Available online at www.ijpe-online.com

International Journal of Performability Engineering

vol. 14, no. 4, April 2018, pp. 665-672
DOI: 10.23940/ijpe.18.04.p9.665672

A Behavior Trust Model based on Fuzzy Logic in Cloud Environment

Zhangwei Yang[a,b,c,*] and Juan Luo[b]

[a]*Institute of Information and Computer Science, Pingxiang University, Pingxiang, 337000, China*
[b]*School of Computer Science and Engineering, Hunan University, Changsha, 410082, China*
[c]*Engineering Research Centre for Cyberspace Security, Pingxiang, 337000, China*

Abstract

Authentication technology in the cloud environment cannot completely prevent the destruction of malicious users to cloud resources. The analysis and evaluation of the user behavior has become the key to effectively improve the security of cloud. This paper improves a multi-parameter behavior trust model (MTEM), which based on Beth model and Josang model. The MTEM model introduces a number of parameters involved in the transaction process of users and cloud service providers. Furthermore, we calculate the behavior weight value by using AHP, through fuzzy logic analysis of user behavior. According to the principle of maximum membership degree, we verified the feasibility and validity of the model by simulation. The simulation results show that the MTEM model can improve the detection accuracy of user's malicious behavior and the effectiveness of the users.

Keywords: MTEM; user behavior; fuzzy logic; trust model; AHP

(Submitted on January 3, 2018; Revised on January 31, 2018; Accepted on March 5, 2018)

1. Introduction

Cloud computing is a combination of P2P computing, parallel computing and grid computing, which embodies the idea of the computer. Cloud computing environment is a shared virtual resource pool by variety of existing network storage space and computing ability. It provides a unified service interface, allows users of cloud services to apply for resources and services according to their needs for saving high cost of hardware and software [3,5]. In the cloud environment, it will produce a serious trust problem because of fraud between CU (Cloud Users) and CSP (Cloud Service Providers) [4,7].

Trust is the prerequisite and basis for network trading activities in the e-commerce and other fields. All of the resource services in the cloud environment are open to users based on trust mechanism; there are two kinds of trust relationships between users and cloud service providers: identity authentication and behavior trust. The identity authentication technology is more mature, but it cannot completely prevent the destruction of malicious users. The trust behavior is a kind of trust relationship based on the direct or indirect experience of the past, which is more suitable for cloud environment. With the increasing number of abnormal behavior, the cloud user behavior analysis and evaluation, and the establishment of corresponding trust model has become most important to effectively improve the security of the cloud [10].

In the cloud environment, behavior trust is a dynamic change. The parameters that affect it include direct trust value, indirect trust value, time decay, etc. Trust model is introduced to evaluate the credibility of the user and the cloud service provider, in order to solve the problem of multi-parameter to the user behavior trust in cloud environment. Furthermore, lots of experts and scholars have put forward a series of trust model in different research fields, mainly as follows.

M. Alhamad [1] pointed out the role of SLA (Service Level Agreement), and established the corresponding SLA reference standards for different service types. At the same time, Alhamad proposed a trust management model based on SLA for the cloud computing environment. This helps users choose reliable service providers by using the SLA proxy to monitor the service activities of the server in real time. The model proposed the solution for cloud users to choose cloud

* Corresponding author.
E-mail address: yang505412@163.com

service providers, but does not conduct further research on the evaluation of the reliability of CSP. There is a lack of concrete implementation algorithm.

H. Jameel [8] proposed a trust model based on the vector operation mechanism between different entities in pervasive computing environment. In this model, trust evaluation is decided by the mutual entity's recommendation, which introduces the influence factors such as history, trust and time to reflect the dynamic nature of the user's trust evaluation. However, there is no solution to the cheating behavior of the entity recommendation in the model. The model solves the problem of multi parameter in the network computing environment, but it cannot solve the cheating behavior of the interactive entities.

W. Tang [14] proposed a trust model which accord with the characteristics of cloud environment based on fuzzy logic. In this model, direct trust is used as evaluation parameter in the process of trust calculation. However, the model does not consider many factors of cloud users, such as reliability, security and malicious recommendation, etc.

Q. Zhou [18] proposed a trust based on defense system model in the cloud environment. The model conducts a scientific quantitative assessment of behavior trust through the user's behavioral evidence. The model can eliminate the risk of malicious attacks, and improve the ability of the cloud environment. However, the model does not take into account the detection and identification of risk users, and the false alarm rate of the model is higher.

The models above propose solutions from different perspectives, which effectively improve the accuracy of behavior trust evaluation. However, different application environments have different requirements for trust evaluation, and the existing models are proposed for the specific application background. This paper proposed a multi-parameter behavior trust model (MTEM), which based on Beth model and Josang model [2,9] . MTEM combine with the SLA and fuzzy analysis method, and introduce a number of parameters involved in the transaction process of users and cloud service providers. Furthermore, MTEM quantify and evaluate the behavior of users and providers in the cloud environment to protect the two trust degree of objectivity and impartiality.

2. Related Work

2.1. Trust Evaluation Based on Fuzzy Logic

The trust in the cloud environment is divided into direct trust and recommendation trust. Direct trust is the trust relationship between two entities (CU and cloud CSP) based on previous transaction records, and recommended trust is the indirect relationship established by the recommendation of other entities. Trust has asymmetric, incomplete transitivity, dynamic, subjective and multidimensional characteristics, such as: If Entity A trusts Entity B, Entity B Trust Entity A cannot be derived; if Entity A trusts Entity B, Entity B trust Entity C, Entity A Trust Entity C cannot be derived. By the membership function. [12], fuzzy logic can solve the qualitative problem that the subjective expression of trust is not clear in the cloud environment.

Due to the openness and dynamics of the cloud environment, many factors will have an impact on the trust evaluation. The main factors are user subjective evaluation, context correlation, time decay and so on [10,13]. For example, the Beth model evaluates the trust as an interactive experience with the number of interactions or failures between entities. In an open network environment such as cloud computing, the interaction experience between entity A and entity B contains many factors that can be expressed as Equation (1).

$$\mu_{L_j}: F_i \rightarrow [0,1]\ (i = 1,2,\cdots,n; j = 1,2,\cdots,n_i) \tag{1}$$

Among the Equation (1), μ_{L_j} denotes the membership function of fuzzy set L_j, $\mu_{L_j}(f)$ denotes the degree which the element belongs to the fuzzy set, and the set F_i is the interaction experience between entity A and entity B.

2.2. Framework of MTEM model

In cloud computing environment, the CSP determines resources according to the user's behavior trust, and users consider the cloud service providers mainly through their availability, reliability and other parameters. The basic idea of the model is introducing the parameters which affect users' behavior trust value into the trust calculation process, and establishing the evolution model [11,15,17]. The model framework as shown in Figure 1.

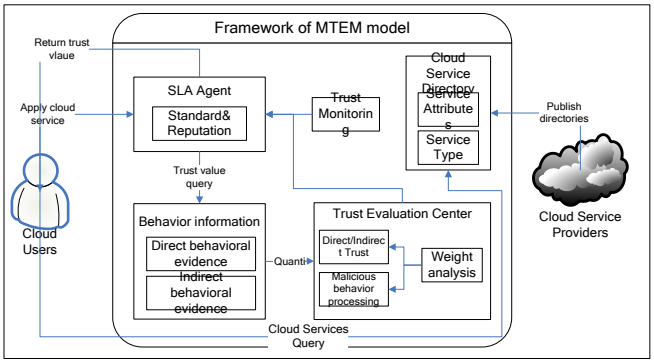

Figure 1. Framework of MTEM model

MTEM consisted of users, cloud service providers, cloud service directory, SLA agent and trust evaluation center, to achieve the trust evaluation and dynamic update of trust value of users and cloud service providers [3]. In the trust evaluation center, availability, reliability, efficiency and honesty of cloud service providers is introduced. Availability is the probability that cloud service provider responds to user requests in a period of time; reliability is the success rate of complete user service request; working efficiency is the time needed to complete the user's request; honesty is the subjective evaluation to cloud service providers after the user request is completed. MTEM involves a number of parameters, and each of them has different basis numerical and relative weight. Also, MTEM is simulation of real transactions, carrying out the weight analysis by AHP method.

3. Analysis of the Trust Model

3.1. Behavior analysis based on fuzzy logic

It is similar to the reality of human, user behavior in cloud computing. It is the conscious activities of cloud users to cloud computing service providers, with the characteristics of trust, risk and randomness. According to the value of the trust value of the discrete value measurement method, the user's behavior can be converted into a set of trust level: {trust, general trust, basic trust, less trust, no trust}. The model subset is used to describe the trust sets, as shown in Equation (2).

$$T_n = \{trust, general\ trust, basic\ trust, less\ trust, no\ trust\} \quad (n = 1,2,3,4,5) \tag{2}$$

According to the trust decision of the cloud service provider to the user behavior, T_n from the Equation (2) needs to meet the following conditions.

$$\begin{cases} T_{i-1} > T_i & (i = 2,3,4,5) \\ T_i \cap T_j = 0 & (i \neq j) \end{cases} \tag{3}$$

The model based on Equation (3) needs to obtain evidence of behavior and property analysis before judging whether the user's behavior is credible or not. In order to ensure the relative accuracy of behavior evidence value, choosing appropriate time granularity to obtain behavior evidence is the key factor to improve the accuracy of behavior evidence value in a certain period of time. Suppose X represents the trust metric value of the user's behavior, then X should be located in the T_n trust level space and meet the conditions of $X \in [T_{i-1}, T_i]$, where T_{i-1} and T_i denote the upper and lower limits of the trust level. Therefore, the mapping function *F (X)* between the trust level and the trust metric is as follows:

$$F(X) = \begin{cases} L_1 & 0 \leq X \leq T_1 \\ L_{n-1} & T_{n-1} \leq X \leq T_n \\ L_n & T_n \leq X \leq 1 \end{cases} \tag{4}$$

In the above Equation (4), L_n represents the user behavior confidence level, satisfying the condition of $L_1 \leq \ldots \leq L_{n-1} \leq L_n$. In other words, L_1 represents the lowest reliability of user behavior, and L_n represents the highest.

Similarly, cloud service providers also need to be trusted by behavioral evidence to measure. The paper introduces availability, reliability, working efficiency and honesty as the evidence of the behavior of users and cloud service providers. The corresponding calculation indicators are shown in Table 1.

Table 1. Behavior index of user and cloud service provider(single attribute)

Behavioral Evidence	Evaluation Index	Expression
Reliability	Number of running threat programs	P_{11}
	Exception rate of access cloud resource	P_{12}
	Exception rate of user IP address	P_{13}
	Number of carrying virus	P_{14}
Security	Number of illegal connection	P_{21}
	Number of scanning cloud server port	P_{22}
	Number of unlawful unauthorized attempts	P_{23}
	Number of attacking other users	P_{24}
	Number of malicious recommendation	P_{25}
Efficiency	Average time to complete user request	P_{31}
	Unit time to accept the number of user requests	P_{32}
	Unit time to run task	P_{33}
Honesty	Task completion rate of user evaluation	P_{41}
	Task failure rate of user evaluation	P_{42}

According to the maximum membership degree principle of fuzzy comprehensive analysis method, it is assumed that the single attribute fuzzy evaluation matrix is *M*, the single attribute fuzzy membership is *m*, the trust value of single attribute *Ti* is {1, 2, 3, 4, 5}, corresponding to the five levels of trust. Therefore, the matrix of fuzzy evaluation to single attribute *M* is defined as follows:

$$M = \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_i \end{bmatrix} = \begin{bmatrix} m_{11} & \cdots & m_{15} \\ \vdots & \ddots & \vdots \\ m_{i1} & \cdots & m_{i5} \end{bmatrix} \tag{5}$$

The matrix above Equation (5) defines the user behavior of a single attribute. However, each single attribute will form a comprehensive evaluation of user behavior based on different weights in the trust evaluation model. Therefore, trust model also needs to determine the weight of each attribute of the user's behavior, and obtain the comprehensive evaluation vector.

3.2. Weight analysis of users' behavior attributes

In the analysis of user behavior in cloud computing, the impact of single attribute on user behavior is different in different research purposes, which is reflected in the different weight value of this attribute in user's behavior. The weight value of single attribute is determined by the important degree of each index, and expressed by the weight vector.

Analytic hierarchy process (AHP) is able to combine the qualitative and quantitative analysis, and scale them by the comparison between the indicators [6]. In this paper, the parameters are compared with each other according to the preferences for users to cloud service providers. The model in this paper constructs the judgment matrix, and tests the consistency of the matrix, to get the reliability, security, efficiency and honesty of the weight distribution table. The hierarchical structure of the trust model is shown in Figure 2.

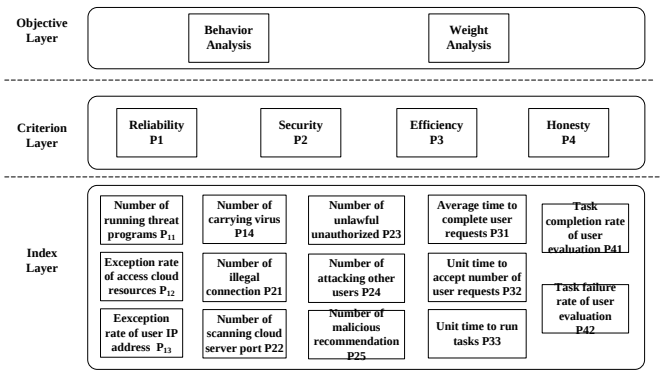

Figure 2. The hierarchical structure of the trust model

In order to make a quantitative analysis of the attribute of the user's behavior, the paper makes compares the important degree of the indexes in the above level chart. The model constructs judgment matrix $N=(n_{ij})_{i*j}$ as a judge, and uses 1-9 level of the ratio to scale, according to the relative importance of the quantitative. The n_{ij} indicate the importance of index *j* relative to index *i*; its range of values is shown in Table 2.

Table 2. 9 level evaluations system of AHP method

Scale	Significance
1	Element n_i and element n_j are equally important
3	Element n_i is slightly more important than n_j
5	Element n_i is more important than n_j
7	Element n_i is strongly more important than n_j
9	Element n_i is extremely more important than n_j
2/4/6/8	The importance of element n_i and element n_j lies between the above two
Reciprocal of 1~9	The reciprocal of importance of element n_i and element n_j

According to the evaluation scale of Table 2 and the evaluation index, a $n\times n$ matrix is constructed, which describes the importance of the two adjacent elements. The values of the matrix elements are in accordance with the following rules, as seen in Equation (6).

$$\begin{cases} n_{ii}=1 \\ n_{ij}>0 \quad \forall_{i,j}\in(1,2,\cdots,n) \\ n_{ji}=1/n_{ij} \end{cases} \tag{6}$$

In order to ensure the coordination and not contradictory of matrix elements to reflect the importance, it is necessary to check the consistency of the matrix *N*. When the matrix is satisfied with the consistency, it is considered that *N* passes the consistency check, otherwise it is necessary to modify *N*. Users can obtain the weight set of each evaluation attribute by calculating and normalizing the characteristic vector of the largest eigenvalue of *N*, according to the judgment matrix. For example, the reliability of user's behavior can be evaluated by indicators such as number of running threat programs (P_{11}), exception rate of access cloud resource (P_{12}), exception rate of user IP address (P_{13}), and number of carrying virus (P_{14}). The weight of the attribute can be expressed as *Q*, $Q=[q_1,q_2,\cdots,q_n]$. Similarly, the weight vector of user's security, efficiency and honesty can be determined and expressed as weight set *A*, $A=[Q_1,Q_2,\cdots,Q_n]$. Furthermore, the evaluation vector can be determined by multiplying of the weight set and the single attribute fuzzy evaluation matrix *M*, expressed as *B*.

$$B=AM=(B_1,B_2,\cdots B_n) \tag{7}$$

In Equation (7), *B* is an evaluation vector, which is a fuzzy subset of the trust degree primitives set. In the MTEM model, the vector *B* is quantified by the user's behavior characteristics, and combined with the weight analysis of the trust evaluation center. Then, *B* is transmitted to the SLA agent by the trust monitoring, as the basis for judging the user to apply for cloud services.

4. Model Validation

4.1. Model Trust Judgment

In order to validate the MTEM mode, we construct a cloud computing experimental environment of 4 servers in Hadoop platform, which installs intrusion detection system SAX2 and level analysis software Yaahp. SAX2 is used to obtain the basic data of user behavior, and Yaahp is used to build the user behavior trust model [16]. Also, the AHP method is used to construct the judgment matrix, and obtain the user's behavior weights. The validation process of the model is shown in Figure 3.

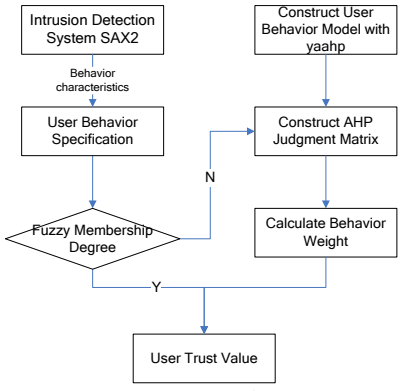

Figure 3. The validation process of MTEM

In the paper, we use SAX2 system to detect and collect the basic data of users' behavior evidence; we also normalize them by taking the number of threatening programs P_{11} and the number of users scanning cloud server P_{22} in the cloud environment as an example. At the same time, five experts were used to evaluate the performance of P_{11} and P_{22}; the scores of P_{11} and P_{22} obtained by SAX2 system were evaluated and can be seen in Table 3.

Table 3. User behavior evaluation（$P_{11}P_{22}$）

P_{11}	P_{22}
7	6
9	8
6	8
5	7
8	9

Fuzzy membership function and the user behavior model is constructed, as shown in Figure 2. Furthermore, the judgment matrix of user A is constructed as Equation (8), according to the parameters such as security, reliability, efficiency and honesty, combined with cloud computing security expert evaluation.

$$N = \begin{bmatrix} 1 & 2 & 3 & 5 \\ 1/2 & 1 & 1 & 1 \\ 1/3 & 1 & 1 & 3 \\ 1/5 & 1 & 1/3 & 1 \end{bmatrix} \tag{8}$$

Next, through calculating and normalizing the characteristic vector of the maximum eigenvalue of N, we obtain the weight vector $A=(0.4886,0.1834,0.2129,0.1152)$ of the user's security, reliability, efficiency and honesty with respect to the behavior of the target. According to the comprehensive evaluation vector $B=AM=(B_1,B_2,\cdots B_n)$, we also get the user's trust fuzzy evaluation vector as follows.

$$B=(0,0.2712,0.4239,0.0455,0.0406) \tag{9}$$

In this vector, from Equation (9), the membership degree of “trust” level is 0.0406, and the membership degree of “no trust” is 0. Therefore, we can determine the trust degree of user A as “general trust”, according to the principle of maximum membership degree of fuzzy logic. In the MTEM, cloud service providers will refuse to allocate resource when user A tries to apply cloud resources, based on the behavior of the trust is “general trust”.

4.2. Simulation and Results Analysis

In order to verify the validity of the model, we simulate an experiment where a user is running a threat program in a short time and continuous port scan on the cloud server, resulting in the instantaneous throughput of the cloud environment, resource requests and other states. After the experiment, random user interacts with the cloud server. As the number of interactions increase, the number of running the threat program and scanning the port of cloud server increase. We use Beth model, Josang model and MTEM model to test the accuracy and false alarm rate, and to judge the accuracy of different models. The comparison results are shown in Figure 4 and Figure 5.

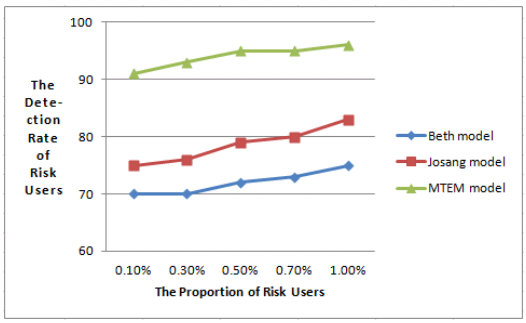

Figure 4. The detection rate of risk users

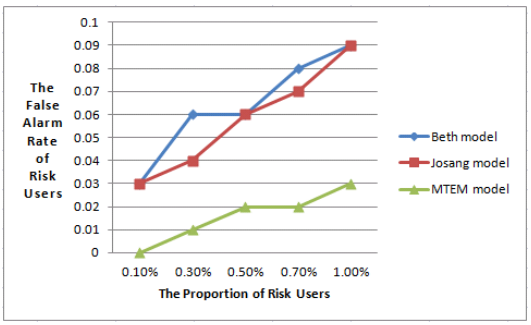

Figure 5. The false alarm rate of risk users

From the results of Figure 4 and Figure 5, we can come to the conclusion that the Beth model, Josang model and

MTEM model can be used to detect the malicious behavior in the cloud environment. With the increase of the proportion of risk users in the cloud environment, the detection accuracy of the three models is higher, and the overall accuracy of MTEM model is higher than Beth and Josang model. In the aspect of false alarm rate, the Beth model and Josang model increased significantly, with the increase in the proportion of risk users. However, the false alarm rate of MTEM model did not change much, and is lower than Beth model and Josang model.

The main prevention method to risk users in cloud environment is preventing them to reach the threshold to apply for cloud resources again by reducing risk users' trust value. The malicious behavior of risk users will be reflected in the change of trust degree. The experiments use the Beth model, Josang model and MTEM model to simulate the user's malicious behavior. The membership of user behavior under different models is calculated, and the changes of users' trust degree are obtained; the results are shown in Figure 6.

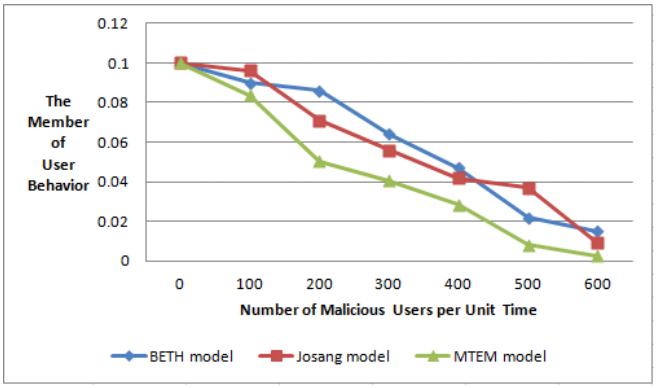

Figure 6. The changes of user trust value of three models

With the gradual increase of malicious behaviors in the interact process of user and cloud services, the trust value calculated by the two models decreases. Furthermore, because the trust value of traditional behavior trust model decreases slowly, malicious users can continue to access cloud server during this period. At the same time, the trust value of MTEM decreases rapidly, It can curb malicious behavior quickly, and reduce the risk of cloud environment.

5. Conclusions

Through the study based on behavior trust model in the cloud environment, the security of cloud computing can be strengthened, which has positive significance to maximize protect cloud services for users, reduce risk of malicious users applying for cloud services resources, and improve mutual trust value of cloud users and cloud service providers. The MTEM trust model proposed in this paper introduces some parameters into process of trust calculation such as security, reliability, efficiency and honesty. MTEM obtains the fuzzy evaluation vector by AHP, and determines the user's trust degree, according to the principle of maximum membership degree through analysis to user behavior by fuzzy logic. The paper provides a train of thought for further reducing the cost of user authentication and detection, and improving the overall security of the cloud environment. The simulation results show that the MTEM model is better than the trust model based on probability and subjective logic in detecting the accuracy and false alarm rate, but its behavior evaluation still has some subjectivity. As a behavior trust model, the fault tolerance and adaptability of the MTEM model needs to be further improved.

Acknowledgements

This work was supported in part by Science and Technology Program of Education Department of Jiangxi Province, China(GJJ171561), Soft Science Program of Jiangxi Province(20161ACA10002), and Teaching Reform in Colleges and Universities of Jiangxi Province, China(JXJG-15-22-3).

References

1. M. Alhamad, T.S. Dillon, T.S. Change. "Conceptual SLA Framework for Cloud Computing," *Proceedings of the 4th IEEE International Conference on Digital Ecosystems and Technologies.* Piscataway: IEEE，2010：606-610
2. T. Beth, M. Borcherding, B. Kein . "Open Net Works," *Proceedings European Symposium Security(ESORICS), Brighton：Springer-Vergag*,l999:59~63

3. A. M. Dillon, T. S. CHANG . " SLA-based Trust Model for Cloud Computing," *Proceedings of 2010 13th International Conference on Network-Based Information Systems*. pp.321-324, 2010.
4. D.G. Feng, M. Zhang, Y. Zhang. "Cloud Computing Security Research," *Journal of Software*. 2011,22(1):71-83.
5. I. Foster, "The Anatomy of the Grid: Enabling Scalable Virtual Organizations," *International Journal of High Performance Computing Applications*, vol.15, pp.200-222, Aug. 2001
6. S.K. Guo, L.Q .Tian, X.L. Shen. "Research on FAHP Method in User Behavior Trust Computation," *Computer Engineering and Application*. Vol. 47. pp.59-61, Dec,2011.
7. T. Hassan B.D. James. A. Joshi,. "Security and Privacy Challenges in Cloud Computing Environments," *IEEE Security& Privacy*,vol.8.pp.24-31, Jun,2010
8. H. Jameel. "A Trust Model for Ubiquitous Systems based on Vectors of Trust Values," *In: The 7th IEEE Int'l Symp. on Multimedia, IEEE Computer Society Press*, Washington. pp.674–679, 2005
9. A. Josang , R. Ismail, C. Body. "A Survey of Trust and Reputation Systems for Online Service Provision," *Decision Support Systems*, 2007, 43(2): 618-644.
10. X. Y. Li, X. L. Gui. "Trust Quantitative Model with Multiple Decision Factors in Trusted Network," *Chinese Journal of Computers*, vol.32, pp. 405-416, May. 2009.
11. Q. Li, X. Zheng. "Research Survey of Cloud Computing," *Computer Science*,2011,38（4）:32-37
12. S. Song ,H. Wang , H. Mac, M. wan. "Fuzzy Trust Integration for Security Enforcement in Grid Computing," *Lecture Notes in Computer Science*, vol.3. pp. 9-21.Jan, 2004.
13. Y.S. Tan, C. Wang. "Trust Evaluation Based on User Behavior in Cloud Computing," *Microelectronics & Computer* vol.11.pp.147-151. Nov, 2015
14. W. Tang, J.B. Hu, Z. Chen. "Research on a Fuzzy Logic-Based Subjective Trust Management Model," *Journal of Computer Research and Developmen*t. vol.42. pp. 1654-1659, Oct, 2005
15. L.Q. Tian, C. Lin. "User Behavior Trust Evaluation Mechanism based on Double Sliding Window ," *Journal of Tsinghua University(Science and Technology)* .2010(5): 763-767.
16. Z.H. Wang, H.B. Pang, Z.B. Li. "An Access Control Scheme for Hadoop Cloud Platform," *Journal of Tsinghua University(Science and Technology)*. Vol.54.pp.53-59, Jan, 2014.
17. H. Xia, Z.P. Jia, H.M. Edwin. "Research of Trust Model based on Fuzzy Theory in Mobile ad Hoc Networks," *IET information security*,2014,8(2).
18. X. Zhou, J. Yu. "Defense System Model based on Trust for Cloud Computing," *Journal of Computer Applications*, vol. 31.pp.1531-1535, Jun, 2011

Zhangwei Yang graduated from the School of Computer Science and Technology, Renmin University of China, for the degree of Master. He entered the Institute of Information and Computer Science in Pingxiang University, as an assistant professor from 2013 to 2016. He visited Hunan University as a visiting scholar from 2016 to 2017. Now he is an assistant professor of Pingxiang University, and the Director of the Engineering Research Centre for Cyberspace Security, Pingxiang, China. He is also a member of China Computer Federation. His current research interests include computer networks and security, cloud computing , and machine learning.

Juan Luo received the Bachelor degree from, National University of Defense Technology, Changsha, China, in 1997, the Master and the Ph.D. degree from Wuhan University, Wuhan, China, in 2005. She visited University of California, Irvine in the U.S.A. as the visiting scholar from 2008 to 2009. Now she is professor of the School of Computer Science and Engineering, Hunan University, Changsha, China. Her current research interests include cloud computing, machine learning and wireless sensors.