A Trust Assessment Model Based on Recommendation and Dynamic Self-adaptive in Cloud Service

Yiqin Lu\textsuperscript{a}, Yahui Fang\textsuperscript{b}, Jiancheng Qin\textsuperscript{c}

School of Electronic and Information Engineering, South China University of Technology, Guangzhou, China
\textsuperscript{a}eeyqlu@scut.edu.cn, \textsuperscript{b}ffangyahui@163.com, \textsuperscript{c}jcqin@scut.edu.cn

Abstract. Cloud computing is a completely distributed sharing platform, through which users can request personalized cloud services. With the continually expansion of cloud services scale, more and more service providers are offering services with similar functions but different qualities. Users are faced with the problem of selecting the most suitable cloud services from numerous cloud services. In this paper, a trust assessment model based on recommendation and dynamic self-adaptive in cloud service is proposed. In the trust assessment model, trust is divided into direct trust and indirect trust, which can make the evaluation of trust value more accurate. In addition, a recommendation mechanism is proposed in this paper, the third-party nodes make recommendations according to the actual situation, and accept reward or punishment automatically after interacting. Experiment shows that the model can accurately evaluate the trust between nodes, and effectively resist the attack of malicious nodes.

1. Introduction
Cloud computing is a distributed resource sharing platform. Users can request personalized cloud services through the network [1]. According to a survey of cloud services, there are nearly 50 million users using personal cloud service. But the security problems of cloud computing are becoming increasingly prominent [2]. In 2007, Salesforce.com, a famous cloud service provider, was attacked during the service process, causing a large number of users’ data information to be leaked or lost. And google also had a large number of users’ files to be leaked.

At present, there are many cloud service providers at domestic and overseas, such as Amazon Cloud Service, Google File System, aliyun and so on. As the scale of cloud services continues to expand, users are faced with the problem of selecting the most suitable cloud services from numerous cloud services. However, trust is subjective, dynamic and influenced by many factors in a cloud environment [3]. Both cloud service providers and users have their own interest needs, this may lead them to choose egoism, even malicious behavior. Trust is one of the most challenging issues in the promotion and application of cloud service. In order to ensure that users can choose high-quality and security services, there must be an effective credibility evaluation and selection method of cloud services. Nevertheless, most existing cloud trust management mechanism has limitations that prevent them from being fully effective [4].

In view of the characteristics like virtualization, openness, transparency, dynamics and security of cloud services, the paper proposed a trust assessment model based on recommendation and dynamic self-adaptive in cloud service. In this paper, trust is divided into direct trust and indirect trust. Direct trust is obtained according to the historical interaction records between nodes, while indirect trust is calculated according to the trust value provided by the third-party recommendation nodes. It can make...
the estimates of trust more accurate. In addition, we propose a recommendation mechanism, the third-party nodes shall be responsible for its own recommendation evaluation, and receive reward or punishment measures according to the real situation to motivate nodes to provide high-quality service and real recommendation. The model can update nodes' trust automatically. It can solve the dynamic trust update problem of cloud service. Experimental results show that the model this paper proposed has high accuracy and dynamic adaptability, and can effectively resist malicious behaviors in the system.

The organization of this paper is as follows: Section 2 is a review of the related works of trust model. Section 3 describes the details of the trust assessment model. In section 4, we take the experiments to support the model, and the results reveal a good effect. Finally, section 5 concludes the paper and describes future work.

2. Related Work
The main problems in the credibility evaluation and selection of cloud service are the accuracy and dynamics of trust, and malicious behaviors of nodes. Scholars at home and abroad have made extensive research on this issue.

Marudhadevi [5] proposed a trust mining model (TMM), which can discover knowledge from previously monitored data sets and generate trust value. The method can achieve better accuracy. A cloud service discovery algorithm based on fuzzy trust estimation is proposed [6]. The model ensures relatively higher trust accuracy and transaction success rate. Li [7] proposed a scheme based on trust for cloud service selection, the scheme includes the service chosen and service delivered, the method can choose cloud service through its trust value. It can ensure the security of the service.

However, the resources and the reliability of cloud services are dynamic, the methods above do not work well in a dynamic cloud environment. Wang [8] proposed a dynamic cloud service trust evaluation model based on service-level agreement (SLA) and privacy-awareness, the model can improve users’ satisfaction. A framework is proposed [9] to quantify and ranking the reliability of cloud services, and the evaluation results are accurate and flexible. Yao [10] proposed a trust dynamic level approach control method to help the user select a trustworthy node in the network. Although the above methods have good adaptability, they cannot effectively resist malicious attacks launched by malicious nodes.

This paper proposed a trust assessment model based on recommendation and dynamic self-adaptive in cloud services: The trust is divided into direct trust and indirect trust, then calculate to get the comprehensive trust value, the method can make the estimates of trust more accurate. And we propose a recommendation mechanism, nodes automatically receive reward or punishment after interacting, it can solve the dynamic trust update problem of cloud service. In a word, the new model has high accuracy and dynamic adaptability, and can effectively resist malicious behaviors.

3. Details of Trust Model

3.1 Interaction Process
Entity: An entity represents a cloud service user or cloud service provider. A cloud service user is denoted as C (Client), a cloud service provider is denoted as S (Server). An interaction between node C and node S is taken as an example to introduce the interaction process. The process can be summarized as follows:

- Step1: Request interaction. Node C makes an interaction request to node S, Nodes C and S query each other’s trust values respectively. Only if both trust values greater than the trust threshold can the interaction proceed to the next step.
- Step2: Calculate direct trust. C calculates the direct trust value to S through historical interaction records.
- Step3: Ask for recommendation. Node C sends recommendation requests to the third-party nodes to obtain the trust information of S, third-party nodes decide whether to make recommendations according to the actual situation.
• Step 4: Calculate indirect trust. According to the trust information that third-party nodes provided, indirect trust can be calculated.
• Step 5: Compute comprehensive trust. Calculate the comprehensive trust, and proceed to the next step only if the comprehensive trust is greater than the trust threshold.
• Step 6: Grant authority. Converts trust value into interactive permission.
• Step 7: Interact. Node C obtains cloud services through interacting with node S.
• Step 8: Update trust value. Node C evaluates the service satisfaction of S after interaction, and updates the recommendation nodes’ trust according to the satisfaction automatically.

3.2 Comprehensive Trust Calculate Model
Each node in the model manages its own trust data, the historical interactive records with other nodes are shown in table 1:

| Identity | Interaction number | Interaction time | Evaluation |
|----------|--------------------|------------------|------------|
| id num   | num                | time             | r          |

The direct trust value (dt) can be obtained according to the mean interactive evaluation value (r) of N times to the target node, as in (1):

$$dt = \frac{\sum_{i=1}^{N} r_i}{N}$$  \hspace{1cm} (1)

Then node C selected recommendation nodes which direct trust greater than 0.5 and rank the top N, respectively send recommendation request to the N nodes. After third-party nodes receive the recommendation request, and send dt of S to C. The indirect trust value is determined by multiplied of the trust value provided by all third-party recommendation nodes and the corresponding weight. The trust value weight of each recommendation node is related to the dt of C to them. The weight $\omega$ is shown in (2):

$$\omega = \frac{dt_u}{\sum_{j=1}^{N} dt_j}$$  \hspace{1cm} (2)

Indirect trust (it) can be obtained by (3):

$$it = \sum_{j=1}^{N} \omega_j * dt_j$$  \hspace{1cm} (3)

Finally, the comprehensive trust can be calculated according to the direct trust and indirect trust, as shown in (4), $\rho$ is the weight of dt.

$$T = \rho * dt + (1 - \rho) * it$$  \hspace{1cm} (4)

3.3 Interactive Permissions
After calculating the comprehensive trust, then we convert the trust value into interaction permissions, and set $T_{th}$ as interaction threshold. When trust value T is less than the threshold, the interaction is rejected; when T is greater than the threshold, different permissions are granted according to the trust value. Authority increases with the increase of trust value, and the growth rate is slow at first, and then accelerates with the accumulation of trust value. The quantitative relationship between authority and trust value can be expressed as (5):

$$auth = \begin{cases} 0.5^* [sin(\pi(T - 0.5) + 1)] * T \geq T_{th} \\ 0 \end{cases}$$  \hspace{1cm} (5)
3.4 Update Trust
Node C will evaluate the service of node S after the interaction. An important point in the recommendation mechanism is that not only the interaction node will be affected by the evaluation, but also recommend nodes will receive corresponding reward and punishment measures. Rewards and punishments are based on the deviation degree error between the trust value provided by the recommendation node and the interactive evaluation $R$, which is expressed as dev, as shown in (6):

$$\text{dev} = |dt_{cs} - R|$$  \hspace{1cm} (6)

Within the tolerance ($\text{tol}$), the smaller the error is, the more reliable the recommendation is, and the node shall receive corresponding reward. On the contrary, the larger the error is, beyond the tolerance of error, the less reliable the recommendation is, and the node shall receive corresponding punishment. $\partial$ represents incentive and penalty factor. Specific reward and punishment formulas for direct trust are shown as (7):

$$dt_{cs}' = dt_{cs} + \partial \times (\text{tol} - \text{dev})$$  \hspace{1cm} (7)

At this point, the entire interaction process is completed, including dynamic adjustment of trust.

4. Experimental Result
In this paper, the performance analysis of Recommendation and Dynamic Self-adaptive Trust Assessment Model (RDSTAM) with different proportions of malicious nodes is carried out through simulation experiments. The simulation experiment realized a simulated cloud file download network through C++. Parameters of RDSTAM are set before the experiment, as shown in table 2.

| Parameter | Parameter describe | The value |
|-----------|--------------------|-----------|
| $T_s$     | Trust threshold    | 0.4       |
| tol       | Tolerance for error| 0.15      |
| $\partial$| Incentive factor   | 0.6       |

And the nodes in the network are divided into two types: normal nodes and collude malicious nodes. Normal nodes always provide accurate information and truthful feedback. However, collude malicious nodes are organized saboteurs, as a service node, it always provides accurate information to nodes within the organization and harmful information to nodes outside the organization. As a recommendation node, it always provides true feedback to the recommendation requests of the nodes within the organization, provides falsely high recommendation trust value to the nodes outside the organization to exaggerate the similar nodes, and provides extremely low recommendation trust value to defame the nodes outside the organization.

4.1 Comparison of Interactive Success Rate
In order to verify the interaction success rate of RDSTAM under different proportions of malicious nodes, several groups of experiments were set up in this paper. There are 100 nodes in the experiment, among which the proportion of malicious nodes increased from 0% to 50%. Each experiment interacts for 10000 times, and the probability of interaction request response is 100%. The other two groups of comparative experiments are CCIDTM model proposed by Xie [11] and classic EigenRep model proposed by Kamvar S.D [12]. In the case of different proportions of malicious nodes, the comparison of interaction success rate of the three models is shown in Fig.1:
According to the experimental results, the interaction success rate of RDSTAM is significantly higher than that of CCIDTM and EigenRep model. Even if the proportion of malicious nodes reaches 50%, the interaction success rate of RDSTAM is still more than 90%. This proves that this model can accurately calculate the trust value of nodes and has good dynamic adaptability.

4.2 Comparison of Harmful Information Download Rate

In order to verify the harmful information download rate of RDSTAM under different proportions of malicious nodes, several groups of experiments were set up in this paper. Similarly, with a total of 100 nodes in the experiment, the proportion of malicious nodes increased from 0% to 50%. Each experiment interacts for 10000 times, and the probability of interaction request response is 100%. The other two sets of comparative experiments are RASTM proposed by Lu [13] and PeerTrust [14] that improved on the basis of EigenRep model. In the case of different proportions of malicious nodes, the comparison of harmful information download rate of the three models is shown in Fig.2:

According to the experimental results, the harmful information download rate of RDSTAM is lower than that of RASTM and PeerTrust model, and when the proportion of malicious nodes increases, the performance gap becomes more and more obvious. Even if the proportion of malicious nodes reaches 50%, the harmful information download rate of RDSTAM is still lower than 10%. It proves that RDSTAM can resist the attack of malicious nodes and reduce the propagation of harmful information.
5. Conclusion
This paper proposes a trust assessment model based on recommendation and dynamic self-adaptive in cloud service. It’s up to nodes to judge the trust degree of other nodes, and the nodes interact with each other to realize cloud services.

Firstly, this model divides trust into direct trust and indirect trust. Direct trust is obtained according to historical interaction records, indirect trust is obtained according to the third-party nodes. Secondly, we proposed a recommendation mechanism, invited the third-party nodes to recommend. Recommendation nodes are responsible for their recommendation, and receive reward and punishment measures according to the evaluation to update the trust values automatically.

In order to verify the effectiveness of this model, a simulation experiment was carried out, and the experimental results showed that this model has higher interactive success rate and lower harmful information download rate than other methods. It proves that this model can accurately evaluate the trust value of nodes, improve the dynamic self-adaptability to better meet the dynamic trust update requirements of cloud services, and effectively resist malicious behaviors.

In addition, malicious nodes have more complex attack methods. In future study, we will continue to analyze more complex malicious attack behaviors and research corresponding strategies to deal with these attacks.

References
[1] Yang ZJ, Zhu SW, and Xue BB, “A Bibliometric Analysis of Cloud Computing Technology Research,” IEEE Electronic and Automation Control Conference, 2018, pp. 2353-2358.
[2] Liu JW and Zhao PC, “Secure cloud computing architecture on mobile internet,” International Conference on Artificial Intelligence, 2011, pp. 619-622.
[3] Anupam Das, “SecuredTrust: A dynamic trust computation model for secured communication in multiagent systems,” IEEE Transactions on Dependable and Secure Computing, 2012, pp. 261-274.
[4] Liang ZQ and Shi WS, “PET: A PErsonalized Trust model with reputation and risk evaluation for P2P resource sharing,” IEEE Conference, 2005, pp. 201-210.
[5] Marudhadevi D, Dhatchayani V N, and Sriram V S S, “A trust evaluation model for cloud computing using service level agreement,” The Computer Journal, 2014, pp. 2225-2232.
[6] Li W, PING L, and LI J, “Cloud service discovery algorithm based on trust fuzzy comprehensive evaluation,” ICIC express letters, An international journal of research and surveys, Part B, Applications, 2012, pp. 331-336.
[7] Li X, Liang H, and Zhang X, “Trust Based Service Selection in Cloud Computing Environment,” International Journal of Smart Home, 2016, pp. 39-50.
[8] Wang YB, Wen JJ, and Wei Z, “A Novel Dynamic Cloud Service Trust Evaluation Model in Cloud Computing,” IEEE International Conference, 2018, pp. 10-15.
[9] Wang L and Wu Z, “A Trustworthiness Evaluation Framework in Cloud Computing for Service Selection,” Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on. IEEE, 2014, pp. 101-106.
[10] Yao LY and Xie Q L, “Use Trust Assessment to Select Service Node in Cloud,” Journal of Computers, 2017, pp. 57-68.
[11] Xie XL, Liu L, and Zhao P, “Trust Model Based on Double Incentive and Deception Detection for Cloud Computing,” Journal of Electronics & Information Technology, 2012, pp.812-817.
[12] Kamvar S D, Schlosser M T, and Garcia-Molina H, “The EigenTrust Algorithm for Reputation Management in,” 2003.
[13] Lu F, Zheng KF, Niu XX, and Yang YX, “Construct a Risk-Aware Peer-to-Peer Security Trust Model,” Journal of Beijing University of Posts and Telecommunications, 2010, pp. 33-37.
[14] Xiong L and Liu L, “PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities,” IEEE Transactions on Knowledge & Data Engineering, 2004, pp. 843-857.