Journal of Computers Vol. 30 No. 1, 2019, pp. 142-152
doi:10.3966/199115992019023001014

A Dynamic Level Interaction Method Based on Trusted Value

Yong-sheng Zhang[1], Yue-qin Fan[1*], Ran-ran Cui[1], Yu Wei[1]

[1] Department of Information Science and Engineering, Shandong Normal University
Shandong Provincial Key Laboratory for Novel Distributed Computer Software Technology, Jinan, China
1372195518@qq.com

Received 23 July 2017; Revised 07 November 2017; Accepted 9 January 2018

Abstract. With the rapid development of the cloud computing, there is a large amount of service providers with low quality in the marketplace. The mendacious service providers cause a serious loss for the users. In order to select an efficient cloud service, it can be trust and meet the user's privacy protection requirements. In this paper, a dynamic level interaction method based on credible value is indicated. The cloud service providers and cloud users are divided into different dynamic levels according to their historical records. The security level of privacy data is decided according to the users' trust level. This model introduces the center degree factor to filter the mendacious service and it can get a more accurate service evaluation by limiting the malicious users to make false evaluation for the service and it can control the providers' access rights to protect the users' information. The results of simulation experiment show that this model can improve the interaction successful rate and strengthen the safety of user privacy data. It demonstrates the efficiency and effectiveness of our approach in trusted interaction with other counterparts.

Keywords: grading thought, privacy data, trusted cloud computing, trusted value

1 introduction

With the development of the internet technology, more and more web services have been deployed by many enterprises. It can provide convenient services for the users. However, it brought many safety problems, such as the service enterprises provide bad service to the user; the user give the service provider false evaluation to affect the providers' trusted value and so on [1-2]. How to establish a credible relationship between service providers and users becomes a hot topic in the field of information security.

The users' malicious evaluation will make negative effect for the services' trusted value. Filtering out malicious evaluations can ensure the trusted value accuracy. According to these discoveries, the problems will be solved summarized as follows:

(1) In the process of interaction, this model can help users find the safe and reliable cloud service providers quickly.

(2) The information submitted to the service provider is safety.

(3) The trusted value is one of the key indicators to the classification for the users and service providers.

The process of classification is introduced in this paper. This model can filter the illegal evaluation effectively, and control the service providers' authority. It also can ensure the safety of user privacy information.

The rest of this paper is organized as follows. In Section 2, we give the related work. Section 3 introduces the process of dividing levels for the service providers and users. Section 4 presents the algorithm of the trust interactive. Section 5 introduces experiment and analysis the related experimental

* Corresponding Author

results to investigate the effectiveness of our approach. Section 6 concludes this paper.

2 Related Work

The trusted interaction model is a fundamental and complex problem in the field of service oriented computing, which has been approached from many different perspectives. Trust model has applications in many fields. For example, [3] presents a comprehensive and adaptive trust model oriented large-scale P2P (Peer to Peer). It adds the confidence factor and feedback factor to overcome the deficiencies of the weight distribution. In the aspect of trust value calculation. [14] presents a trust model based on context aware. This model adds context similarity and the concept of trust rules into the calculation process of the direct trusted value. It increases the accuracy of the direct trusted value and filters out the unqualified service providers. [4] proposes a trusted combination service selection method based on Monte Carlo algorithm. It can help the user find the optimal service composition.

In terms of trusted computing, some scholars use recommendation algorithm to calculate the trust value of the service. [5] introduces a service recommendation algorithm based on trusted alliance. This algorithm can improve the accuracy rate and reliability of the recommendation. [16] judges the users' behavior and preference by collaborative filtering algorithm, and puts forward a personalized QoS prediction method.

Some scholars analyze credible values from different angles. [15] computes service entity credible value from the recent trust, history trust and other aspects. [12, 17] establishes a trust evaluation mechanism to calculate the service provider trusted value based on interaction records. Some scholars analysis the influence factors, [6] proposes a dynamic trust model to analyze the trust evaluation impact factors. It can solve the computing trusted value problem of malicious users. [7-8] proposed a trust management framework for multi-cloud environments based on trust service providers. It uses the users' feedback information to evaluate the objective trust value and the subjective trust value of the providers.

Some scholars analyze credible values based on different mechanism. [9] proposed a trust broker mechanism. In this mechanism, the users can get reputation ratings of the service providers, and the brokers can leverage their partners to aggregate the unfamiliar service providers' reputation. [18] proposed a trust model based on SLA. It evaluates cloud services in the conceptual SLA framework. [10] proposed a mendacious evaluation filtering method. Firstly, calculating the average value of the users' evaluation; Secondly determining the upper and lower bounds score threshold; Lastly, deleting the users' evaluation which is beyond the threshold. In this paper, a new identify method is put forward. It can weaken the evaluation weight of malicious users and limit the data privacy level for malicious users. This way instead of removing the malicious users' evaluation. It can ensure that each user has the right to evaluate the service.

In summary, despite the large number of approaches for trusted interaction model there is a lack of efficient techniques. They take no incentive measures to the mendacious providers and the mendacious users. On the one hand, the number of service providers is huge. But the ability is indeterminacy. It is necessary to find an effective interactive model for the users. On the other hand, the malicious evaluations affect the trust value accuracy for the service providers. Some service providers destroy and steal the user's privacy data. These behaviors can cause a huge loss for the users. In this trust model, the malicious users should be analyzed and filtered before the trust value is calculated. The security of privacy data needs a better guarantee. This paper will solve this problem from four aspects:

(1) The services' evaluations should have different weight for different user entities. The user entities with a high credibility will have a big weight to evaluate the services. By this way, this model can filter out the malicious evaluations.

(2) The users' level should be divided according to the user's credibility degree. The users with a low credibility level will have low security level for privacy information. It can prevent users from giving malicious evaluation effectively.

(3) The service provider will be divided into different levels according to the users' evaluation. The users don't want to choose a low level service provider.

(4) This model protects the users' privacy information and it encourages service providers to promote the trust level. It will promote the providers compete healthily in the market.

3 The Process of Dividing Levels

There are two kinds of entities in the interactive system: the user entity, the number is M, $SC=\{sc_1, sc_2, sc_3, \ldots, sc_m\}$; the service provider entity, the number is N, $SP=\{sp_1, sp_2, sp_3, \ldots, sp_n\}$. The attribute information of service providers is stored in matrix structure as shown in the below:

$$SP=\begin{bmatrix} sp_{s1} \\ sp_{s2} \\ \vdots \\ \vdots \\ sp_{sn} \end{bmatrix}=\begin{bmatrix} SG_{s1}^{1} & SG_{s1}^{2} & SG_{s1}^{m} \\ SG_{s2}^{1} & SG_{s2}^{2} & SG_{s2}^{m} \\ & \cdots & \\ & \cdots & \\ SG_{sn}^{1} & SG_{sn}^{2} & SG_{sn}^{m} \end{bmatrix}$$

$$SG_{sn}^{m}=\{QoS_{sn}^{m}, \cos t_{sn}^{m}, t_{sn}\}$$

SG_j^b, represents the number b attribute of the cloud service provider j. The QoS attribute set of service provider SP represents $SP_{si}=[SG_{si}^{1}, SG_{si}^{2}, SG_{si}^{3}, \ldots, SG_{si}^{m}]$, SG_{sn}^{m} represents the number M attribute set of the service provider n. It includes attribute set Qos_{sn}^{m}, cost set $cost_{sn}^{m}$, evaluation time set t_{sn}. Sap_{si} represents trusted value of service si, $Sap_{si}=\sum_{n=1}^{n=m} w_i SC_{SI}^{n}$, w_i represents the attribute weight set of service i. Assigning different weights for different users' attributes. Safety, availability, reliability and other attribute value are called attribute A. For attribute A, the bigger the attribute value is, the better the services' performance will be. The response time, service cost and other service attributes called attribute B. For attribute B, the bigger the attribute value is, the worse the services' performance will be. Therefore, it is necessary to standardize the attribute value matrix. For attribute A,

$$A_{i,j}=\frac{Q_{i,j}-\min\{Q_{i,z}\}}{\max\{Q_{i,z}\}-\min\{Q_{i,z}\}} \quad \textbf{(1)}$$

$\min\{Q_{iz}\}$ represents the minimum value in the z column attribute. The $\max\{Q_{iz}\}$ represents the maximal value in the z column attribute. For attribute B,

$$B_{i,j}=\frac{\max\{Q_{n,z}\}-Q_{i,j}}{\max\{Q_{i,z}\}-\min\{Q_{i,z}\}} \quad \textbf{(2)}$$

Through the standardized operation, the value of the attribute matrix is transformed into the positive increase value. Its range is [0,1].

3.1 The Level Division of the User

The credibility degree of users will be distributed into different levels. The user with a high credibility level will have a bigger weight to evaluate the service. The users' evaluation results are stored as follows:

$$SC_{sp}=\begin{bmatrix} sc_{sp1} \\ sc_{sp2} \\ \vdots \\ \vdots \\ sc_{spn} \end{bmatrix}=\begin{bmatrix} SC_{s1}^{1} & SC_{s1}^{2} & SC_{s1}^{m} \\ SC_{s2}^{1} & SC_{s2}^{2} & SC_{s2}^{m} \\ & \cdots & \\ & \cdots & \\ SC_{sn}^{1} & SC_{sn}^{2} & SC_{sn}^{m} \end{bmatrix}$$

The evaluation set of user$\alpha$to service $SP1$ can be expressed as: $SC_{sp1}^{\alpha}=[SC_{s1}^{\alpha 1}, SC_{s1}^{\alpha 2}, SC_{s1}^{\alpha 3}, \ldots, SC_{s1}^{\alpha m}]$, the evaluation set of user β to service $SP1$ can be expressed as: $SC_{sp1}^{\beta}=[SC_{s1}^{\beta 1}, SC_{s1}^{\beta 2}, SC_{s1}^{\beta 3}, \ldots, SC_{s1}^{\beta m}]$. The malicious users will make the false evaluation. How to identify and remove malicious users? For example, service $sp1$ has δ users. The evaluation which is made by user α is the trusted evaluation. Calculating the evaluation difference between the numbers δ-1 users and user α. It

need calculate δ-*1* times. The credibility levels are graded for users according to the difference value. The formula of difference value between user β and user α is calculated as follows:

$$\delta_{sp1}^{(\alpha,\beta)} = \frac{\sum_{i=1}^{i=m} \omega_i \left| SC_{S1}^{\alpha i} - SC_{s1}^{\beta i} \right|}{\sum_{i=1}^{i=m} \omega_i \left| SC_{s1}^{\alpha i} \right|} \tag{3}$$

The w_i represents the different users' attribute weight. $\sum_{i=1}^{i=m} w_i = 1$. If the users thought the response time attribute is more important, they would assign a larger weight for this attribute. The users are divided into different levels according to the difference trust value. The calculation process is as follows:

$$\theta_{sp1}^{(\alpha,\beta)} = \mu - \left\lfloor \delta_{sp1}^{(\alpha,\beta)} / \mu \right\rfloor - 1 \tag{4}$$

μ represents the gradient of division level. The trust level is in the range [0,μ]. The higher the user level is, the bigger the users' evaluation weight will be. The weight is represented by *wi*.

$$wi = \frac{\theta_{sp1}^{(\alpha,\beta)}}{\mu} \tag{5}$$

wi is in the range [0,1]. When the value of *wi* is 0, it indicates that this user's evaluation has no effect for the providers' reputation.

In order to make punishment measures for the legal evaluation, the credibility level will be determined by the security level. The user with high credibility can have a high security level. If the user with low confidence level wanted to get a higher security level, it would be required to spend more money. In this way, it can keep the user to evaluate the cloud services accurately.

3.2 The Level Division of the Service Provider

The services' trusted value is decided by the users' feedback evaluation. At present, there have been a lot trusted evaluation models about service. In the traditional calculation process, the users' evaluation value has a same weight for the users' trusted value. Then, this kind evaluation model will be attacked by the malicious users easily. Based on [11], the service trusted value calculation process is improved in this paper.

First step, calculate and analyze the evaluation value of each service attribute. the user *ci* makes evaluation for the different attributes.

$$\delta(\mathrm{c}_i, \mathrm{s}_j, \mathrm{t}_k) = \sum_{m=1}^{m=k} w_\sigma \delta_{(c_i, s_j)}^{t_1 \to t_k} k_m \tag{6}$$

w_σ represents the different weight for the different attributes. For service providers, it needs to calculate the direct credible value, the indirect credible value and the recommended credible value. Comprehensive value is given by the calculation of the three kinds credible value. There are *u* service providers participating in the direct evaluation for the service provider s_j. Then calculate the direct credible value for s_j.

$$DTV_{(c_1 ® c_u, s_j)}^{t_k} = \frac{\nabla(f_i^t) \sum_{t=t_1}^{t=t_k} \sum_{i=1}^{i=u} \rho_i \theta(t) \delta(c_i, s_j, t_k)}{u} \tag{7}$$

$\nabla(f_i^t)$ represents the frequency degree function. Within the time range [t_1, t_k], the user who has a high frequency will has a high credibility in the direct credible value compute process. $\theta(t)$ represents time function. The service evaluation occur in the least distance operation point will show the service provider's current service level. σ_I represent users' different credibility weights. If the user had a high credibility, its weight would be big.

The calculation results of service reliability can't be used as the only standard for the trusted level division. Then we will introduce the concept of center degree. The center degree can reactivate the relationship between the user and the service provider.

$$C_D(s_k)=\sum_{j=1}^{j=n} a(s_k,c_j) \tag{8}$$

When s_k has direct interaction with c_j, $a(s_k, s_j)=1$; there is no interaction, then $a(s_k, s_j)=0$. $C_D(s_k)$ indicate the interaction activity degree in the cloud computing system. The higher the activity concentration degree is, the higher the service level will be. Operating frequency indicates the interactive times for the service providers. It can prevent users to give the mendacity evaluation for the providers. Center degree is another influencing factor for the service level classification.

When the service has high credibility and low center degree, the users' quantity is small. The providers' trusted value is high, but this conclusion loses the objectivity. It is possible that the service providers take some measures to get high service levels. If the service providers have high center degree, they will have wide range types of users. Then its credibility value will be more objective and real. So the service providers with high center degree can obtain a high trust value level. The initial value of $C_D(s_k)$ is 0. With the interacting of the interactive number, $C_D(s_k)$ will increase. When the center degree is more than a certain threshold, the service will get a higher level.

The service level is divided according to the trusted value, and the classification algorithm is described as follows:

The level divide of service (SP, SP_1, int σ, int n, int α)

// this algorithm divides provider levels and return the result of the classification in the end.

(1) The trusted value of SP entity set is inputted in the queue SP.

(2) The trusted value is ordered in ascending sequence and the result is stored in the entity set SP_1. $SP_1=[sp_1, sp_2, sp_3 \cdots sp_n]$

(3) $\alpha = n\%\mu$; // μ is the grade gradient, α is the grade level.

(4) Return the results of the classification: $(P_1, P_\alpha), (P_{\alpha+1}, P_{2\alpha}), (P_{2\alpha+1}, P_{3\alpha}) \cdots (P_{\sigma\alpha+1}, P_n)$

The relationship between service providers and data access rights can be expressed by the following matrix:

	A_1	A_2	A_3	$\cdots$	A_m
P_1	(P_1, A_1)	(P_1, A_2)	(P_1, A_3)	$\cdots$	(P_1, A_m)
P_2	(P_2, A_1)	(P_2, A_2)	(P_2, A_3)	$\cdots$	(P_2, A_m)
P_3	(P_3, A_1)	(P_3, A_2)	(P_3, A_3)	$\cdots$	(P_3, A_m)
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
P_n	(P_n, A_1)	(P_n, A_2)	(P_n, A_3)	$\cdots$	(P_n, A_m)

The value of (P_i, A_j) is 0 or 1. When the value of (P_i, A_j) is 1, it represents that the service provider P_i obtains the right to access to the j information of user A. If the value of γ was high, the service providers would have more authorities. The authority for the service provider P_i to access to the privacy data is expressed as:

$$\gamma=\sum_{j=1}^{j=m}(P_i, A_j) \quad (\gamma \subset [0, m]) \tag{9}$$

4 The Trust Interactive Process and the Algorithm Realization

In the interaction process, some service providers declare that it has a high service capacity, but its trusted value is low in the fact. These providers may give the false QOS information to the users. Some providers with a low service capacity have a high trusted value; but its service price is cheap. They are

also a good choice for the users whose service requirements are not high and the economic ability is not strong.

In the interactive process, some respects should be paid attention to:

(a) The low trusted level providers should have few operating authorities for the users' privacy data.

(b)The users with low trusted level have low data privacy level. Users can choose the providers with same level or lower level. If the users need the service provider with a higher credibility level, they should pay more money. In this way, the illegal users will be punished.

(c)The service providers with high trusted level have a high price [17]. This paper makes the attribute of the service completion time as an example to analyze the relationship between the service providers and the users. The service completion time exists rev(vt) function with service payment costs, as shown in Fig. 1.

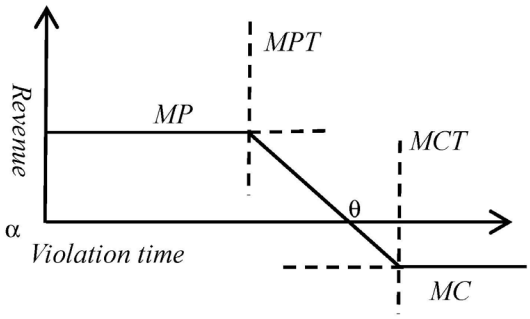

Fig. 1. The relationship of service revenue and time

MP (the max price) is the upper limit value of the service price. *MC* (the max compensation) is the upper limit value for service compensation. [α, *MPT* (the max price time)] express that the fee should be paid in full. In the time range of [*MPT, MCT* (the max compensation time)], service prices decline with the increasing of time and the price will be reduced. When the time is θ, there is no price will be paid to the service providers. At this time, the price is equal to the compensation. In the time range of [θ, *MCT*], the service entities will compensate the user. *MC* is the highest threshold for the compensation.

(d) Guarantee this model is dynamic. When the service provider entity finishes the interaction with the user entity, the system will update the credible value and the privacy information level for the users and services in the history record database.

The dynamic level interaction algorithm based on trusted value is as shown in Fig. 2.

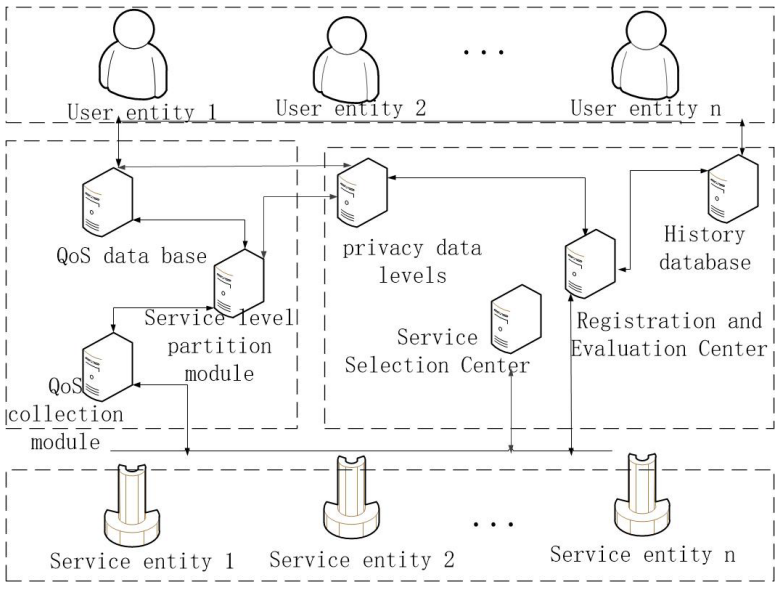

Fig. 2. The relationship of entity based on dynamic level interaction method

The algorithm consists of three processes:

Step 1: The user puts forward a service request. Then the system calculates the credible value for the user, assigns the user credibility level and determines the user privacy data level.

Step 2: The system calculates the providers' trusted value and assigns a credibility level for the provider.

Step 3: According to the rules, the two entities establish an interaction. There are two kinds probabilities: ①. If the level of users' privacy data is higher or equal to the service providers' trusted level, then the interaction will be agreed. ②. If the level of users' privacy data is lower than the providers' trusted level, the users will need to pay much more money. In this way, the users' malicious evaluation will be limited and the privacy data will be protected.

The process of interaction (sc_i, sp_i, sc, sp, Csr, cr, cspr)

input : sc_i, sp_i; // enter user entity set sc, service entity set sp
output: true, false; // output the interaction result is successful or not
$Csr=sr(sc_j)$; //gets the user's credible value from the history record database
$\delta=Formula3(Csr)$; //calculate the difference of the user
$\theta= Formula4(s)$; //calculate the trust level for the user
$cr=Fq(req);$ //get the user's privacy information security level and the service evaluation weight
$\delta_{sp}=Formula6(sp)$; // make preliminary treatment for the service provider
$DTV^{t_k}_{(c_1 \to c_u, s_j)}=Formula7(sp)$; //get the direct credible value of service provider
$cspr=Fq(req, sp)$; //get the service trust level and the privacy information security level
if$(Fq(req)>=Fq(req, sp))$ // if the user privacy data level is higher than the service level, then the user will be agree to interact with the user.
update *cr, pr, cspr*; // update the users' trust level, privacy level, and service entity trust level
return true; //interactive success
}
else if
{
users to pay more money; // the users agreed to pay more money
return true; //interactive is successful
}
return false; // interaction is failed

4 Results and Analysis

In this section, to verify the effectiveness of our method, we conduct a series of experiments. The cloud simulation system Cloudsim3.0 as the simulation experiments' platform, Java language as a programming language. Related configuration: Pentium (R) DuanCore 2.1 GHz CPU 4GB memory, 500GB hard disk, Windows 10 operating system; the development environment is IntelliJ IDEA 2017. The experiment involved two kinds of entities: SC, user entity, SP, service entity. User entities are classified as trusted entities (the evaluation is true) and malicious users; Service entities are classified as trusted service entities and mendacious service entities.

Experiment 1: the effect of computing the users' trusted value in this model. There are three kinds of user entities (Fig. 3), user entities SC1: trusted users accounted for 100%; user entities SC2: trusted users accounted for 70%, non-trusted users accounted for 30%, user entities SC3: trusted users accounted for 55%, malicious users accounted for 45%. The service entities are trusted entities. In the process of interaction, observe the different changes of the trust value of the three type entities.

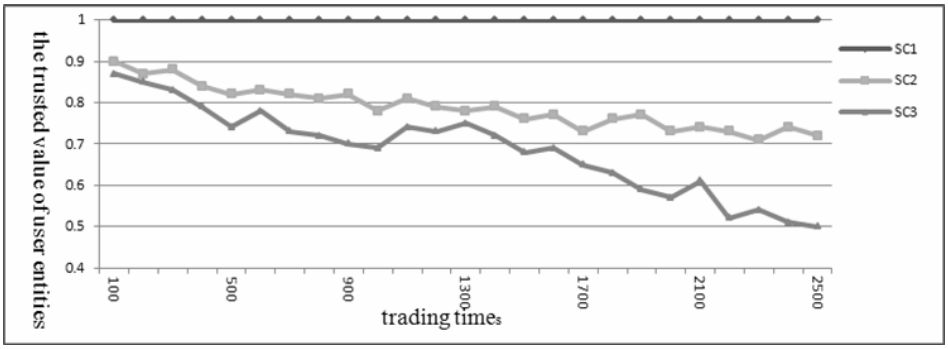

Fig. 3. The trusted value for three kinds of users

With the increasing of the interaction number, the trust value of SC1 remained a stable state. The trust value is 1.0. The trust value of SC2 decreased gradually. There are some users making malicious evaluation. The difference of the change between SC2 and SC3 user entities shows that the uses entities with bigger proportion malicious users have lower trust values. The experiment 1 shows that this model can reflect the change for the different kinds users accurately. It is the basis for the next experiments.

Experiment 2: the effect of filtering illegal users in this model. The service provider's ability changes dynamically in this experiment. The service ability will be raise gradually. The malicious users will do negative evaluations (the value is much lower than the actual service performance). From Monday to Wednesday, the service entities' capability keeps a stable state; the service capacity is increasing gradually from Thursday to Sunday. Compare the change of the trust value in different models. The model proposed in this paper marked as model A, and the comparison model proposed in [13] marked as the model B. The same users interact with the two models at the same time (Fig. 4).

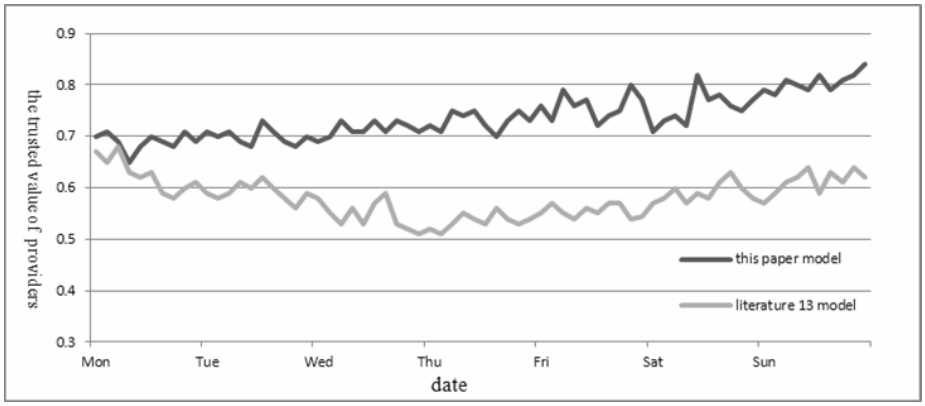

Fig. 4. Simulation result 1 for the experiment 2

For model A, from Monday to Wednesday, the service quality tends to be stable and the service trusted value tends to be stable. From Thursday to Sunday, the trusted value of the service is increasing. For the model B, the malicious evaluation can't be filtered. From Monday to Wednesday, the service capability is stable, but the trusted value of the service has a downward trend. From Thursday to Sunday, as the service quality improved gradually, the service's trusted value is increased. But the rising process is slower and not obvious.

Three kinds of user entities interact with the model A. Observe the changes of the credible value.

As shown in Fig. 5, three groups of users interact with the model A at the same time. The trusted value of service providers is increasing gradually and the difference is getting smaller among the different types of user entities. For the user entities SC1, the trusted value can reflect the service capacity. For the user entities SC2 and user entities SC3, the trusted value is lower than the user entities SC1 at the beginning of the interaction. User entities SC3 have a larger proportion of malicious users. Their trusted value is the lowest. In model A, the evaluation weight of malicious user is reduced. The malicious users make a little weight for the trusted value, then the trusted value has an upward trend. This experiment result shows that the model A can filter out the malicious evaluation for providers by reducing the malicious users' evaluation weight. It can improve the accuracy of service evaluation.

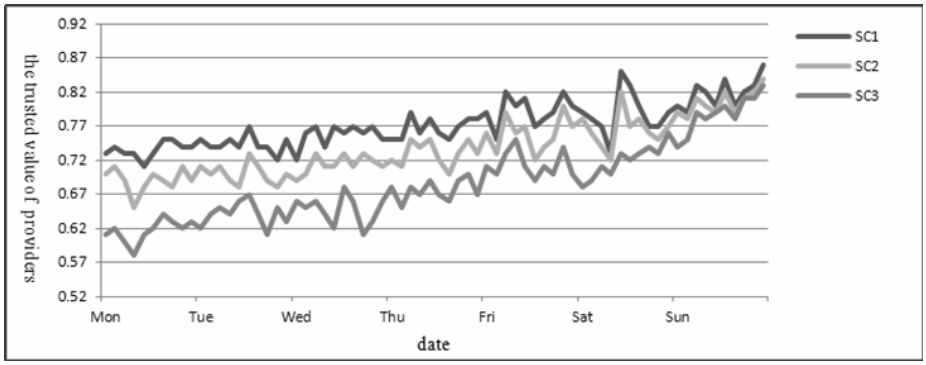

Fig. 5. The trusted value from three kinds users

Experiment 3: the effect of privacy data protection. In this experiment, the user entities are all trust users. The proportion of the trust service entity is 90% and the proportion of the malicious service entity is 10%. In the process of interacting, the destroyed times of data will be recorded. The contrast model selects the trusted interaction model which proposed in the literature [8]. The experimental results are shown as Fig. 6.

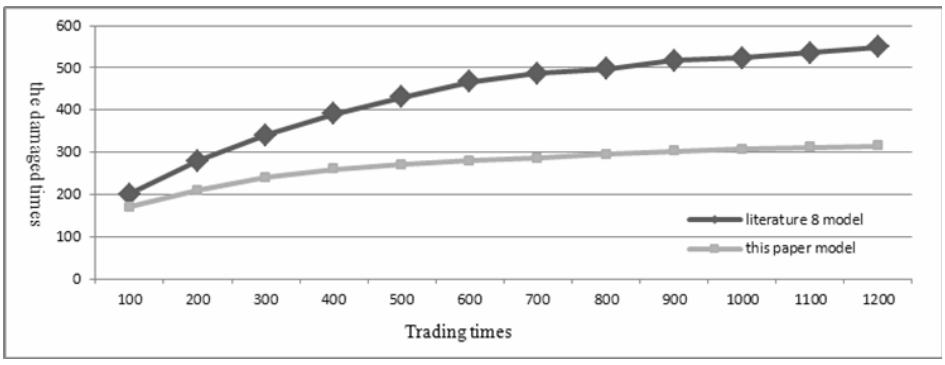

Fig. 6. The damaged times for different model

We can make a summarize from the experiment results, model B can't reduce the damage rate and the damaged times are rising with the interaction times. Because it can't limit the operation rights of malicious providers. The model A can reduce the credible value of malicious service provider and limits their operation rights. The malicious providers have fewer rights to access to the privacy data. With the increasing of interactions times, the operation rights of malicious providers are limited and the damaged times of privacy data are reduced in a certain extent. This experiment results show that model A proposed in this paper can reduce the damage rate effectively.

5 Summary

In the dynamic cloud computing environment, the service entities and the user entities have a complex relationship. The malicious service and users will affect the interaction results. This paper divides two kinds entities into different levels. First of all, it filters out the illegal users' evaluation by reducing the evaluation weight; the second, it determines different privacy data levels for different users. The last, it makes rewards and punishments according to the user's behavior. Through the experimental verification, this model can grad the levels according to the trusted value and limit the access rights of service providers. It can reduce the damage rate of the privacy data and provide an effective new idea for the interaction between users and services providers.

But the new entities have no history data, we can't divide levels for them in this paper. The next step will make a detailed study about how to divide the trusted level for new users and new service providers. It will improve the dynamic interaction model further.

Acknowledgments

This research is supported by Natural Science Foundation of Shandong Province of China under Grant No. ZR2011FM019 and Postgraduate Education Innovation Projects of Shandong Province of China under Grant No. SDYC15042. In addition, the authors would like to thank the reviewers for their valuable comments and suggestions.

Reference

[1] A. Mazhar, S.U. Khan, A.V.Vasilakos, Security in cloud computing: opportunities and challenges, Information Sciences 305(2015) 357-383.

[2] Z.A. Soomro, M.H. Shah, J. Ahmed, Information security management needs more holistic approach: a literature review, International Journal of Information Management 36(2)(2016) 215-225.

[3] U.M. Gias, M. Zulkernine, S.I. Ahamed, CAT: a context-aware trust model for open and dynamic systems, in: Proc. the 2008 ACM symposium on Applied computing, 2008.

[4] X.Y. Li, X.L. Gui, A comprehensive and adaptive trust model for large-scale P2P networks, Journal of Computer Science and Technology 24(5)(2009) 868-882.

[5] L. Li, Y. Wang, E.P. Lim, Trust-oriented composite services with QOS constraints, Journal of Universal Computer Science 16(13)(2010) 1720-1744.

[6] L. Bin, M. Xing, J. Zhu, T. Che, A dynamic trust model for the multi-agent systems, in: Proc. 2008 International Symposiums on Information Processing, 2008.

[7] H.Y. Wang, W.B. Yang, S.C. Wang, S.-R. Li, A service recommendation method based on trustworthy community, Chinses Journal of Computers 37(2)(2014) 301-311.

[8] L. Shao, J. Zhang, Y. Wei, J. Zhao, B. Xie, H. Mei, Personalized QoS prediction for web services via collaborative filtering, in: Proc. International Conference on Web Services, 2007.

[9] S. Singh, D. Chand, Trust evaluation in cloud based on friends and third party's recommendations, in: Proc. Engineering and Computational Sciences(RAECS), 2014.

[10] D. Anupam, M.M. Islam, SecuredTrust: a dynamic trust computation model for secured communication in multiagent systems, IEEE Transactions on Dependable & Secure Computing 9(2)(2011) 261-274.

[11] W.J. Fan, H. Perros, A novel trust management framework for multi-cloud environments based on trust service providers, Knowledge-Based Systems 70(C)(2014) 392-406.

[12] W. Wang, G. Zeng, D. Tang, J. Yao, Cloud-DLS: dynamic trusted scheduling for cloud computing, Expert Systems with Applications 39(3)(2012) 2321-2329.

[13] Y.-J. Hsu, K.-J. Lin, T.-H. Chang, C.-J. Ho, H.-S. Huang, W.-R. Jih, Parameter learning of personalized trust models in broker-based distributed trust management, Information Systems Frontiers 8(4)(2006) 321-333.

[14] A. Mohammed, T. Dillon, E. Chang, SLA-based trust model for cloud computing. in: Proc. International Conference on Network-Based Information Systems(NBiS), 2010.

[15] H.Y. Wang, W.S. Jin, Service recommendation based on trustworthy community under big data environment, Journal of Huazhong University of Science and Technology (natural science edition) 44(03)(2016) 22-27.

[16] L. Zhang, K.L. Rao, R.C. Wang, Dynamic trust evaluation model based on evaluation credibility in cloud computing environment, Journal of Communication 34(z1)(2013) 31-37.

[17] M. Mario, J. Guitart, SLA negotiation and enforcement policies for revenue maximization and client classification in cloud providers, Future Generation Computer Systems 41(C)(2014) 19-31.

[18] C.H. Hu, X.X. Luo, S.C. Wang, Y. Liu, Approach of sercive evaluation based on trust reasoning for cloud computing, Journal on communications 32(12)(2011) 72-81.