Journal of Computers Vol. 28, No. 1, 2017, pp. 57-68
doi:10.3966/199115592017022801005

Use Trust Assessment to Select Service Node in Cloud

Lei-Yue Yao[1*], Qiang-Lai Xie[1]

Department of Information Engineering, Jiangxi University of Technology,
Nanchang, Jiangxi, China
special8212@sohu.com, xjy9@21cn.com

Received 15 June 2015; Revised 9 July 2015; Accepted 1 September 2015

Abstract. The interaction between nodes to achieve service in Cloud computing is allowed. In the complex and dynamic network environment, access control and security communications are the main ways to protect the security. It provides a trust dynamic level access control method by simulating social trust, which can help users select a trustworthy node in internet. The comprehensive trust model is composed of direct trust and indirect trust. The direct trust value is deduced from user's satisfaction with interaction, amount of interactions, time decay, and punishment factor. The indirect trust is computed by direct trust in other nodes for the feature of trust transference. The trust dynamic access method will help users to select more secure service and provide reliable candidate nodes. The experiments show that trust mechanism can improve the credibility of the system in a certain extent and reduce deception task execution. The method can improve the efficiency of interaction, and is suitable for cloud computing environments.

Keywords: access control, cloud computing, trusted access control, trust evaluation

1 Introduction

Cloud computing is another name for Internet computing nowadays. National Institute of Standards and Technology (NIST) defined Cloud computing is shared pool where people can enjoy the lower operating costs, improved operational efficiency and get various conveniences [1]. There are various services in cloud computing, and users can achieve the on-demand resources and services over internet by only some clicks. They have no need to know where the services are hosted. Moreover, the cloud computing will become a common service like water, electricity and other public resources [2]. The cloud computing is lack of centralized authentication center to guarantee the reliability of the recommended information service, so it also face severe information security challenges. One important problem is that the massive important user data in cloud systems have a greater temptation to an attacker. The interface provides with users in the cloud enables cloud users can directly use and operate the cloud service provider of software, operating systems, and even programming environment and network infrastructure. It is obvious that the destruction of cloud resources is much more serious than the current use of the Internet for the resource sharing [3]. The another problem is that users always worry about resource sharing, The cloud computing has unlimited resources, but users do not know that these resources are credible; it almost has the service in everywhere, but users do not know that these services are credible; it has unlimited storage space, but users can not perceive the existence of their own data stored in where, cannot control data. So cloud services easy for users to generate mistrust [4-5]. Therefore, under the cloud computing environment, the open operating environment faces some significant security challenges. The reasons for the security risks in cloud computing can be divided into two categories, one is from outside of cloud system, such as: 1) the data are intercepted in the delivery process; 2) The content of information is polluted or deleted by malicious tampering; 3) Some malicious nodes are masquerading as legitimate users or ISP. These problems need security communication technology, just like Information encryption, digital certificates. The other is from the inside of system, which is generated by the service node itself. Usually including some dishonest behavior, such as 1) Malicious nodes provide false services; 2) Some selfish nodes are just

* Corresponding Author

going to consume system resources, but do not provide the resources to the system; 3) Unreliable nodes may even result in a failure to work together [6]. As cloud computing platform integrates mass information systems and services users, having different and dynamic security management and secure borders, and based on privacy and other reasons, we cannot monitor all the details of service node entity, these conventional user access control method cannot meet the charge of cloud computing environments [7]. Currently authentication technology is relatively mature, but that does not can stop identity authentication fails or legal status of malicious destruction of end users of the system [8]. The traditional network security technology can't constraints on node behavior. People rely on trust to do some interaction in real life. Many researches also proved that the best way to deal with the behavior of the dishonest node is simulating the trust mechanism in the human social relations [7, 8]. In recent years, many researchers use trust management thinking, combined with relevant technical methods of trusted Network and trust cloud. It is desirable to establish a trust relationship between users and cloud services to address service security cloud environment [9-12]. So the analysis of cloud user behavior for effective control of cloud applications is an important research work of cloud computing in current.

In the work, a method to select a service node in cloud based on trust is provided. The rest of the paper is organized as follows. Section 2 is a review of the related works on trust model and its effect on cloud. In this section, a comparison of other studies was concluded. Section 3 describes a trusted access control scenario in application, and the detail diagram of the policy that based on dynamic trust is also being given. Section 4 constructs the trust evaluation model based on direct and indirect interactions. In this section, the trust model takes the quality of service and time decay into account. In section 5, we take the experiments to support the model, and the results reveal a good effect of policy. Finally in section 6, we make a conclusion of the paper and point out the significance of dynamical trust research in cloud. The main contribution of this paper is that it proposed a dynamic, comprehensive trust model to evaluate the service node. The trust model simulated direct and transitive indirect trust in social network communication, and considering the trust decay with time, punitive action on trust. It can reduce the possibility to interact with malicious nodes, and provide a better mechanism to select service in cloud.

2 Related Work

Currently, Internet provides two ways to protect the security mechanisms: access control and secure communications [1]. Access control is essential to high-performance computing in a very important component for cloud environments. Almost all cloud computing applications need to interact with a strategy to implement security between nodes. So a new generation of cloud-based network is faced with the safe, effective and properly implemented interaction problems between nodes [3].

The protocols including efficient subsequent login authentication, data confidentiality, user privacy protection, and non-repudiation are important in communication services. Hwang proposed that the important login authentication is also provided to enhance the user identity privacy protection, and register are always based on trust [8]. In this context of central servers, Ryan believes consumers are aware that "trust" problem is very important in the cloud environment. But users of cloud computing should recast their view of trust in a similar way of consumers' perceptions of trust to banking or others [9]. Sun analyzed the high security requirements in high open cloud computing, and highlights the privacy and trust in cloud computing environments currently. It can help users recognize the tangible and intangible threats associated with their use, quantifiable research the importance of assessment methods [10]. Bose considered that it is not easy to build trust for any new technology, such as trust in cloud computing. It is gradually established over time based on the good reputation of performance and security vendors and has won the trust of users [7]. Abbadi believed that the establishment of cloud trust model is important, although the complexity and dynamic nature of cloud infrastructure makes it difficult to solve. He proposed a trust framework for IaaS cloud type and cloud user [11]. 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 DS evidence theory is calculated based on the interaction of recommended trust through transitive trust fusion [12]. Yuan believed that credible behavior of user is the core in reliable network research [13]. He proposed a trust dynamic level scheduling (TDLS) algorithm to meet users' requirements which are an assessment, prediction and control architecture for user behavior in trust network. It is realized through sociology relationships by establishing a relation among users, uncertainty resources and services. Dai proposed to construct a trusted Cloud Platform to remove high cost, low efficiency and less

content in knowledge management. The trust method can effectively improve the efficiency, reduce the cost and enhance the content value of service in cloud. The trusted computing can ensure the confidentiality and integrity of cloud service [14]. Kokash researched a recommendation system which based on the history of user-system interactions and client-service communications logs. The service discovery method based on the user's experience and web service Qos, which indicated the experience can be used as evidence of trust. [15]. Zhao proposed Bayesian network based on user behavior to predict trust and control algorithms, then established quantifiable evidence of trust and the corresponding level of trust [16]. It used Bayesian network for users to predict the future behavior of the trust like Tian's research. But neither of them takes the user's historical behavior and time decay into account the evaluation [17]. Wu proposed service reliability factors, including QoS credibility and results of the implementation of the service user satisfaction. Through the evaluation of the quantized values corresponding services by user's feedback, the trust of the evaluation system services is based on satisfied rate on QoS [18]. Du proposed a section model based on trustworthiness and personality preference in order to select a trusted service under the cloud computing environment. The service will satisfy the personality preference according to hierarchical trust management architecture; and the model also has certain resilience to fraud [19]. Naseer proposed a model to help the users in finding out the efficient and trustworthy service provider in cloud on the basis of data taken from regulatory authorities, performance of provider in last one year and feedbacks taken from the other users. Also the Qos is kept in consideration during the development of this trust model [20].

The related researches have supported that trust is important to cloud, and revealed what trust can help select credible server nodes, and improve efficiency of interaction. Compared with existing studies, the model in this work combine direct and indirect trust to compute trust value, which is more accurate than the single trust way. Others often based on transitive or real-time behavior, and have signal evidence. They didn't fully consider interaction reputation in history, and have no dynamic evolution of trust mechanism. In this work, we add time decay to reflect the dynamic feature, and use quality of service, the amount of interactions, feedback of satisfaction as the main factors of trust, the combining method can improve the objectivity and effectiveness for assessment of credibility of node. The experiments show that it can also improve success rate of service interactions and reduce the possibility to interact with malicious nodes.

3 Trusted Access Control Policy

3.1 Trusted Access Scenario

The Cloud computing network is composed of many randomness nodes. The result of the execution may have very big difference in the different execution conditions. The paper use file-sharing system as an example for a convenient description. A service request node downloads files from the response node (hereinafter referred to as the process of interaction between nodes). The results fall into two categories including: S (success, file download is successful), F (false, file download is failed). Three responding nodes A, B, and C provide 500 MB packet available for download, supposed that perform to download tasks from node A takes 5 minutes, but it has Trojans in the packet. If performs the same tasks from the node B, file download takes about 30 minutes, but it has good quality. If download the same packet from node C, it has a good quality and only need only 5 minutes. Completed the same download task, but the result was not the same. The various satisfactions will generate various sense of trust to the nodes.

Yin constructed Multidimensional Dynamic Trust Measurement Model in a social network by using direct trust and recommend trust [21]. In general, trust relationship cannot transitive fully. That is, under the circumstance that A trusts B and B trusts C, however, A does not always trust C (see Fig. 1). In real life, if A deeply trusts B, and B deeply trusts C, to some extent, A would trust C. So in this paper, the trust model is composed of direct and indirect trust referring to interpersonal trust of sociology shown in Fig. 2.

The trust can be quantified by using the historical trust and reputation of the current by users, and through the refinement of quantitative trust to control the access to resources in network environment. The quality of service (QoS) can be used to compute trust for it reflects the quality and time to complete the task and build a trust relationship in the cloud computing environment.

The user will produce trust by the Qos in history interaction behavior. Then a dynamic level access control method is proposed to the trust is dynamically with time (see Fig. 3).

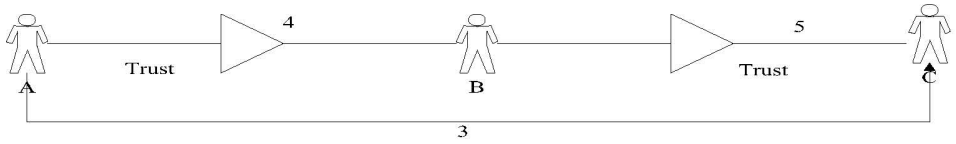

Fig. 1. Trust transfer

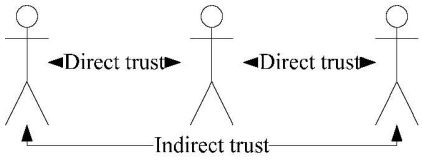

Fig. 2. Trust relationship

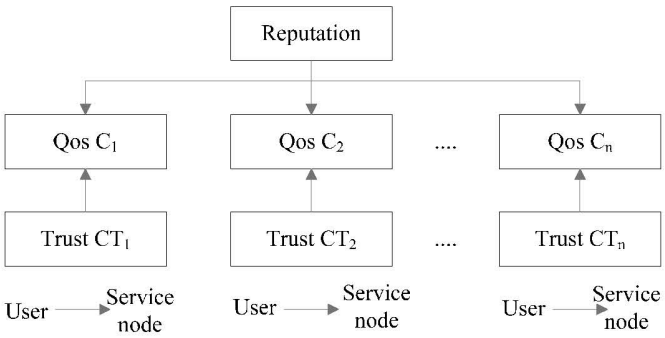

Fig. 3. Relationship of reputation, Qos and trust

3.2 Dynamic Trust level Access Control Method

Cloud computing environment is an open platform that allows interaction between the nodes. When a node applies to resources from service providers, it will select a credible node to interact. The specific access control method is shown in Fig. 4. For the resources requester will use a first-come, first-served method. The providers of resources are stored in a candidate queue in the paper.

When started, the system will search service nodes based on user's request. All the service nodes will enter the candidate list. System will deal with node list. If the list is empty, the reply is no service can be provided to user, and finish. Otherwise, the node will enter into the trust evaluation period. If the node has no any evidence on trust or it is the unique node is list, the system will give the suggestion rules to users. Users can decide whether to interact with the node according to their needs. The suggestion rules are described in 3.3. If there is direct interaction between nodes, the direct trust value will be computed by user nodes. If there is no direct interaction, it will access to indirect trust judgment. And if there is also has indirect interaction, the indirect trust value will be computed too. Then a comprehensive trust will be computed by direct and indirect trust value. If only has indirect interaction or has direct interaction, the indirect or direct trust value may instead as comprehensive trust. If the trust value of the candidate node is greater than the threshold value, and it is the biggest trust value, the interacting will start. Otherwise the system will point to the next node, and judged the trust of the node in the way again. If the system has evaluated all the nodes and hasn't found the qualified node, the nodes will be provided to users ordered by trust value, or provided the candidate node. Users can give their decision according to the suggestion rules provided by system. The Interaction among nodes is so effectively can ensure the response to all service requestors is able to get the service to improve the chances of a successful mission execution.

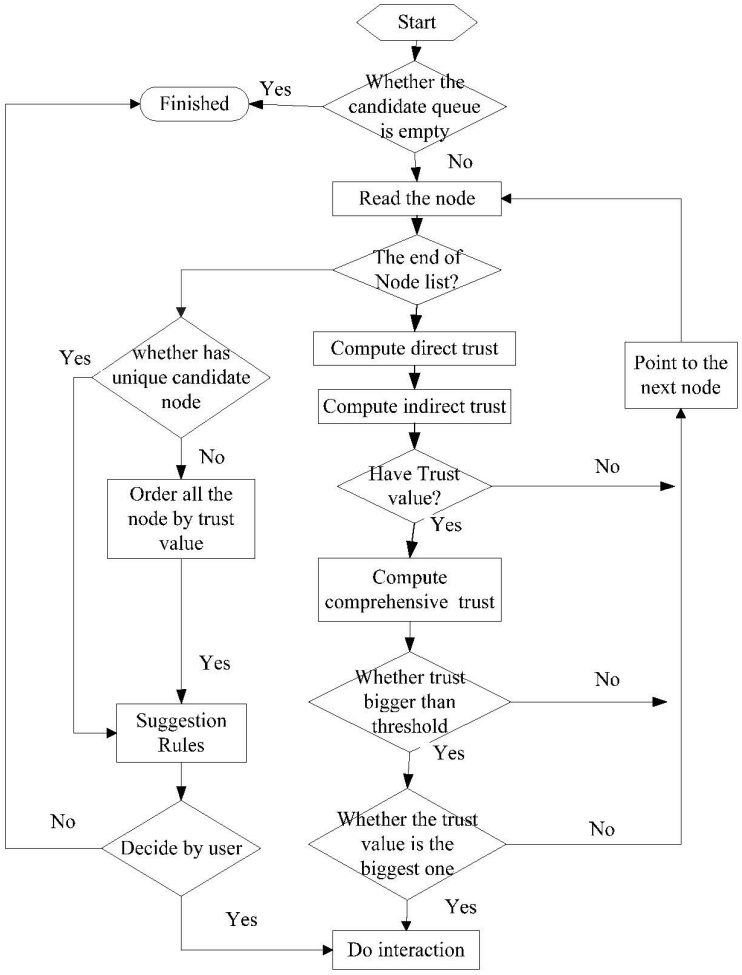

Fig. 4. Dynamic trust access mechanism

3.3 Suggestion Rules on Interaction According to Risk

Trust is a priori information for the user to select service nodes, the Qos feedback and evaluation belong to posteriori information. In trust-based access control, measurement results directly affect the interaction and service selection. In general speaking, an information game theory is existed in a trust access control model as Fig. 5. User will select the service node in cloud according to the comprehensive trust and risk of service itself. If the trust of node is above the threshold value, the system will give service selection suggestion according to the service risk rules as Table 1.

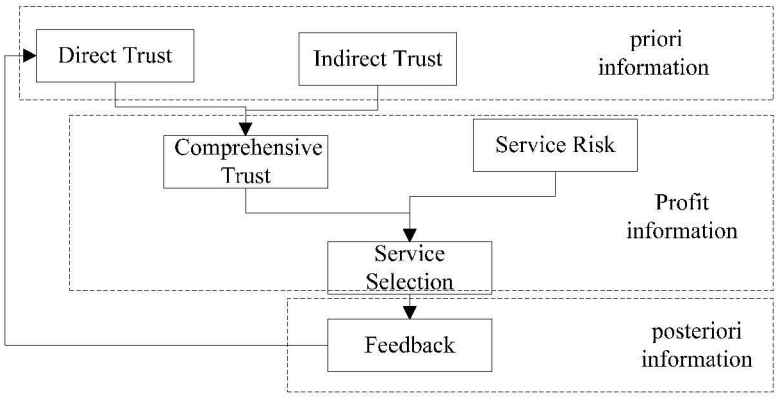

Fig. 5. Gambling information in service selection

Table 1. Risk rules of trust

Trust Level	Explanation	Range	High Risk	Medium Risk	Low Risk	No Risk
1	Very untrust	[0,0.05)				
2	No trust	[0.05,0.25)				✓
3	Basic trust	[0.25,06)			✓	✓
4	Medium trust	[0.6,0.8)		✓	✓	✓
5	Most trust	[0.8-1]	✓	✓	✓	✓

The situation of risk is according the service features, as a description listed in Table 2. For example the trust level G={1,2,3,4,5}, the trust value is divided into following {0.05,0.25,0.6,0.8}. the rang of trust value is corresponding to trust level, and the relation rules between service risk and trust level is in Tab.1. Most of the server nodes are medium and basic trust in the practical interaction, and very untrust and most trust is only small number. If the node has basic trust, it means the system will recommend the low risk or no risk service to the users, and give warning to users when they choose these services.

Table 2. Risk rules of trust

Risk Level	Situation
High Risk	Execute service, get user information automatically, store important information
Medium Risk	store some information is not important
Low Risk	Download some information will not automatically run
No Risk	Only browsing the information on server.

4 Trust Model

4.1 Concept Definition

Referring to the sociology interpersonal trust model, the paper proposed direct trust, indirect trust and comprehensive trust model. All the concept of trust is explained below.

Trust: it is used to quantify the level of trust between nodes. The value of it can be defined in {0,1}, 0 means the node *a* distrust node *b*; while 1 means the node *a* trust node *b* completely. The trust value of each node all considering direct trust and indirectly interact with the node in a period of time.

Quality of Service Qos (a, b): the service requester *a* made an evaluation of the resources on resource provider *b* according to the situation of their own resources obtained after an interaction.

Direct trust DT: nodes can make judgments on possible future behavior of the target nodes based on its own historical experience and observation. The direct trust is to establish the appropriate relationship to trust by summing up past experience of direct interaction.

Indirect trust IDT: node to evaluate the destination node through interaction with other nodes. The way to establish trust relationship with the others is also called recommendation trust.

Comprehensive Trust CT: If both the direct and indirect interaction existed between nodes, it should to choose to calculate their comprehensive trust value.

4.2 Direct Trust

Direct trust value primarily through the historical experience of direct trade between the nodes to obtain, which is on behalf of the local node *a* to node *b*'s views. This information is available to calculate the direct trust value of node *a* deal with the use of node *b*, the direct trust of node *a* to node *b* is:

$$DT(a,b) = P \cdot \frac{1}{k} \sum_{i=1}^{k} Qos_i(a,b) \quad \textbf{(1)}$$

DT(a,b): The direct trust of node a on node b; P is punishment factor; $Qos_i(a,b)$: The degree of satisfaction of node a on node b in transaction *i ; k:* The number of times of successful transaction.

Method to Compute Qos. Taking into account in the difficult to quantify the quality of service, we measure the quality of service from the download time *Qt* and file quality *Qf* two ways in the context of this paper. For the time and the quality of the documents specified as an enumeration value as a measure

of service standards: {satisfied, basically satisfied, very satisfied}, the specific term of each enumeration value takes the following quantified values {0, 0.5, 1}.

$$Qos(a,b) = \alpha \cdot Qt + \beta \cdot Qf \tag{2}$$

The results of interactive service fall into two categories according to the file download: S (Success, File downloaded successfully), F (False, file download failed). The unsuccessful connection system is set to 0 as the quality of service feedback.

Method to Compute Punishment Factor P. If some malicious node appeared in cloud computing environment, it must take some punishment on its trust value. A punishment factor P is added to compute direct trust. P is defined as $P= (1/2)^n$, and n is the number of times of malicious behavior. So trust value will fall by each fraud behavior of the node. The trust value of a node increases slowly, but reduces faster. Thus the service node will cherish every interaction, and reduce failing rate in interactions.

4.3 Indirect Trust

Indirect trust is used in the case of node *a* and node *b* has not been traded ever. For example, the node *a* intends to carry out the transaction with *b*, the node *a* do not know the situation of node *b*'s trust. But the node *a* transacted with node *c*, and node *c* conducted transactions with node *b*, sociology interpersonal trust model can be used to analog indirect trust.

$$IDT(a,b) = \sum_{j=1}^{n} (Dw_j \cdot \frac{1}{k_j} \sum_{i=1}^{k_j} Qos_i(c,b)) \tag{3}$$

IDT(a,b): The indirect trust of node a on node *b; n:* Behavior to judge *b* is divide *n* time period; Dw_j*:* Weight value of *j* time period; $Qos_i(c,b)$*:* The satisfaction degree of recommendation node *c* on *b.*

Method to Compute Time Decay *Dw*: Due to the different contribution for consideration trusted node from different time periods, is should be set different weights to different time period. For example, the transaction data are one year ago and transaction data over are ten days ago, it is obviously that the period of ten days has large effect to evaluate trust. The inspection time period is divided into four time segments, i.e., n = 4, different time weight is expressed as follow (Fig. 6).

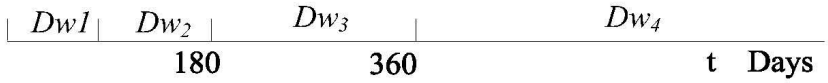

Fig. 6. Time decay period

Different weight function for each time period is as follow:

$$Dw(t) = \begin{cases} 0.4 & ,t < 90 \\ 0.3 & 90 \le t < 180 \\ 0.2 & 180 \le t < 360 \\ 0.1 & 360 \le t \end{cases} \tag{4}$$

Due to the different importance of different intermediate nodes for computing trust value, if the node with high direct trust value, it will bring a high credibility of recommendation, which must give bigger trust weight value.

4.4 Comprehensive Trust Model

The target node trust evaluation is according to a feature of the social network of interpersonal interaction. If there are multiple direct interaction experience (especially recently) between the source node and the destination node, it is easy to establish a relationship of trust with the target node. But in fact, there are often two kinds of situations. Firstly, the nodes are large in a cloud environment network, the possibility of repeated interaction between nodes is low, or the time between their interactions are too long. So that the source node will have no confidence in the trust when assessing the target node, they hope to get more evidence. Secondly, the source node needs to interact with an unfamiliar destination node, and there

is no historical experience of interaction to be investigated. So the trust from tripartite recommendation is particularly important. Thus, how to obtain reliable recommended trust is very important in the cloud computing network.

When there is a direct and indirect interaction between both nodes, we choose their comprehensive trust to calculate trust value. Here, set up direct trust and indirect trust weighting factor for the W1 and W2. When there are direct trust and indirect trust, the value of W_1 bigger than W_2, as shown in the follow: $W_1 > W_2$, and $W_1 + W_2 = 1$.

So the direct trust and recommended trust in some way to obtain a final comprehensive trust of the node as (5), the trust function is defined as:

$$CT = \begin{cases} IT; DT = 0, IDT = 0 \\ DT; DT \neq 0, IDT = 0 \\ IDT, DT = 0, IDT \neq 0 \\ W_1 \cdot DT + W_2 \cdot IDT; DT \neq 0, IDT \neq 0 \end{cases} . \quad \textbf{(5)}$$

5 Experiment

5.1 Calculated Examples

Example: The nodes Pa and Pb are service node in cloud, the nodes A, B, and C are the users in cloud. The feedback of each user on the nodes is as Table 3, each feedback includes the mark of Time and Quality.

Table 3. Feedback of each user

Node	*A (<90 days)*	*A (90-180 days)*	*B(<90 days)*	*B(90-180 days)*
Pa	(0.7,0.9)	(0.8,1)	(0.9,0.6)	(0.8,1)
Pb	(0.9,0.9)	(0.9,1)	(0.9,0.7)	(0.9,1)

Assuming the interaction between each node will only under the condition that trust value is greater than a threshold value *Tm*. The other parameters are set in Table 4.

Table 4. Value of other Parameters

Parameters	W_1	W_2	α	β	*Tm*
Values	0.7	0.3	0.4	0.6	0.5

Step 1: Compute Qos of Pa and Pb as Table 4, e.g. Qos(Pa, A)=0.4*0.7+0.6*0.9=0.82

Step 2: Compute DT, e.g., a user interact with Pa two times, and DT(Pa,A)=(0.82+0.92)/2=0.87.

Table 5. Compute the Qos value and CT by Feedback

Node	*A*	*A*	*B*	*B*	*DT-A*	*DT -B*
Pa	0.82	0.92	0.72	0.92	0.87	0.82
Pb	0.9	0.96	0.78	0.96	0.93	0.87

Step 3: Compute IDT, e.g., the weight of time period when below 90 days is 0.4, and between 90 and 180 days is 0.3. So IDT(Pa, A)=0.4*0.72+0.3*0.92=0.564, as displayed in Table 6.

Step 4: Compute CT, e.g., CT(Pa, A)=0.7*0.87+0.3*0.564=0.778.

Table 6. Compute the Qos value by Feedback

Node	*IDT-A*	*IDT-B*	*CT-A*	*CT-B*
Pa	0. 564	0.604	0.778	0.755
Pb	0.6	0.648	0.831	0.803

5.2 Experiment Simulation

Experimental simulation environment is under the context of ADM1.6 GHz, 1 GB, and simulation is based on MyEclipse 6.0. Experimental evaluation criteria used the interactively success rate (Ratio of Successful Transaction, RST). It is the proportion of successful interaction while system satisfaction is greater than 0.8. In the experiment, the total number of nodes is 100. Malicious nodes provide connectivity services with 50 percent probability; while providing connectivity services with 50 percent probability too, but the satisfaction degree is less than 0.5 with the same probability. Truthful nodes provide connectivity services, and service satisfaction on time and file quality distributed between 0.9 and 1. The initial trust value of each node is 0.6.

Each node has simulated 50 times interactions. The relationship between the proportion of malicious nodes and interaction success rate under direct trust, indirect trust and comprehensive trust model are tested. Simulation results are shown in Fig. 7, Fig. 8, and Fig. 9.

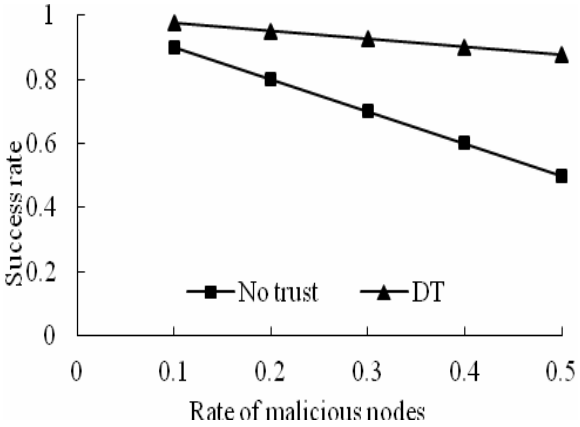

Fig. 7. Comparisons between IDT and no trust mechanism

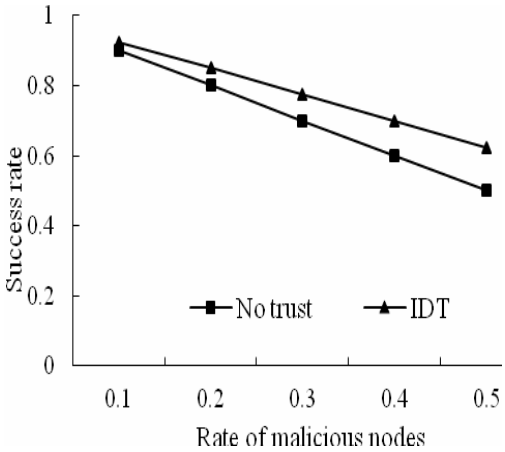

Fig. 8. Comparisons between DT and no trust mechanism

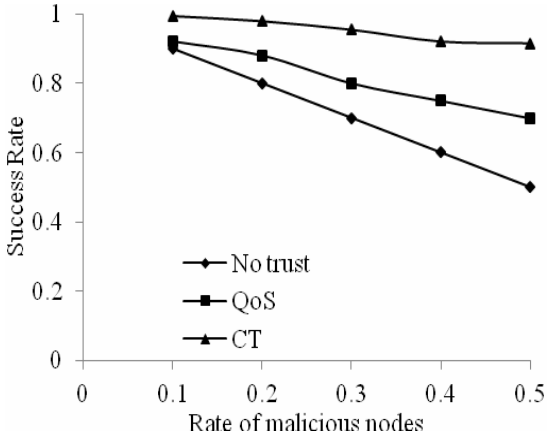

Fig. 9. Comprehensive comparison among three methods

From the three results, it is obviously that it will access to a higher success rate when a smaller proportion of malicious nodes, that is to say interaction has low risk if nodes are truthful. But if don't adopt trust as a trading controlling indicator, the interaction success rate decreased rapidly when the proportion of malicious nodes increases, and the simulation results are shown in Fig. 7, and Fig. 8. For direct trust model, the trust value is determined by calculating the success rate in the process of historical interaction of nodes to perform the mission. If the nodes with non-interactive experience, they can't get trust information. So they may interact with malicious nodes, and led to the failure interactions, then reduce success rate. But the node will select candidate nodes according to their history when considering interact in direct trust model. If a node's mission success rate is not high, it will be excluded from the candidate by the request node. It will have some effect on the stability of the system. As shown in Fig. 7, the direct trust is largely effective in reducing the failure rate of the task.

The indirect trust simulation result is shown in Fig. 8. Since a node may not have directly trust, then the evidence of trust can only find from other nodes. The provided recommended evidence of node to another is incomplete, inaccurate, and not completely reliable. Therefore, system reliability is relatively unstable in the case of not considering trust. The probability of failure will be increased when executing the task. However, considering the value of the feedback and task performance in the history of recorded interactions from other recommending node, the indirect trust will be used to judge the provider's trust instead. The indirect trust can improve successful ratio of interaction, meanwhile improve system reliability.

The comparison among comprehensive trust model, Qos depended method and no trust method, simulation result of interaction success rate is shown in Fig. 9. The experiment shows that the comprehensive trust model effectively reduces the failure rate of the tasks performed. It is in fact that in real social activities, interpersonal trust relationships can greatly improve the success rate of interaction, and ensure security. In the internet environment, comprehensive trust formation mechanism takes consideration of the direct trust and indirect trust. On the one hand, the model recorded the transaction behavior of nodes in history; on the other hand, it provides an important basis to protect the stranger node transaction. The comprehensive trust considers the credibility of the nodes directly interact with the node, and then consider the indirect interaction node. Comparing to the Qos model, it takes more evidence to compute trust, and consider the weight of direct evidence and recommend evidence, so it can improve the efficiency of interaction, and reduce the proportion of the task execution failure.

As the Fig. 10, if you do not use the trust model to assess the credibility state of the server node, the error of service node in cloud platform between default value and its real value of credibility will increases with an increasing proportion of malicious nodes. The method adopted the CT trust model is more objective. Although there will also some change due to a certain probability, it doesn't increase with malice proportion. So using a trust assessment of the credibility allows users to more objective understanding of the service node status, and makes a reasonable choice of the service node.

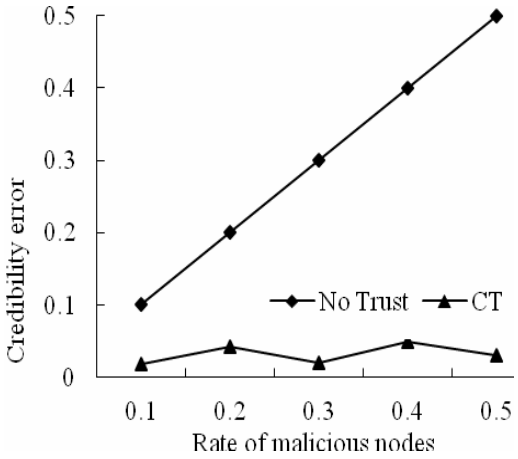

Fig. 10. Credibility error between DT and no trust mechanism

6 Conclusion

Since the interaction among nodes only occurred in the Internet in the cloud computing environment, the reliability of node will determine the reliability of the system. The research can improve overall system reliability through the trust accessing control. Trust model refers to the user satisfaction on the quality of service and the execution time of the task. It uses transitive trust to reduce the lack of trust bring by no direct experience between the nodes. Divide the indirect trust into different time window for the trust time decay effect, and set various trust weights for each time period can effectively mitigate the effects of one transaction on the overall trust value. It enables service providers to cherish every opportunity to perform a task, for it can effectively prevent malicious nodes on the overall affect the value of the trust, and reduces the proportion of inter-node task fails. In order to achieve better application, the further work will concentrated on computational efficiency, trust started. The first 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. The second is how to define the initial trust value to solve start-up trust. Some authentication mechanism may adopt to solve start-up trust, and a trust transfer network can be established to recommend service node in cloud when lack of trust on interaction.

Acknowledgement

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] S. Sharma, G. Gupta, P.R. Laxmi, A survey on cloud security issues and techniques, International Journal on Computational Sciences & Applications (IJCSA) 4(1)(2014) 125-132.

[2] Y.Y. Chen, J.C. Lu, J.K. Jan, A novel design of authentication-as-a-services (AaaS) architecture in cloud computing, Journal of Computers (Taiwan) 24(3)(2013) 19-47.

[3] C.M. Rong, S.T. Nguyen, M.G. Jaatun, Beyond lightning: a survey on security challenges in cloud computing, Computers and Electrical Engineering 39(1)(2013) 47-54.

[4] B.R. Kandukuri, P.V. Ramakrishna, A. Rakshit, Cloud security issues, in: Proc. of 2013 IEEE International Conference on Services Computing, 2013.

[5] S. Pearson, A. Benameur, Privacy, security and trust issues arising from cloud computing, in: Proc. of 2010 IEEE Second

International Conference on Cloud Computing Technology and Science (CloudCom), 2010.

[6] H. Sato, A. Kanai, S. Tanimoto, A cloud trust model in a security aware cloud, in: Proc. of 2010 10th Annual International Symposium on Applications and the Internet, 2010.

[7] R. Bose, X. Luo, Y. Liu, The roles of security and trust: comparing cloud computing and banking, Procedia Social and Behavioral Sciences 73(2013) 30-34.

[8] S.J. Hwang, C.H. You, An unlinkable delegation-based authentication protocol with users' non-repudiation for portable communication systems, Journal of Computers (Taiwan) 25(1)(2014) 35-47.

[9] P. Ryan, S. Falvey, Trust in the clouds, Computer Law and Security Review 28(5)(2012) 513-521.

[10] D. W. Sun, et al. Surveying and analyzing security, privacy and trust issues in cloud computing environments, Procedia Engineering 15(2011) 2852-2856.

[11] I.M. Abbadi, M. Alawneh, A framework for establishing trust in the cloud, in: Proc. of Computer and Electrical Engineering, 2012.

[12] J.B. Wu, G. Lü, Trust and reputation evaluation for web services based on user experience, Journal of Computer Applications 29(8)(2009) 2291-2293.

[13] L.L. Yuan, G.S. Zeng, L.L. Jiang, C.J. Jiang, Dynamic level scheduling based on trust model in grid computing, Chinese Journal of Computers 29(7)(2006) 1217-1224.

[14] J. Dai, L. Zhang, Trusted cloud platform oriented to knowledge management, Journal of Computational Information Systems 9(12)(2013) 4997-5004.

[15] N. Kokash, A. Birukou, V. D'Andrea, Web service discovery based on past user experience, in: Proc. of Business Information Systems, 2007.

[16] J. Zhao, N.F. Xiao, J.R. Zhong, Behavior trust control based on Bayesian networks and user behavior log mining, Journal of South China University of Technology (Natural Science Edition) 37(5)(2009) 94-100. [in Chinese]

[17] L. Q. Tian, C. Lin, A kind of game-theoretic control mechanism of user behavior trust based on prediction in trustworthy network, Chinese Journal of Computers 30(11)(2007) 1930-1938. [in Chinese]

[18] X. N. Wu, et al. A trust evaluation model for cloud computing, Procedia Computer Science 17(2013) 1170-1177.

[19] R. Z. Du, J.F. Tian, H.G. Zhang, Cloud service selection model based on trust and personality preferences, Journal of Zhejiang University 47(2013) 53-61. [in Chinese]

[20] M.K. Naseer, S. Jabbar, I. Zafar, A novel trust model for selection of cloud service provider, in: Proc. of 2014 World Symposium on Computer Applications & Research (WSCAR), 2014.

[21] G. Yin, J. Zhang, D. Gao, Multidimensional dynamic trust measurement model for social network, Journal of Computational Information Systems 9(18)(2013) 7427-7434.