Research and Development of Trust Mechanism in Cloud Computing

Jun Xu[1](✉), Feng Xu[1], Wenna Chang[2], and Haiguang Lai[3]

[1] Nanjing University of Aeronautics and Astronautics, Nanjing, China
Xuj023@126.com
[2] Yancheng Teachers University, Yancheng, China
nuanxin@syyz.com
[3] PLA University of Science and Technology, Nanjing, China
lite@263.net

Abstract. As a flexible security mechanism, trust mechanism is widely used in various complex application scenarios. The research on trust and its spread mechanism has become a new hotspot in the fields of E-commerce, Internet of things and Cloud computing. In this paper, we first deeply analyzed the relationship between trust mechanism and cloud computing security, and pointed out the existing problems of current models. We then surveyed some typical trust mechanism according to different mathematic theories of trust computation. We also summarized the latest research achievements of trust model and trust calculation method in cloud computing environment. Based on these studies, we forecasted the direction of further research on trust mechanism.

Keywords: Cloud computing · Trust mechanism · Trust calculation · Reputation · Cloud computing security

1 Introduction

Cloud computing is a new kind of computing model, which takes resource rent, application hosting and outsourcing as the core. Cloud computing has become a hotspot of computer technology quickly, and enhance greatly the ability of processing resources. However, the security challenges of cloud computing should not be overlooked. Only in 2014 occurredpan-European automated real-time gross settlement system 70 million user information was leaked. Home Depot company's payment systems suffered cyber attacks and nearly 56 million credit card users' information was in danger. Sony Pictures was attacked by hackers. Therefore, to make companies organize large-scale application of cloud computing technology and platform, we must thoroughly analyze and solve the security problems in cloud computing.

There is ubiquitous latent danger about data security and privacy because of cloud computing's dynamic nature, randomness, complexity and openness. The main security issues of the current cloud computing are how to implement a mechanism to distinguish and isolate bad users to refrain users from potential safety threat. Meanwhile, services and the quality of service providers in the cloud computing environment are uneven, and the service provider is not sure to provide authentic, high-quality content

© Springer International Publishing Switzerland 2015
Z. Huang et al. (Eds.): ICCCS 2015, LNCS 9483, pp. 218–229, 2015.
DOI: 10.1007/978-3-319-27051-7_19

and services. Therefore, it is essential to confirm the quality of cloud services and cloud services provider.

Current research to solve the above problems are concentrated on the study of trust and the mechanism of reputation aspect, whose basic idea is to allow trading participants to evaluate each other after the transaction, and according to all the evaluation information to each participant to calculate this participant's credibility to provide references about choosing trade object to the other trading partners in network in the future.

This paper is based on the key issues of trust mechanism to introduce its latest research achievements. Section 2 of this paper introduced the concepts of cloud computing. Section 3 analyzed relationship between the trust mechanism and cloud computing security deeply. Section 4 selected the latest and typical trust model to classify and review based on different methods of mathematics calculation. Section 5 to review separately based on trust mechanism's application situation of security problems in cloud computing layers. Section 6 analyzes current problems and prospects new research opportunities.

2 Cloud Computing

At present, although there are many versions of the definition of cloud computing, the most comprehensively accepted is the definition of the National Institute of Standards and Technology [1], they believe cloud computing has five indispensable characteristics: On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured service, and the cloud services are divided into 3 levels: IaaS, PaaS, SaaS. In order to achieve localization of computing resources, now Microsoft, IBM and other companies can be considered to provide a new service model of server container leasing services, which is called Hardware as a Service, HaaS [2].

HaaS, IaaS, PaaS, and SaaS are different in the functional scope and focus. HaaS only meets the needs of tenants hardware resources, including storage space, computing power, network bandwidth and so on, focusing on the performance of the hardware resources and reliability. IaaS provides pay-as, measurable resource pools function in heterogeneous resources environment, taking the full use of hardware resources and users' requirements into account; not only the integration of the underlying hardware resources does PaaS concern about, but also provides users with customizable applications services by deploying one or more application software environments. SaaS not only achieves the full advantage of the underlying resources required, it must also provide users with customizable application services through the deployment of one or more application software environment. Paper [3] summarizes a cloud service delivery model according to various embodiment ways of various service models, which is shown in Fig. 1:

Cloud computing is essentially a methodological innovation in infrastructure design, which has shared pool of IT resources composed by a large number of computer resources. Cloud computing model has significant advantages in information processing, information storage and information sharing, making dynamical creation of highly visualized application services and data resources available to users.

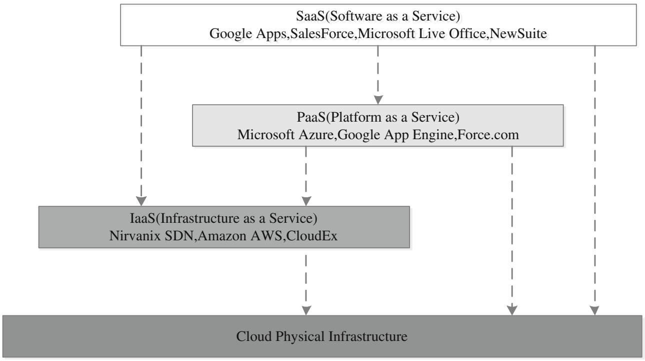
SaaS(Software as a Service)
Google Apps,SalesForce,Microsoft Live Office,NewSuite
PaaS(Platform as a Service)
Microsoft Azure,Google App Engine,Force.com
IaaS(Infrastructure as a Service)
Nirvanix SDN,Amazon AWS,CloudEx
Cloud Physical Infrastructure

Fig. 1. Cloud service delivery model

3 Trust Mechanism and Cloud Computing Security

In the complex network environment, threats to security may be in the form of various ways. But generally speaking, the network security is intended to provide a protective mechanism, to avoid being vulnerable to malicious attacks and illegal operations. Basically all security mechanisms have adopted some trust mechanism to guard against security attacks. But the development of any mechanism is accompanied by the game between user and mechanism builder. With the understanding of the trust mechanism, a variety of attacks to trust mechanism have emerged.

The key issues included in trust mechanism are trust modeling and data management. The tasks of trust modeling are to design scientific trust model, describing and reflecting the trust relationship in the system accurately by using appropriate metrics. Data management relates to safety, efficient storage, access trust and their distribution in a distributed environment which is in the absence of centralized control.

Security and privacy are the most concerned issues of cloud computing users. With the emergence of more and more security risks, industry and academia have put forward appropriate security mechanisms and management methods. Its main purposes are to prevent cloud service providers from malicious leak or sell privacy information of user, collecting and analyzing user data. Paper [4] summarized security problems faced by cloud computing of specific services from technical perspective for the layers. Paper [5] proposed a Framework including Cloud Computing Security Service System and Cloud Computing Security Evaluation System.

Trust modeling and study of credibility management in cloud computing are still in their infancy. Study of Trust Management in the current includes the establishment and management of trust between service providers and their trust with users. Its main information security ideas can be summarized as the three-dimensional defense and defense in depth, forming a whole life cycle of the safety management whose main feature are warning, attack protection, response and recovery.

4 Trust Model

For different application scenes, many scholars used different mathematical methods and tools to build various models of trust relationship. This section will introduce common trust modes from the perspective of mathematical methods such as weighted average, probability theory, fuzzy logic, gray reasoning, machine learning, statistical analysis and analyze specific trust calculation.

4.1 Trust Model Based on Weighted Average

Trust model based on weighted average is the trust value to be formed by the weighted average, forming the trust evaluation from comprehensive views of different aspects, which may be divided into global trust model and local trust model. EigenTrust model [6] is the most representative incalculation model study of global trust model. EigenTrust obtain global trust value of each peer by iteration based on the reputation of peers' transaction history by using a similar Page Rank algorithm, as shown in Eq. (1):

$$\vec{t}^{(k+1)} = (1-a)C^T\vec{t}^{(k)} + a\vec{p} \tag{1}$$

Where, C represents a global trust value vector which is a normalized local trust value matrix $[c_{ij}]$, $\overrightarrow{t}^{(k)}$ is the trust value vector afterK iterations, $\overrightarrow{p}$ is global trust value vector of the pre-trusted peers ($p_i = 1/|P|$ if $i \in P$, otherwise $p_i = 0$), P is pre-trusted peer set.

PowerTrust algorithm [7] has improved algorithm EigenTrust mainly from three aspects: (1) confirm trusted peers collection reasonably. By mathematical reasoning, proved the existence of the power-law relationship among peers evaluation, namely there is a few Power peers, which formed credible set of peers by PowerTrust. (2) speed up the convergence of the iteration process. PowerTrust put forward the strategy of Look-ahead Random Walk (LRW), which made trust value polymerization rate improved greatly. (3) establish a dynamic applicable mechanism. Its disadvantages include: (1) It calculated the trust value without considering about the volume of transaction, which allow malicious users to accumulate trust by small transactions and deceive on large transactions easily. (2) there is no penalty to malicious behaviors.

PeerTrust [8] gives a local trust model, the trust value of peers is calculated only by the peers who have had dealings with them, without the entire network iteration, the mathematical description of the model is shown as Eq. (2):

$$T(u) = \alpha\sum_{i=1}^{I(u)} S(u,i) * Cr(p(u,i)) * TF(u,i) + \beta * CF(u) \tag{2}$$

Where $p(u,i)$ is the set of peers which trade with peer μ in the i-th transaction, and the credibility of peer v is $Cr(v)$, $TF(u,i)$ is the trust factor produced by the transaction with peer μ, α and β are weight parameter of standardized trustvalues, and $\alpha + \beta = 1$.

PeerTrust's advantages are: (1) the evaluation factors are normalized so that malicious peers can't submit too high or too low rating. (2) proposed a trust evaluation polymerization method PSM based on personal similarity to resist malicious peers' collusion attack. (3) established a trust calculation method by using adaptive time window to inhibit dynamic swing behavior of peers.

DyTrust model [9] presented a dynamic trust model based on the time frame, which takes the impact of time on the trust calculations into account, the authors also introduced four trust parameters in computing trustworthiness of peers, namely, short time trust, long time trust, misusing trust accumulation and feedback credibility. Paper [10] refined trust algorithm by introducing the experience factor, improving the expansibility of feedback reliability algorithms in Dytrust model. Paper [11] further improved the Dytrust model and enhanced the aggregation ability of feedback informationby introducing risk factor and time factor.

4.2 Trust Model Based on Probability

In the probabilistic trust model mainly use the maximum likelihood estimation, Bayesian and other mathematical methods to calculate the value of the trust.

Maximum Likelihood Estimation (MLE) is a method of probability-based trust reasoning, mainly for the probability model and beliefs model. In the circumstance of probability distribution of trust is known and the parameters of the probability distribution are unknown.

Despotovic et al. [12] presented a way of calculating the peers trust by using MLE, the algorithm thought: Supposing θ_j is peer j's honest interaction probability, $p_1, p_2, \ldots, p_n$ is the peer has history interaction with peer j, after the interaction, $l_1, l_2, \ldots l_k, \ldots, l_n$ is the probability that $p_1, p_2, \ldots, p_n$'s dishonest feedback evaluation to peer j, $P[Y_k = y_k]$ presents the probability of observing report y_k from peer p_k, it was expressed as follow:

$$P[Y_k = y_k] = \begin{cases} l_k(1-\theta_j) + (1-l_k)\theta_j \ \mathit{if}\ y_k = 1 \\ l_k\theta_j + (1-l_k)(1-\theta_j) \ \mathit{if}\ y_k = 0 \end{cases} \quad (3)$$

The likelihood function can be expressed as:

$$L(\theta_j) = P[Y_k = y_k]P[Y_2 = y_2]\ldots P[Y_n = y_n] \quad (4)$$

Where, $y_1, y_2, \ldots, y_n$ are independent reports of each other. Their experiment showed that good calculations can be accomplished even with 10–20 reports recovered. In order to improve the accuracy of the estimate, the author introduced the concept of peers liedegree, but not giving calculation of the peers liedegree, and estimate value got by this method is either 0 or 1, which is difficult to accurately portray the credibility of peers.

Bayesian approach is posterior probability estimate based on the outcome, which is suitable for the probability model and the belief model. The difference with the MLE is that it specifies the prior probability distribution for presumed parameters, and then according to the transaction results, using Bayes' rule to speculate posterior probability of parameters.

In Bayesian methods, Dirichlet prior probability distribution is assuming there are k kinds of results, the prior probability distribution of each result appears uniform distribution, i.e., the probability of each occurrence is 1/k. There is a total of n transactions, and each transaction gives the evaluation, wherein the number of appearance of i (i = 1, 2, …, k) evaluation is $m_i(\sum m_i = n)$. The posterior distribution of parameter p to be estimated is:

$$f(p, m, k) = \frac{1}{\int_0^1 \prod_{i=1}^{k} x^{(m_i + C/k - 1)} dx} \prod_{i=1}^{k} p_i^{(m_i + C/k - 1)} \tag{5}$$

Wherein, C is a preset constant. The bigger is C, the smaller is evaluation results 'expectation value to the parameters p. C is generally chosen as k. Bayes estimate expected value of the i-th evaluation results' appearance probability is:

$$E(p_i) = \frac{m_i + C/k}{C + \sum_{i=1}^{k} m_i} \tag{6}$$

Paper [13] proposed trust algorithm based on Dirichlet distribution. Using probabilistic expectations to express confidence reflect the uncertainty of confidence. Introducing time decay factor in the calculation process, it can suppress partially malicious users' malicious transactions after accumulating certain confidence value. But it didn't give too much consideration to the ability of the algorithm's resistance to malicious acts or to the recommendation trust and transaction volume.

4.3 Trust Model Based on Fuzzy Logic

Membership in the fuzzy theory can be regarded as the extent that body belonging to a trusted collection. After fuzzy evaluation of data, according to fuzzy rules based on these fuzzy data, trusted system inferthe trustworthiness degree of the body. Fuzzy reasoning process can be divided into three procedures: fuzzification, fuzzy inference and defuzzification (Fig. 2).

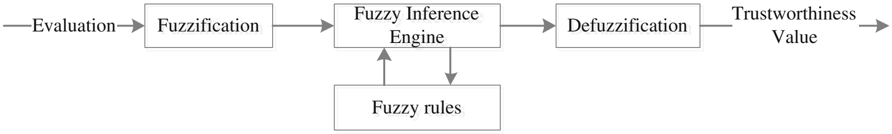

Fig. 2. Fuzzy inference framework

Paper [14] proposed a method of Fuzzy-based Trust Evaluation FTE, based on fuzzy reasoning, which has three input parameters in the fuzzy process: Weighted Trustworthiness Value (WTV), Opinion Weight (OW) and Agent Credibility (AC). When calculating WTV, consider two aspects of the data, direct transaction record and recommended transaction record. Supposing S is the amount of transactions, t_{val} was trading evaluation, n is the current time, and m is the evaluation time, calculation formula of WTV is shown as (7).

$$WTV = \frac{\sum_{s=1}^{S} \left[e^{-(n-m)/D} * ((t_{val} - t_{\min})/(t_{\max} - t_{\min})) * 5 \right]}{S} \tag{7}$$

D is the time decay function, fuzzy membership function value triangular fuzzy reasoning fuzzy when trust. After defuzzification, numerical trust value can be obtained. FTE algorithm enhanced the ability to resist against malicious behavior by adjusting WTV, OW and AC three input parameters. The downside is that: (1) There is no calculation or assessment of OW. (2) It can be challenging to choose the membership function with high efficiency. (3) There is no demonstration of the model's convergence.

FuzzyTrust [15] use the fuzzy logic inference rules to compute peers' global reputation. It has a high detection rate of malicious peers, however, the model did not consider the trust factors that affect the quality of the evaluation, and the authors did not demonstrate the convergence of the model. FRTrust [16] uses the fuzzy theory to calculate the peer trust level, reducing the complexity of the trust computation, and improves the trust ranking precision. Paper [17] puts forward the ETFT model by the combination of the evidence theory and fuzzy logic, which improves the adaptation ability of the model in the dynamic environment, and the aggregation speed of the recommendation trustis accelerated.

4.4 Trust Model Based on Statistical Analysis

It's based on statistical analysis method, depending on different application context by integrating multiple dimensions associated with the trust, such as historical information, contextual information, and reputation information to predict the trust relationship of high accuracy.

UgurKuter et al. [18] proposed an inference trust relationship based on probability network, and proposed trust reasoning algorithm SUNNY to calculate the trust value of social network. Jie et al. [19] presented presumed framework of social relationships by learning various networks, which synthesized social theory as a factor graph model, and validly improved the accuracy of reasoning the category of social relations in the target network. Rettinger et al. [20] resolved the problem of trust reasoning based on past observations and contextual information and proposed trust model IHRTM, which uses statistical relationship learning to obtain context sensitive information, including trustee's individual characteristics and situational state. However, the model due to lacking of adaptive learning strategy that it has some limitations in practical applications.

Khiabani et al. [21] propose to build trust model UTM by the integration of history, recommendations, and other contextual information to calculate the scores between individuals, which can be efficiently used for low-interaction environments.

4.5 Trust Model Based on Machine Learning

Methods based on machine learning can be divided into two categories: forecasting methods of supervision trusts and unsupervised trusts forecasting methods. The main idea is to use machine to learn methods to dynamically generate rules, then combining fuzzy reasoning and rule-based reasoning to obtain the trust level of the entity.

Supervision Trusts prediction method first extracts features from the source data, and then based on these features of the training binary classifier. Liu et al. [22] presented a classification method to deal with the trust prediction problem. However, the results of the assessment are absolute, that is, trust and not, and the uncertainty of trust is ignored. Zolfagharet al. [23] proposed the formation of trust incentive framework, and use data mining and classification method for the formation of the trust, the trust proposed framework consists of knowledge, association, similarity, self-confidence and other factors.

Unsupervised trust prediction methods are mostly based on trust evolution, which depends on the trust relationship already existed in the user; but when the trust relationship is very sparse, trust evolution may fail. Tang et al. [24] research trust prediction through exploration homogeneous effect, and build trust forecasting model hTrustby using low- rank matrix factorization technique. Ref. [25] take the impact of sociological theory on the trust relationship predict into account, through the study of social class theory and homogeneity theory to obtain the development law of trust relationship, and then build a trust relationship prediction model to solve the data sparseness problem, increasing the precision of trust relationship forecast.

5 Trust Model in Cloud Computing

Cruz et al. [26] have summed up the security problem in cloud computing, which includes the infrastructure security, data security, communication security and access control. Trust management has become the bridge of interaction entities in cloud computing. This section describes the application of trust model in the aspects of virtual machine security, user security, application reliability and service quality.

5.1 Trust Model in Virtual Machine

In the cloud infrastructure, the virtual machine is widely used as the carrier of the user data, and how to guarantee the credibility of the virtual machine becomes the key means to ensure the cloud computing security. Because of the trust evidence sources of cloud computing nodes are usually insufficient, and during the attestation process sensitive information of the involved nodes is easily exposed. [27] presented a trust-based trustworthiness attestation model (TBTAM) for virtual machine, when calculate the trustworthiness of virtual machine, TBTAM considers both direct trustworthiness and feedback trustworthiness, and then uses the group-signature method for proof protection, which protects the privacy of nodes and reduces the attack possibilities. Their experimental results indicate that the model can validly identify spiteful peers and protect privacy of virtual machine peers during the running process.

5.2 Trusted Service Mechanism for Cloud Computing

Due the uncertainty and the reliability of the application in cloud computing. Tan et al. [28] presented a cloud workflow trust model TWFS service-oriented scheduling to meet the requirements of ES integration. They proposed balance strategies to help users to balance different requirements, including trust evaluation, execution time, execution cost of fuzzy multi-objective problem. The key idea of the TWFS algorithm is to find the optimum solution with the deadline constraint by adjusting the weights of time and cost.

When assign the weight of recommendation trust, the similarity between users a and i was computed by the Pearson correlation coefficient (PCC) as follows:

$$\omega_{ai} = \frac{\sum_{j \in S} (v_{aj} - \overline{v_a})(v_{ij} - \overline{v_i})}{\sqrt{\sum_{j \in S} (v_{aj} - \overline{v_a})^2 + (v_{ij} - \overline{v_i})^2}} \tag{8}$$

where $avg(v_i)$ is the average rating by user i.

Using max-min as the operator, when calculate the trust evaluation of the service. The calculation of the execution time and the execution price is similar to that of this.

TWFS can form an optimum workflow application while meeting different constraints from users. Meanwhile, it puts a general trust metric scheduling algorithm to consider direct trust and recommendation trust. However, TWFS does not consider the dynamic of the cloud environment, and be vulnerable to malicious attacks.

5.3 Services Quality Evaluation

Jagpreet et al. [29] proposed a trust model to estimate service providers to help users choose the most dependable service provider and service, the model based on feedback trust by introducing three different types of trust (namely, interaction-based trust, compliance-based trust and recommendation-based trust.), According to its priority assigned different weights, in order to calculate the trust service providers. However, their paper didn’t introduce how the weight is distributed, and the model is lack of dynamic.

For cloud computing environment dynamic presence of trust issues, paper [30] proposed a trust model based on double excitation and detection of deception (CCIDTM). The model proposes a set of cloud computing services property evaluation, and used the service attribute weight factor to measure the service attribute relative service evaluation of the important degree. This model introduced a dynamic trust mechanism trust decay with time, the establishment of the service provider service user behavior and evaluate the behavior of a double incentive. It presents a conspiracy to deceive detection algorithm to improve dynamic adaptability and comprehensive evaluation model. Compared with the existing trust model, the model assessment results closer to service provider of real service behavior, can effectively resist all kinds of malicious conduct attacks, showed good robustness, but the model does not consider the quality of composite services in cloud computing environment.

5.4 User Trust Evaluation

In order to distinguish user behavior from cloud computing environment, the paper [31] proposed a cloud computing trust model based on user behavior called Fuzzy ART. To ensure the identity and behavior of users in the system, a softcomputing technique is proposed which an unsupervised learning technique to classify the virtual clients based on their behavior.

To ensure cloud security in complex and dynamic environment, LVet al. [32] effectively confirmed the untrusted cloud terminal users and correctly analyzing their abnormal behavior. This paper adopted the method of fuzzy analytic network process (FANP) based on triangular fuzzy numbers, which can reflect the fuzziness of expert evaluation through using fuzzy numbers, and weaken the subjectivity of simply using ANP. However, the node trust value of the model has a large time complexity, and is not suitable for large-scale distributed environment, and the algorithm is not effective and the lack of convincing.

To solve the increasingly prominent security issues during the process of multi-tenants visit in cloud computing, the paper [33] proposed a security access control model based on user behavior trust. The model obtained the user's behavior evidence through real-time monitoring of massive users' access behavior in the cloud. The comprehensive evaluation of user's behavior trust based on fuzzy consistent matrix effectively improves the operation efficiency of the model, eliminating the complex judgment matrix adjustment process. It established the dynamic allocation mechanism of user service level based on behavior trust level, not only can effectively control the users' non security access behavior, protecting the important resource in the cloud, but also establish long-term trust mechanism between the users and the cloud service by the real-time feedback of user behavior trust status.

6 Summary and Prospect

The research of trust management system is from centralized trust to distributed trust relationship, from static to dynamic trust model, from single to multiple input factor model, from evidence theory model to a variety of mathematical model. It can be said that the study of trust relationship is a very active direction.

However, through summary we can see that the research on the trust mechanism has the following problems in the theory and the realization: (1) The current study of trust mechanism is lack of risk mechanism and performance evaluation criteria of the unified trust model. (2) In the existing research, the performances of the trust model are mostly evaluated by the method of simulating experiment, and there is no real performance evaluation.

Through this paper, we can see that in the cloud computing and other new computing environment, various security requirements and application mode have put forward new challenges to the trust mechanism. With the emergence of new computing models and computing environments, such as cloud computing, internet of things and so on, refining scientific problems under the new situation of trust mechanism and carrying on the research have more urgent significance.

At the same time, it should also continue to explore new models suitable for describing the dynamic trust relationship, combining knowledge of other subjects, such as machine learning, artificial intelligence, etc.

Acknowledgments. This work is supported by the China Aviation Science Foundation (NO. 20101952021) and the Fundamental Research Funds for the Central Universities (NO. NZ2013306).

References

1. Mell, P., Grance, T.: The NIST definition of cloud computing. Nat. Inst. Stand. Technol. **53**, 50 (2009)
2. Chuang, L., Wen-Bo, S.: Cloud Computing Security: Architecture, Mechanism and Modeling. Chin. J. Comput. **36**, 1765–1784 (2013) (in Chinese)
3. Almorsy, M., Grundy, J., Müller, I.: An analysis of the cloud computing security problem. In: Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30 November 2010
4. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. **34**, 1–11 (2011)
5. Feng, D.G., Zhang, M., Zhang, Y., Zhen, X.U.: Study on cloud computing security. J. Softw. **22**, 71–83 (2011)
6. Kamvar, S.D., Schlosser, M.T., Garcia-Molina, H.: The Eigentrust algorithm for reputation management in P2P networks. In: Proceedings of the 12th International World Wide Web Conference, WWW 2003 (2003)
7. Kai, H., Zhou, R.: PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing. IEEE Trans. Parallel Distrib. Syst. **18**, 460–473 (2007)
8. Li, X.: Liu, L.: PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. IEEE Trans. Knowl. Data Eng. **16**, 843–857 (2004)
9. Jun-Sheng, C., Huai-Ming, W.: DyTrust: A time-frame based dynamic trust model for P2P systems. Chin. J. Comput. **29**, 1301–1307 (2006) (in Chinese)
10. Shao-Jie. W., Hong-Song, C.: An improved DyTrust trust model. J. Univ. Sci. Technol. Beijing, **30**, 685–689 (2008) (in Chinese)
11. Zhi-Guo, Z., Qiong, C., Min-Sheng, T.: Trust model based on improved DyTrust in P2P network. Comput. Technol. Dev. 174–177 (2014) (in Chinese)
12. Despotovic, Z., Aberer, K.: Maximum likelihood estimation of peers; performance in P2P networks. In: The Second Workshop on the Economics of Peer-to-Peer Systems (2004)
13. Haller, J., Josang, A.: Dirichlet reputation systems. In: 2012 Seventh International Conference on Availability, Reliability and Security, 112–119 (2007)
14. Schmidt, S., Steele, R., Dillon, T.S., Chang, E.: Fuzzy trust evaluation and credibility development in multi-agent systems. Appl. Soft Comput. **7**, 492–505 (2007)
15. Song, S., Kai, H., Zhou, R., Kwok, Y.K.: Trusted P2P transactions with fuzzy reputation aggregation. IEEE Internet Comput. **2005**, 24–34 (2005)

16. Javanmardi, S., Shojafar, M., Shariatmadari, S., Ahrabi, S.S.: FRTRUST: a fuzzy reputation based model for trust management in semantic P2p grids. Int. J. Grid Util. Comput. **6**, (2014)
17. Tian, C., Yang, B.: A D-S evidence theory based fuzzy trust model in file-sharing P2P networks. Peer Peer Netw. Appl. **7**, 332–345 (2014)
18. Kuter, U.: Using probabilistic confidence models for trust inference in web-based social networks. ACM Trans. Int. Technol. Toit Homepage **10**, 890–895 (2010)
19. Tang, J., Lou, T., Kleinberg, J.: Inferring social ties across heterogeneous networks. In: WSDM 2012, 743–752 (2012)
20. Rettinger, A., Nickles, M., Tresp, V.: Statistical relational learning of trust. Mach. Learn. **82**, 191–209 (2011)
21. Khiabani, H., Idris, N.B., Manan, J.L.A.: A Unified trust model for pervasive environments – simulation and analysis. KSII Trans. Int. Inf. Syst. (TIIS) **7**, 1569–1584 (2013)
22. Liu, H., Lim, E.P., Lauw, H.W., Le, M.T., Sun, A., Srivastava, J., Kim, Y.A.: Predicting trusts among users of online communities: an epinions case study. In: Ec 2008 Proceedings of ACM Conference on Electronic Commerce, pp. 310–319 (2008)
23. Zolfaghar, K., Aghaie, A.: A syntactical approach for interpersonal trust prediction in social web applications: Combining contextual and structural data. Knowl. Based Syst. **26**, 93–102 (2012)
24. Tang, J., Gao, H., Hu, X.: Exploiting homophily effect for trust prediction. In: Proceedings of the Sixth ACM International Conference on Web Search and Data Mining, 53–62 (2013)
25. Ying, Wang, Xin, Wang, Wan-Li, Zuo: Trust prediction modeling based on social theories. J. Softw. **12**, 2893–2904 (2014). (in Chinese)
26. Cruz, Z.B., Fernández-Alemán, J.L., Toval, A.: Security in cloud computing: a mapping study. Comput. Sci. Inf. Syst. **12**, 161–184 (2015)
27. Zheng-Ji, Z., Li-Fa, W., Zheng, H.: Trust based trustworthiness attestation model of virtual machines for cloud computing. J. Southeast Univ. (Nat. Sci. Ed.) **45**(1), 31–35 (2015) (in Chinese)
28. Tan, W., Sun, Y., Li, L.X., Lu, G.Z., Wang, T.: A trust service-oriented scheduling model for workflow applications in cloud computing. IEEE Syst. J. **8**, 868–878 (2014)
29. Sidhu, J., Singh, S.: Peers feedback and compliance based trust computation for cloud computing. In: Mauri, J.L., Thampi, S.M., Rawat, D.B., Jin, B. (eds.) Security in Computing and Communications, vol. 467, pp. 68–80. Springer, Heidelberg (2014)
30. Xiao-Lan, X., Liang, L., Peng, Z.: Trust model based on double incentive and deception detection for cloud computing. J. Electron. Inf. Technol. **34**(4), 812–817 (2012) (in Chinese)
31. Jaiganesh, M., Aarthi, M., Kumar, A.V.A.: Fuzzy ART-based user behavior trust in cloud computing. In: Suresh, L.P., Dash, S.S., Panigrahi, B.K. (eds.) Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, vol. 324, pp. 341–348. Springer, India (2015)
32. Yan-Xia, L., Li-Qin, T., Shan-Shan, S.: Trust evaluation and control analysis of FANP-based user behavior in cloud computing environment. Comput. Sci. **40**, 132–135 (2013) (in Chinese)
33. Guo-Feng, S., Chang-Yong, L.: A security access control model based on user behavior trust under cloud environment. Chin. J. Manag. Sci. **52**, 669–676 (2013) (in Chinese)