the new evidence can be computed by new evidence value, time decayed old evidence and its stability. The stability is a measurement to assess how much transaction to form the evidence in history. It is obviously that more interactions in history may indicate the evidence is more trustworthy. The fusion algorithm of Evidence can be expressed as Eq. 3.

$$et_{new} = (et_{old} * c + et_c) / (c + 1) \quad (3)$$

4 Experiment

4.1 Description of Experiment

In this simulation, the service providers and service requesters are set independent. While the service requesters can be divided into the following three categories:

Users of Class A: the high trustworthy users are using cloud resources with high integrity in the network. To each type of users, it is supposed that the behavior for every evidence is with the average distribution of 90% probability below the half of threshold value, and other behavior is with average distribution of 10% probability between half of threshold to 1 times of the threshold value.

Users of Class B: the common users, they usually use cloud resources in the normal way. But

there may be some non-normal operation occasionally because of some unforeseen circumstances, such as input errors and network failures. For the type of users, it is supposed that the behavior for every evidence is with the average distribution of 90% probability below the threshold value, and other behavior is with average distribution of 10% probability between threshold to 3 times of the threshold value.

Users of class C: they are malicious users who occupy network resources in malicious way or have intention to attack others. Assuming that the type of user C is opposite to the type A users. It is supposed that the behavior for every evidence is with the average distribution of 10% probability below threshold value, and other behavior is with average distribution of 90% probability between threshold to 3 times of threshold value.

Experimental simulation environment is under the context of ADM1.6 GHz, 1GB, and simulation is based on MyEclipse 6.0. In the experiment, the number of Service Providers (SP) is 1000, and the number of Service requestors (SR) is 120. Class A, B, and C occupy the same proportion; the number of each type is 40. The other simulation parameters are set as the Table 8.

Table 8. Default of paramters' value

Parameters	Default value	Description
IT	0.5	Init value
Wp	0.19	Weight value of performance
Wr	0.16	Weight value of reliability
Ws	0.65	Weight value of security

4.2 Trust Evaluation

In Experiment 1, the initial trust values for all types of users are set to 0.5, and changes of trust value for users are observed with the increasing of interactions. The SP's trust value changes of the three categories in the course of interaction are shown in Fig. 3. As shown in the figure, the trust value of Class A and Class B grows with the increasing of interaction, and Class A has a big growth than Class B users. But the trust value of Class C declines with the increasing of interaction. This is mainly because the users of Class A are set to the most honest, and they can obtain high integrity for their honest behavior in the case of small volume of interaction. The increase of interaction volume further enhances the stability of trust evidence, assesses to the evidence of the value more comprehensively, and then obtains more actual trust value evaluation. Class B is set as the common users, who do some dishonest network behavior by accident. The dishonest probability is set to 10 % in this experiment, but the probability of behavior within a reasonable range is set to 90%. So with the increase of interaction, most of the evidence in establishing trust still plays a positive role in the process. The trust value of the Class B also increases by the amount of interaction, and it obtains a higher value from the most honesty behavior in history. However, these users still have small probability of bad behavior, causing the reduction of the overall trust in part. So the value of class B is lower than that of class A. Although Class C users also present a certain trust value in the initial, with the occurrence of interaction, the high probability of bad behavior quickly reduces the evidence of the trust value. Then with the increase of interaction, more interactions enhance the stability degree of mistrust, further complete evidence of trust value, which reduce the evaluation of trust value to very low. These results are also in line with the formation of people's trust in social interaction behavior.

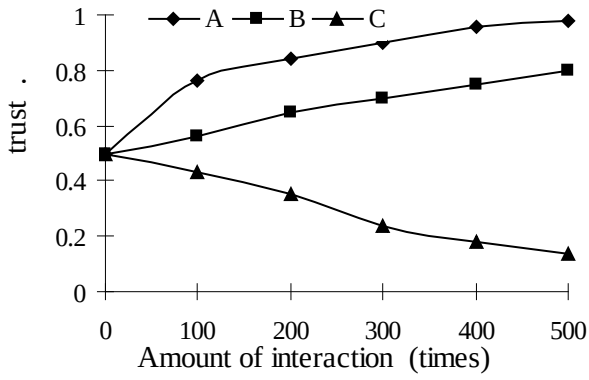

Fig. 3. Result of trust value of each Class users

4.3 Service Rejected Ratio

User is rejected when their trust value does not reach the threshold determined by services providers. Suppose that *TN* is the total number of the interaction and *RN* is the total number of the rejected service interaction, the service rejected rate *SRR* is defined as:

$$SRR = \frac{RN}{TN} \quad (4)$$

The experiment simulates interaction for 200 times in Fig. 4. By observing the rejected rate of different types of users in the context of different threshold of trust, we found it is obviously that the entire service requirement will be accepted while the trust threshold is a minimum value 0. With the growing of threshold value, the rejected rate of Class C user has a most significant increase, which is bigger than Class A and class B in any case of trust threshold. We have known the trust value of Class C drops below 0.4 after interaction for 200 times. If the trust threshold bigger than 0.4, a great amount of service request is rejected, which leads to a big *SRR*. If the trust threshold value is less than 0.4, the service request can be accepted with a big probability. But in general, it has no possible to set such a low threshold value. Class B and Class C can achieve a higher trust value after transactions for 200 times. But Class B users still have a certain probability of bad behavior, thus as the threshold value increases and exceeds the initial value of the trust, their service is denied in a certain. In the evolution process of the trust value, the value of Class A user has not yet fully stable. It may lead to some denied interaction owing to the initial value of the trust is set lower than a threshold. These problems can be solved effectively by adjusting the threshold through the user interaction history, and then the denial of service for Class A is avoided.

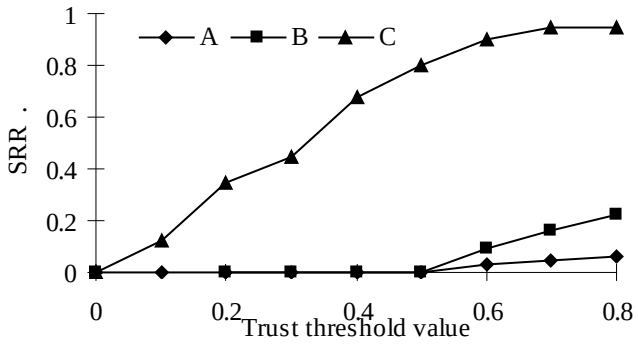

Fig. 4. Result of SRR of each class users

4.4 Service Request Success Ratio

An interaction between SP and SR can consider as a successful interaction if it satisfies both sides. If the SP gives a feedback to malicious users beyond the normal range after the interaction, it is considered as a failure. Suppose that *TN* is the total number of interaction; *SN* is the total number of successful interaction, then the service successful rate *SSR* is defined as:

$$SSR = \frac{SN}{TN} \tag{5}$$

There are 100 end users in the experiment, who are marked with type A and type C. In order to explain more clearly, we choose the opposite of two types of users here, and exclude the type B. If the providers select type C users, it is a failure; otherwise select type A users is a success. Each type of user is 50, and the interaction of user node is extracted by the same probability among the three types. Fig. 5 is the result of comparing the access policies using the history behavior trust mechanism (HBT) in this paper with traditional access policy (TAP), and current behavior trust (CBT). The TAP does not use the trust mechanism, while CBT does not consider the history of user and the trust evolution with interactions. Experimental result indicates that the composition process of service increases with the interaction. The TAP that has no trust mechanism in selecting users, and it leads to a low successful interaction rate due to more malicious service requestors. The possible reason why SSR value is always in the vicinity of 0.5 is that the two types of users have a similar proportion. The CBT model used the current evidence as trust, and it can distinguish the malicious users and trustworthy users in largely degree. But the model cannot reach a high SSR value with the increasing of interactions. It may be because it lacks of stability caused by ignoring history behavior and trust evolution. Comparing with the above two mechanisms, the HBT model is able to do an effective organization to the service in cloud platform. The reason can be concluded as the trust evolution with time decay and history behavior, and the trust model is computed in more comprehensive way. It has the maximal SSR value in experiment. So the model in this study has improved the success interaction rate and the effect of service selection after the introduction of trust mechanisms based on history behavior.

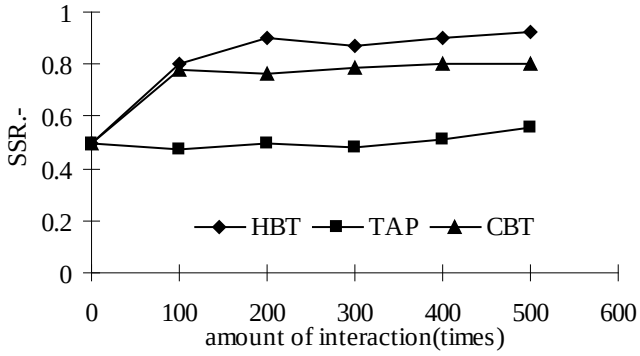

Fig. 5. Result of SSR of three mechanisms

5 Conclusion

Authentication technology is relatively mature currently, but it can't prevent the failure of identity authentication or malicious destruction of legal users. So the effective analysis of users' behavior is important in current cloud computing. In this paper, we proposed a method based on FCE and AHP to make quantitative analysis on each factor and its weight for users' behavior. It not only provides a scientific strategy to quantify user history behavior for cloud service providers, but also provides guidance for users to improve their behavior. Through trust assessment of user behavior and monitoring trustworthy behavior real time, it guarantees the security of cloud computing environments, and lays a foundation to realize active safety mechanism. In order to achieve better application, two main issues need to solve in further study. The first is to extend the trust value, extend the obtained trust value of user behavior in other sophisticated systems to the current system, and combine with the current system user behavior to get a more accurate trust value, which is particularly suitable for the early establishment of behavior trust value in a system. The second is to optimize trust value algorithms to reduce the time complexity, especially in cloud computing environments under a huge user scale and an amount of evidence on behavior.

Acknowledgment

This work was supported by Youth Fund Projects and National Science Foundation, from Science and Technology Agency of Jiangxi Province, NO. 2012ZBAB201003, and NO. 20132BAB201055.

References:

[1] C. M. Rong, Son T. Nguyen, and Martin Gilje Jaatun. Beyond Lightning: a Survey on Security Challenges in Cloud Computing, *Computers & Electrical Engineering*, Vol. 39, No. 1, 2013, pp. 47-54.

[2] Namje Park, Secure Data Access Control Scheme Using Type-Based Re-Encryption in Cloud Environment, in *Semantic Methods for Knowledge Management and Communication, Studies in Computational Intelligence*, Vol 381, 2011, pp. 319-327.

[3] Khan Khaled M., and Qutaibah Malluhi, Establishing Trust in Cloud Computing, *IT Professional*, Vol. 12, No. 5, 2010, pp. 20-27.

[4] K. L. Ko Ryan, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. H. Liang, and B. S. Lee, Trust Cloud: a Framework for Accountability and Trust in Cloud Computing, Services, *2011 IEEE World Congress on IEEE*, 2011, pp. 584-588.

[5] Ryan Patrick, and Sarah Falvey, Trust in the Clouds, *Computer Law & Security Review*, Vol. 28, No. 5, 2012, pp. 513-521.

[6] Abbadi Imad M., and Muntaha Alawneh, A Framework for Establishing Trust in the Cloud, *Computer &. Electrical Engineering*, Vol. 38, No. 5, 2012, pp. 1073-1087.

[7] H. Noor Talal, Q. Z. Sheng, S. Zeadally, and J. Yu, Trust Management of Services in Cloud Environments: Obstacles and Solutions, *ACM Computing Surveys (CSUR)*, Vol. 46, No. 1, 2013, p. 12.

[8] Dewangan, Bhupesh Kumar, and Praveen Shende, Survey on User Behavior Trust Evaluation in Cloud Computing, *International Journal of Science, Engineering and Technology Research*, Vol. 1, No. 5, 2012, pp. 113.

[9] J. B. Wu, and G. Lv, Trust and Reputation Evaluation for Web Services Based on User Experience, *Journal Computer Application*, Vol. 29, No. 8, 2009, pp.2291-2293.

[10] Ray, Indrajit, and Indrakshi Ray, Trust-Based Access Control for Secure Cloud Computing, in *High Performance Cloud Auditing and Applications*, Springer: New York, 2014, pp. 189-213.

[11] Y. S. Zhang, M. Tian. S. J. Lv, and Y. D. Zhang, Design of Trust Model Based on Behavior in Cloud Computing Environment, in *Frontier and Future Development of Information Technology in Medicine and Education*. Springer: Netherlands, Vol. 269, 2014, pp. 1021-1028.

[12] S. K. Guo, L. Q. Tian, and X. L. Shen, Research on FAHP Method in User Behavior Trust Computation, *Jisuanji Gongcheng yu Yingyong (Computer Engineering Application)*, Vol. 47, No. 12, 2011, pp. 59-61.

[13] Siddiqui, Mohd Noman, Vinit Saini, and Ravinder Ahuja. Trust Management for Grid Environment Using Rule Based Fuzzy Logic, in *Advances in Network Security and Applications*. Springer: Berlin Heidelberg, Vol. 196, 2011, pp. 649-657.

[14] Bee, Karin, Stephan Hammer, Christian Pratsch, and Elisabeth Andre, The Automatic Trust Management of Self-Adaptive Multi-Display Environments, in *Trustworthy Ubiquitous Computing*. Atlantis Press, Vol. 6, 2012, pp. 3-20.