Journal of mathematics and computer science 14 (2015), 315-325

Contents list available at JMCS

Journal of Mathematics and Computer Science

Journal Homepage: www.tjmcs.com

Trust Model to Enhance Security of Cloud Computing

Ali. Mohsenzadeh

Information Technology Department, Mazandaran University of Science and Technology, Babol, Iran
ali.mohsenzadeh@ustmb.ac.ir

Article history:
Received November 2014
Accepted December 2014
Available online January 16, 2015

Abstract

Trust is one of the most important means to improve security and enable interoperability of current heterogeneous independent cloud platforms. Trust is a level of subjective probability between two entities, a trustor and a trustee, which is formed through the direct observation nature and/or recommendation from trusted entities. Today, there is no special trust evaluation model for cloud computing environment. Hence, in this paper, we present a trust model based on fuzzy mathematics in cloud computing environment according to success and failure interaction between cloud entities.

Keywords: cloud computing, trust model, trust recommendation.

1. Introduction

Cloud computing based on many other existing technologies is a new method for sharing infrastructure which provides customers with extremely strong computation capability and huge memory space while with low cost. But now cloud computing is faced with many problems to be resolved especially security. Till now most IT enterprises' cloud platforms are heterogeneous, independent and not interoperable. Compared to traditional technologies, cloud has many specific features, such as it is ultra-large-scale and resources belong to each cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity validation, authentication and authorization were no longer suitable for cloud. Trust which is originally society notion in constructing human beings' relationship is now an essential substitute for former security mechanism in distributed environments. Some experts said the biggest issue of cloud computing 2009 is trust [1- 4].

In fact, trust is the most complex relationship among entities, because it is extremely subjective, context-dependant, non-symmetric, uncertain, par-tially transitive, and difficult to evaluate and establish [3,7]. Today, there is no special trust evaluation model for cloud computing environment. Therefore, in this paper, we present a fuzzy trust model in cloud computing environment.

The rest of the paper is organized as follows. In Section2, we present a trust model of choosing trust-ed entities base on the fuzzy relationship theory in fuzzy mathematics in cloud environment. In section 2.1, 2.2 and 2.3 we calculate direct trust, indirect trust and total trust, respectively. Experiment results in Section4 show that proposed model can effectively prevent selfish entities. Finally the summary and future work is presented in Section6.

2. Proposed Trust Model

In general trust can be classified into different categories according to different standards.

- According to attributes: identity trust and behavior trust
- According to obtaining way: direct trust and recommended trust
- According to role: code trust, third party trust and execution trust, etc.
- According to based theory: subjective trust and objective trust

In this paper, we use the second category to evaluating trust

Definition 1: (Trust). Trust is a level of subjective probability between two entities, a trustor (i.e. source entity) and a trustee (i.e. target entity), which is formed through the direct observation nature and/or recommendation from trusted entities, to fulfilling a particular service within a specific time and context.

It is supposed that the trustor is a cognitive entity with an ability to make assessments and decisions about the received information and past experiences. Trust is usually evaluated by trust degree and described with trust relation[7,10].

Definition 2: (Trust degree). Trust degree Tdij is used to evaluate the degree of trust from a domain set of possible trust values that trustor ei in views trustee ej and denotes entity's ei trust attitude (opinion) towards entity ej in time t and context cz . The trust degree can be expressed as the following relation:

$$Td_{ij} = \begin{cases} DT\left(e_i, e_j, c_z, t\right), \\ RT\left(e_i, e_j, c_z, t\right), \\ IDT\,(e_i, e_j, c_z, t), \\ Otherwise \end{cases} \qquad (1)$$

Where $Td_{ij}=DT(e_i,e_j,c_z,t)$, $Td_{ij}=RT(e_i,e_j,c_z,t)$ and $Td_{ij}=IDT(e_i,e_j,c_z,t)$ are the direct trust degree , recommendation trust degree and indirect trust degree between trustor e_i (i.e. source entity) and trustee e_j (i.e. target entity) in context Cz and time t.

In real cloud environment, Trust and Reputation both depend on some contex[10,11,13].t. For example, entity A trusts entity B as multimedia provider, but it does not trust B as a storage provider. So in the context of requesting a multimedia service, B is trustworthy. But in the context of providing storage service, B is untrustworthy.

In this paper, we calculate trust degree with fuzzy set theory, so the mathematical model of fuzzy trust should be firstly created.

Suppose $E=\{e_1,e_2,\ldots,e_n\}$ is the problem domain of fuzzy trust model, where e_i(i=1,2,…,n) is an entity in the problem domain [3,6,12]. A membership function μ(e) defines the degree to which a fuzzy variable x is a member of a set. $\mu(e)$ map e into the interval [0,1] . Full membership is represented by 1 and no membership by 0. The values between 0 and 1 characterize fuzzy members, which belong to the fuzzy set only partially [15]. Supposing the problem domain E is not the empty set, TR is a fuzzy set of Cartesian product of E×E; E is the set that includes all the entity in cloud environment. There exists a mapping:

$$\begin{aligned} &TR \ : E \times E \to [0,1], \qquad\qquad (2) \\ &(e_i, e_j) \to \mu_A(e_i, e_j) \in [0,1] \end{aligned}$$

To manage a collection of trust related activities across domains, we need to understand trust itself. From different points of views, trust can be categorized into different classes: direct trust and indirect trust (the indirect trust relation is a composite fuzzy relation of recommending relation and direct trust relation).

2.1 Fuzzy direct trust relation

When we say entity ei is trustworthy or untrustworthy for entity ej, there is a trust relationship between entity ei and entity ej. If this statement is based on entity ei's direct experiences with entity ej completely, this relationship is called the direct trust relation or direct trust model. Fig. 1 shows fuzzy direct trust degree between entity ei and entity ej at context Cz and time t .

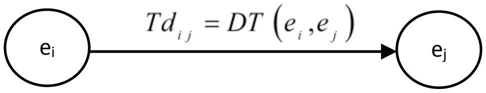

Fig1. Direct trust relation between e_i and e_j

Direct trust relation is not a crisp binary relation that is either true or false. For example, entity ei usually says an 80 percent probability that entity ej is a trusted peer. This hints that trust has different levels or degrees. Direct trust relation just has fuzzy properties. We can use fuzzy relation to describe direct trust relation. Fuzzy direct trust degree between two entities can be denoted by fuzzy graph.

Definition 3.(trust graph): The trust relations in the cloud computing environment of entities are represented as a trust graph G. [7,10,13]. It represents a directed graph with entities as nodes and edges as trust relations among them. The edges are directed and If an edge indicates a trust relation of entity ei towards entity ej, it is directed from entity ei to entity ej with the trust degree Tdij. A possible way of representing a directed graph is a matrix defined as follows.

Definition 4.(Trust matrix): interactions in a cloud computing environment of n entites is represented with a trust matrix M, where elements Tdij indicate a trust relation of entity ei towards entity ej, and have values, where each value denotes the degree of trust[7,10,13,17].. If a relation is not defined, it is indicated as zero(Note that Tdij=0 does not imply Tdji=0). The matrix represents trust in a cloud computing environment at a specific time t ∈ T and specific context Cz denoted M(t,Cz) as:

$$M(t, \mathrm{c_z}) = \begin{pmatrix} Td_{11} & \cdots & Td_{1n} \\ \vdots & \ddots & \vdots \\ Td_{m1} & \cdots & Td_{mn} \end{pmatrix} \qquad (3)$$

Based on the assumption that trust relation is reflexive, it follows that all the diagonal elements in diagonal are equal to one which indicates the maximum trust degree.

2.1.1 Fuzzy Direct Trust Degree Computing

Suppose in the past entity e_i has p times successful interactions and q times failure interactions with entity e_j at a specific time t and context c_z. We define the fuzzy direct trust relation membership function:

$$T_z d_{ij} = DT(\mathrm{e_i}, \mathrm{e_j}, \mathrm{c}_z, \mathrm{t}) = \frac{p_z}{p_z + q_z} \qquad (4)$$

It is worth to mention again that, as a entity behavior is not always constant but often changes with time, therefore, the recent experience is more credible than the general historical experience, therefore, We have considered the function to determine the successful experiences over time. This function calculates the successful interaction rate based on historical successful interaction between trustor ei and trustee ej at a specific time t and context c_z. This function is given below:

$$\begin{aligned} & p(Tp_i) = \alpha p(\Delta T_i) + (1-\alpha) p(T_{i-1}) \quad , \\ & Tp_i = Ti \quad , \\ & \Delta T_i = Tp_i - Ts_{i-1} \quad , \\ & p(T_0) = p(Ts_0) = 1 \quad , \\ & Ts_i = Tp_i \quad ,(i > 0) \end{aligned} \qquad (5)$$

Where α is the adjustable parameters and presents the weight of successful interactions in different timescales (ΔT_i). $P(\Delta T_i)$ is recent successful interactions and $P(T_{i-1})$ is historical successful interaction. moreover T_p and Ts represent present time, start time respectively. Also Ts_0 represents the first interaction between trustor e_i and trustee e_j at time t and context c_z.

We have considered the weights of the past negative behavior β which can be regulated to punish the selfish entity action. Then the fuzzy direct trust relation can be revised as:

$$T_z d_{ij} = DT(\mathrm{e_i}, \mathrm{e_j}, \mathrm{c}_z, \mathrm{t}) = \frac{p_z(Tp_i)}{p_z(Tp_i) + \beta q_z} \qquad (6)$$

It is difficult to decide whether an entity is bad or good based on only few interactions. In determining trust it is important that an entity has sufficient experience on which to calculate trust[9]. So we define the confidence level in the experience for a particular context c_z as an interaction threshold value Co_z of interaction times.

$$\begin{aligned} & p_z + q_z \le Co_z \\ & p_z + q_z > Co_z \end{aligned} \qquad (7)$$

Thus, if the interaction times are too small (i.e $p_z+q_z<=co_z$) between trustor e_i and trustee e_j, this computing as defined in relation4 may be an arbitrary decision and the following equation can be used.

$$T_z d_{i\,j} = DT\,(\mathrm{e_i}, \mathrm{e_j}, \mathrm{c}_z, \mathrm{t}) = 0.5 + \frac{p_z\,(Tp_i) - \beta q_z}{2 \times Co_z} \qquad (8)$$

2.2 Fuzzy Indirect trust relation

Only one entity as trustor ei always has limited direct interaction experiences with trustee ej. If he wants to get a more accurate trust degree, a natural way for trustor ei is to ask its acquaintances about their opinions at specific context cz. Therefore even trustor ei has not any direct experience with trustee ej in the past, trustor ei can builds a trust relation with trustee ej through his acquaintances. We call the trust relation built by its acquaintances Indirect Trust Relation, which is shown in fig 2. Actually an indirect trust relationship builds from recommendations by a trusted third party (i.e acquaintances) or a chain of trusted partied, which create an indirect trust path, which has fuzzy properties. In other words, the indirect trust integrates the recommendation trust and direct trust model.

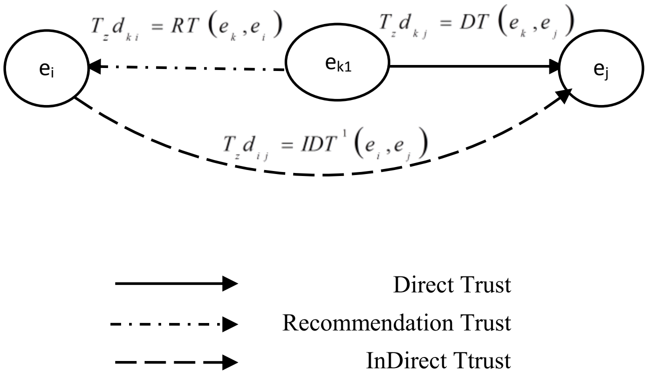
$T_z d_{k\,i} = RT\left(e_k, e_i\right)$
$T_z d_{k\,j} = DT\left(e_k, e_j\right)$
e_i
e_{k1}
e_j
$T_z d_{i\,j} = IDT^1\left(e_i, e_j\right)$
Direct Trust
Recommendation Trust
InDirect Ttrust

Fig2.one-level fuzzy Indirect trust

As shown in fig 2, entity ek has directed interaction experiences with trustee ej, so there has a direct trust relation between entity ek and trustee ej noted as DTkj. There also has a recommending relation between entity ek and trustor ei. entity ek recommends its direct experiences to trustor ei noted as RTki, and then these experiences become indirect experiences for trustor ei noted as IDTij

Peer k has directed interaction experiences with peerj, there has a direct trust relation between k and j noted as DTkj. There also has a recommending relation between k and i. Peer k recommends its direct experiences toi, and then these experiences become indirect experiences fori. But maybe kis not a very familiar friend of peeri ,or k has recommend i inaccurate experiences in the past, peer I does not think k's recommendation is completely right.

2.2.1 Fuzzy recommendation trust relation

In figure 2 entity e_k recommends its direct experiences to trustee. But maybe entity e_k is not a very familiar friend of entity e_i, or e_k has recommend dishonest in the past, entity e_i does not think e_k's recommendation is completely right. Thus the recommending relation also has fuzzy properties. We also can use fuzzy relation to describe the recommending relation.

The fuzzy relation membership function defines a degree of recommending relationship between entity e_i as trustor and entity e_k as recommender, which is similar to fuzzy direct trust relation membership function:

$$T_z d_{ki} = RT\,(\mathrm{e}_k, \mathrm{e}_i, \mathrm{c}_z, \mathrm{t}) = \begin{cases} 0.5 + \dfrac{r_z(Tr_i) - \alpha s_z}{2 \times Co_z} & if \quad r_z + s_z \le Co_z \\ \dfrac{r_z(Tr_i)}{r_z(Tr_i) + \alpha s_z} & if \quad r_z + s_z > Co_z \end{cases} \qquad (9)$$

Where r represents the number of successful recommendation interactions and s represents the number of failure recommendation interactions between entity e_j and entity e_k at a specific time t and context c_z.

Intuitively, seems reasonable that the higher the trust value of the entity, the more important the recommendation view. However, the entity's trust value is not entirely consistent with the credibility of the recommendation. On the other hand, some malicious entity may exist in the system. In such cases, different types of attacks can be considered (such as bad-mouthing and on-off).[13,15] In all attacks, malicious one tries to be keeping herself as a trusted entity using misleading actions or reputation. Parts of selfish entity through camouflage get the higher trust values, while they give the higher recommendations to their acquaintances, but those recommendations are obviously incredible. So, the credibility of the recommendation of a entity is different from that of itself, especially under some collective or disguised selfish entity. Therefore every proposed model for trust must be able to consider these attacks and also should be able to verify the system against them.

2.2.2 Fuzzy InDirect Trust Degree Computing

As mentioned, The fuzzy indirect trust relation IDT_{ij} is a composite fuzzy relation of fuzzy recommending relation and fuzzy direct trust relation, In this paper we have used min-max composition to composite fuzzy direct trust value and fuzzy recommendation value. Therefore, the fuzzy indirect trust relation for fig.2 is given by:

$$\begin{aligned} T_z d_{ij} &= IDT^{1}(\mathrm{e}_i, \mathrm{e}_j, \mathrm{c}_z, \mathrm{t}) = RT \circ DT \\ &= RT\,(\mathrm{e}_k, \mathrm{e}_i, \mathrm{c}_z, \mathrm{t}) \circ DT\,(\mathrm{e}_k, \mathrm{e}_j, \mathrm{c}_z, \mathrm{t}) \qquad (10) \\ &= \left\{ Max_{ek}\, Min\left(RT\,(\mathrm{e}_k, \mathrm{e}_i, \mathrm{c}_z, \mathrm{t}), DT\,(\mathrm{e}_k, \mathrm{e}_j, \mathrm{c}_z, \mathrm{t})\right)\right\} \\ &= \vee_{ek \in E}\,(RT\,(\mathrm{e}_k, \mathrm{e}_i, \mathrm{c}_z, \mathrm{t}) \wedge DT\,(\mathrm{e}_k, \mathrm{e}_j, \mathrm{c}_z, \mathrm{t})) \end{aligned}$$

In the above equation, we calculated one-level fuzzy indirect trust value which includes one level recommendation based on fig.2. Fig.3 shows the two-level fuzzy indirect trust which includes two level recommendation. In this fig, entity e_{k2} has the direct interaction experiences with entity e_j, there has a direct trust relationship them.

Entity e_{k2} recommends its direct experiences to e_{k1}, then entity e_{k1} recommends its indirect experiences to trustor e_i, and then these experiences become indirect experiences for trustor e_i. the two level fuzzy indirect trust is computed as follows:

$$
\begin{aligned}
T_z d_{i\,j} = IDT^{2}(\mathrm{e_i},\mathrm{e_j},\mathrm{c_z},\mathrm{t}) &= RT \circ RT \circ DT \\
&= RT^{2} \circ DT
\end{aligned}
$$

$$
\begin{aligned}
RT^{2} &= RT\,(\mathrm{e}_{k\,2},\mathrm{e}_{k\,1},\mathrm{c_z},\mathrm{t}) \circ RT\,(\mathrm{e}_{k\,1},\mathrm{e}_{i},\mathrm{c_z},\mathrm{t}) \qquad (11)\\
&= \left\{ Max_{e\,k}\, Min(RT\,(\mathrm{e}_{k\,2},\mathrm{e}_{k\,1},\mathrm{c_z},\mathrm{t}), RT\,(\mathrm{e}_{k\,1},\mathrm{e}_{i},\mathrm{c_z},\mathrm{t})) \right\}\\
&= \vee_{e_{\,k\,1}\in E}\,(RT\,(\mathrm{e}_{k\,2},\mathrm{e}_{k\,1},\mathrm{c_z},\mathrm{t}) \wedge RT\,(\mathrm{e}_{k\,1},\mathrm{e}_{i},\mathrm{c_z},\mathrm{t}))
\end{aligned}
$$

If entity e_i continues in this manner, there have three, four… n levels indirect trust relation and it can get more and more accurate trust degree with entity e_j in context c_z .The multi-level composite fuzzy indirect trust is calculated as:

$$
\begin{aligned}
T_z d_{i\,j} = IDT^{n}(\mathrm{e_i},\mathrm{e_j},\mathrm{c_z},\mathrm{t}) &= RT \circ RT \circ ... \circ RT \circ DT \\
&= RT^{n} \circ DT \qquad (12)\\
RT^{n} = RT^{n-1} \circ RT\ ,(\mathrm{n} = 1, 2, 3, ...)
\end{aligned}
$$

If there is some trust path between trustor e_i and trustee e_j, the indirect trust value between e_i and e_j calculates from the union of all indirect trust value in different path(one-level, two-level,…):

$$
\begin{aligned}
T_z d_{i\,j} = IDT\,(\mathrm{e_i},\mathrm{e_j},\mathrm{c_z},\mathrm{t}) &= IDT^{1} \cup IDT^{2} \cup ... \cup IDT^{n}\\
&= \bigcup_{i=1}^{n} IDT^{i} \qquad (13)
\end{aligned}
$$

Usually trustor ei has not only direct interaction experiences with trustor ej (in context cz), but also indirect experiences from asking its acquaintances.

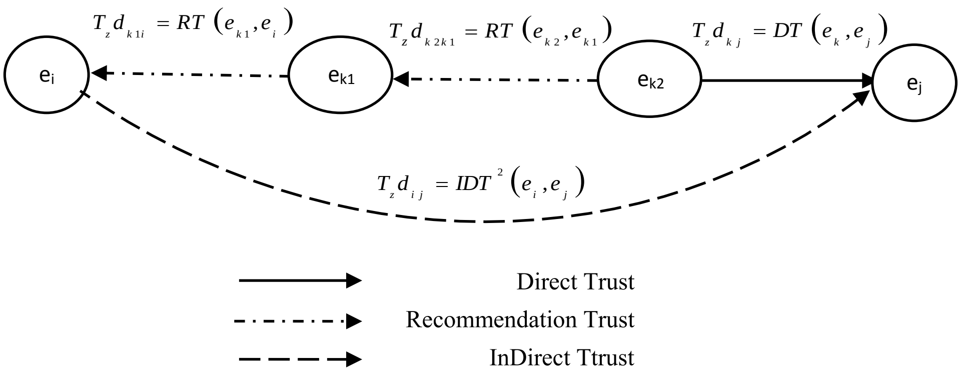
$T_z d_{k1i} = RT\,(e_{k1}, e_i)$
$T_z d_{k2k1} = RT\,(e_{k2}, e_{k1})$
$T_z d_{kj} = DT\,(e_k, e_j)$
e_i
e_{k1}
e_{k2}
e_j
$T_z d_{ij} = IDT^{2}\,(e_i, e_j)$
Direct Trust
Recommendation Trust
InDirect Ttrust

Fig3. Two-level fuzzy Indirect trust model

Then there are two fuzzy trust relation (i.e fuzzy direct trust relation and fuzzy indirect trust relation) between trustor ei and trustor ej, If trustor ei wants to get more accurate trust value with trustor ej, it must integrate the direct and indirect experiences. The fuzzy global trust relation is a union of fuzzy direct trust relation and indirect trust relation obtained from relation 14.

$$T_z d_{i\,j} = DT \cup IDT^{1} \cup IDT^{2} \cup \ldots \cup IDT^{n}$$

$$= DT \cup \bigcup_{i=1}^{n} IDT^{i} \qquad (14)$$

3. Experimental Result

In order to evaluate the performance of the proposed model in this paper, simulation environment and parameters set are firstly discussed in this section, and then precise performance evaluation results are given.

3.1 Experiments environment and configuration

The platform of simulation environment is CloudSim toolkit (Buyya et al., 2009) which is a simulation platform based on Java, which supports modelling and simulation of large-scale cloud computing data centers. Therefore, it is feasible to simulate our proposed model of cloud computing environments by CloudSim. We create ten data centres in the simulation environment, We set 500 virtual machines. Moreover, we submit 1000 tasks to the 500 virtual machines. Also recommenders are divided into three types:

1. virtuous recommenders who provide honest service and recommendation
2. random recommenders who provide random service and recommendation
3. malicious recommenders who provide malicious service and recommendation.

We have designed simulation experiments for cross domain transactions, all the virtual machines in the same data centre belong to one intra-domain, and the virtual machines in different data centre belong to one inter-domain. Moreover, we submit 1000 tasks to the 500 virtual machines, each task is submitted according to Poisson distribution after its previous task, the length of each task is considered as a random number within the range of [10,000, 20,000] MI. We set five trust dimensions in DMTC model. There are reliability, availability, safety, maintainability, and integrity. Table 1 shows the main parameters used in this set of experiments.

Table1.Configuration Parameters

direct trust relation	
0.7	α : the weight of successful interactions in different timescales
1.1	β : the weights of the past negative behaviour
30	ΔT :the timescales determine the number of successful interactions
25	Co$_z$: the threshold value for direct trust relation
1	The initial direct trust when there is no interaction between entities
recommendation trust relation	
0.6	α : the weight of successful interactions in different timescales
1.1	β : the weights of the past negative behavior
30	ΔT :the timescales determine the number of successful interactions
40	Co$_z$: the threshold value of the recommending times

3.2 Comparison among trust models

An important application of the proposed trust analysis is to facilitate comparison among different trust establishment methods. There are some trust schemes proposed for cloud environment, so, it is difficult to list all the trust models to compare with each other.In the Section, we make a comparison with DMTC [7].

3.2.1 Trust accuracy rate

We use absolute error metrics for evaluating the accuracy. Absolute error: It is the difference between the actual value of trust for an edge and the calculated value from a method.

$$\text{Absolute error}=|\text{trust calculated}-\text{actual trust}| \qquad (15)$$

As shown in Figure 4, in the first simulation time, when there is no interaction between entities, we set direct trust equal to one. Therefore Absolute error is set one. The success interaction rate declines with malicious interactions at the beginning. After a time, the success interaction rate keeps rising. Also, with the increase of the malicious rate, the proposed model can ensure trust accuracy rate in a high level.

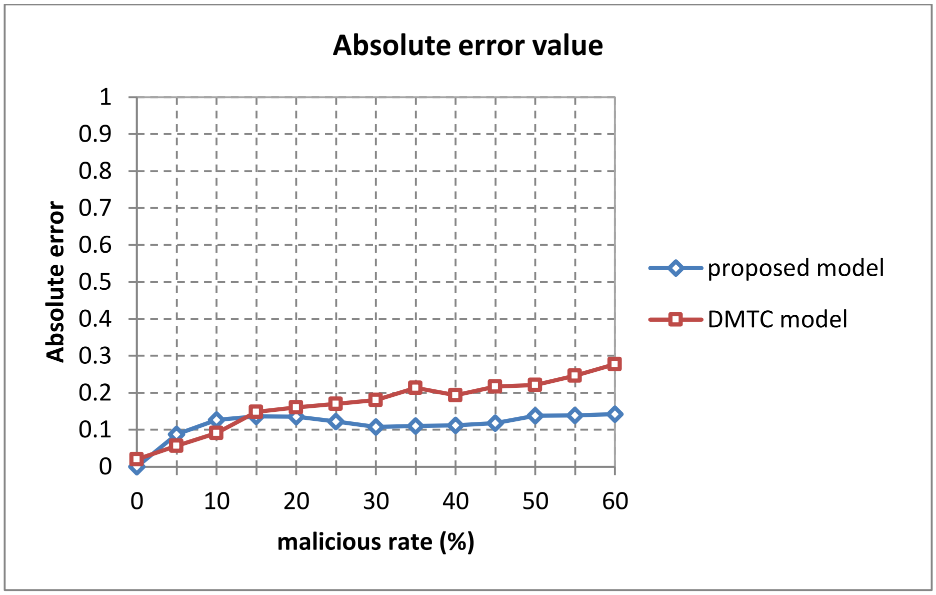

Fig4. Absolute error value

3.2.2 Success interaction rate

The good entities can be differentiated from the misbehavior entities by their trust values after a few interactions. At the beginning, all entities have the same initial trust value, the trustors randomly select a entity, after a few numbers of interactions, and the normal entities can get the higher trust value than the other selfish entities. With a help of the trust computing based on proposed model, we can identify the malicious entities efficiently. Thank to it, we can restrict the interaction of malicious entities further. It can help to increase the success interaction rate of the system.

Success interaction rate is the ratio of successful interactions to overall interactions in the simulation time denoted as:

$$success\ interaction\ rate = \frac{p}{p+q} \qquad (16)$$

The experiment results are shown in Fig 5. Results show that the success interaction rate with proposed model is higher than DMTC model. From Figure5, we can see that the changing of success interaction rate is divided into two stages: decline stage and rise stage. The success interaction rate declines with malicious interactions at the beginning. After a time, the success interaction rate keeps rising. It is because that the system with trust computing has begun to identify the malicious entities and refuse to provide service for them.

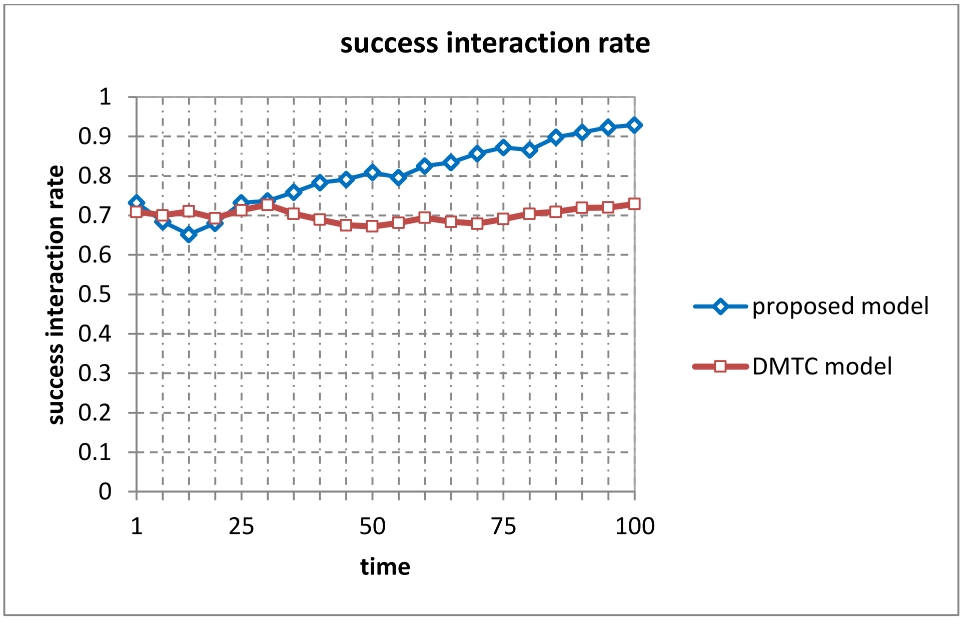

Fig5. Success interaction rate

4. Conclusion

In this paper, we use the fuzzy relation theory in fuzzy mathematics to build trust model between entities, which bases on fuzzy recommendation in cloud environment. Simulation results show that the proposed model has some identification and containment capability in synergies cheating, promotes interaction between entities, and improves the performance of the entire cloud environment. In the future, we will offer new dynamic scheduling algorithm according to proposed model for cloud computing.

References

[1] Dimitrios Zissis, Dimitrios Lekkas "*Addressing cloud computing security issues*" Journal of Future Generation Computer Systems, (2010) Elsevier.

[2] Md. Tanzim Khorshed, A.B.M. Shawkat Ali, Saleh A. Wasimi "*A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing*" Journal of (2012) Elsevier.

[3] Dawei Sun, Guiran Chang, Lina Sun, Xingwei Wang "*Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments*" journal of Procedia Engineering. (2011) Elsevier.

[4] Z.Malik, Bouguettaya "*Reputation Bootstrapping for Trust establishment among Web Services*" IEEE Internet Computing. vol 13, no. 1, (2009) Computing and Applications, Vol. 3, No. 4, (2011).

[5] A. Josang, R. Ismail, C. Boyd, "*A survey of trust and reputation systems for online service provision*", Journal of Decision Support Systems, vol. 43 (2007), no. 2.

[6] F. Azzedin, A. Ridha, A. Rizvi, "*Fuzzy trust for peer-to-peer based systems*", in: Proceedings of World Academy of Science, Engineering and Technology 2007 PWASET (2007), pp. 123–127.

[7] Dawei Sun, Guiran Chang, Lina Sun, Fengyun Li, Xingwei Wang "*A dynamic multi-dimensional trust evaluation model to enhance security of cloud computing environments*" Int. J. Innovative Computing and Applications, Vol. 3, No. 4, (2011), Inderscience Enterprises Ltd

[8] Wenjuan Li, Lingdi Ping "*A Trust Model to Enhance Interoperability of Cloud Environment*" CloudCom 2009, LNCS 5931, (2009) pp. 69–79. Springer.

[9] I. Mouline, "*Why assumptions about cloud performance can be dangerous to your business*," Cloud Comp. J., vol. 2, no. 3 (2009), pp 24–28.

[10] Damjan Kovac, Denis Trcek "*Qualitative trust modeling in SOA*", Journal of Systems Architecture. (2009) Elsevier.

[11] Junhai Luo, Xue Liu, Mingyu Fan "*A trust model based on fuzzy recommendation for mobile ad-hoc networks*" Journal of Computer Networks. (2009) Elsevier.

[12] Tsung-Yi Chen , Yuh-Min Chen, Chia-Jou Lin, Pin-Yuan Chen "*A fuzzy trust evaluation method for knowledge sharing in virtual enterprises*" Journal of Computers & Industrial Engineering, (2010) Elsevier.

[13] Fajiang Yu, Huanguo Zhang, Fei Yan "*A Fuzzy Relation Trust Model in P2P System*". IEEE (2006).

[14] Hyukho Kim, Hana Lee, Woongsup Kim, Yangwoo Kim "*A Trust Evaluation Model for QoS Guarantee in Cloud Systems*" International Journal of Grid and Distributed Computing Vol.3, No. 1 (2010), March.

[15] Zhao-xiong ZHOU, He XU, Suo-ping WANG "*A Novel Weighted Trust Model based on Cloud*", Advances in Information Sciences and Service Sciences. Vol. 3, No. 3 (2011), April.

[16] S. Lee, R. Sherwood, B. Bhattacharjee, "*Cooperative peer groups in nice*", in IEEE Infocom, April (2003).

[17] S. Schmidt, R. Steele, T.S. Dillon, E. Chang, "*Building a fuzzy trust network in unsupervised multi-agent environments*", in: OTM Workshops, (2005), pp. 816–825.

[18] Badrul Sarwar, George Karypis, "*Joseph Konstan, and John Riedl," Item-Based Collaborative Filtering Recommendation Algorithms*", ACM 1-58113-348-0/01/0005. ,May 1-5, (2001), Hong Kong.