Study on Trust Evolution and Simulation Oriented to Cloud Services

Zhou Yuejin
School of Management and Engineering, Nanjing University, Nanjing, China
yjzhou@nju.edu.cn

***Abstract*—Cloud computing, as a novel business model, has been paid more and more attention from academia and industry. The security issue of cloud computing is a key constraint for its applications. Some scholars studied the security issues of cloud computing from the viewpoint of trust. However, the past researches of trust mainly focused on the computation of trust degrees and overlooked the research of evolution of trust relationships. In addition, these research models could not completely adopt the environment of cloud computing. This article constructed a trust evolution model based on the trade evaluation mutually combined with the theory of interpersonal society trust relationship and characteristics of cloud services. Simulation was made on the Netlogo platform and the simulation results proved the model is reliable and effective. The model has a certain applied value.**

***Index Terms*—cloud computing, cloud service, trust, evolution, simulation, the behavior similarity theory**

I. Introduction

Cloud computing is a novel business model that enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. Its essential characteristics include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Cloud services are a fundamental component in cloud computing: infrastructure, platforms, and software are provided and consumed as on demand services [2].

In the recent years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is [3]. So cloud security is regularly cited as an inhibitor for the more rapid adoption of cloud services [4]. Cloud security involves many aspects including access control, identity management, monitoring, encryption, data, privacy protection, infrastructure, and trust. Among them, trust is one of the core issues of cloud security.

Manuscript received September 1, 2013; revised November 27, 2013.

In this paper, trust study is focused as a research direction of cloud security. The article first examined the related researches about trust in the condition of cloud services. And then the paper provided a model of the trust evolution based on the theory of the life cycle. After that the paper described the simulation results with the model on the Netlogo platform. Finally the article discussed the contributions and implications of the research as well as the future study work.

II. Literature Review

A. Definition of Trust

Trust is a complex concept for which there is no universally accepted scholarly definition at present. There are a great number of papers that studied trust definitions from different views such as a psychological state [5]; a behavior [6]; an attitude [7]; a confidence [8]; an expectancy [9] and [10]; a belief or set of beliefs [11]; a dispositional variable [9]; a situational variable[12]; a structural variable [13]: a social agency relationship variable [14]; an interpersonal variable [15]; an organizational relationship [16]; a cooperation [17]; and reliability, fairness, and goodwill/benevolence [18].

Another component of trust is reputation. Reputation is perhaps a company's most valuable asset [19]. Trust is subjective while reputation is objective. Both reflect the different aspects of trust.

In this paper we define trust as a relationship between the user entities and service provider entities under the environment of cloud services. Trust makes the user entities are willingness to try using the services and resources provided by the service provider entities and to take a certain risk.

B. Related Theories about Trust Forming Mechanism

Social Exchange Theory (SET)

Social exchange involves the voluntary actions of individuals, which are motivated by the expectation that future returns received from others will be much larger than current costs input. SET explored by Blau [20], therefore, is to explain the phenomena through stating the formation of social contracts between two or more parties, where present social costs are invested in exchange for future, non-guaranteed social rewards.

People form relationships on the basis of trust, especially during initial exchanges according to the SET. It is even the truth on the Internet, where customers

doi: 10.12720/joams.2.2.88-95

typically perceive higher risks compared to conventional shopping environment as a result of long distances, virtual identities, or lack of regulations [21].

Expectation-Confirmation Theory (ECT)

ECT is proposed by Oliver [22] to widely study consumer satisfaction, repurchase intention and behavior. The underlying logic of the ECT framework is: consumers firstly form an initial expectation prior to purchase, and then engender perceptions about its performance after a period of initial consumption. Thus, they may decide the satisfaction level based on the extent to which their expectation is confirmed through assessing the perceived performance vis-à-vis their original expectation. Finally, the satisfied consumers form repurchasing intentions.

Theory of Reasoned Action (TRA)

TRA originated by Fishbein and Ajzen [23] is to analyze the correlation of belief, attitude, intention and behavior. The TRA mainly asserts that beliefs affect the person's attitudes, that is, their favorable or unfavorable evaluations of the others; and attitudes in turn influence behavioral intention, which is a good predictor of actual behavior. In addition, it also supports that the subjective norm concerning the behavior that is the totality of normative pressures coming from the referents who think the person should or should not perform the behavior is an indispensable alternative antecedences of behavioral intention. The normative norm, or normative pressure is mainly derived from external environment.

The above theories are helpful to understand trust formation. It is also a theoretical base of our model construction.

C. Study of Trust Management

Based on the definition of trust in this paper we focus on the trust study between entities under the condition of cloud services. In order to solve the trust problem among strange entities Blaze et al provided the concept of trust management [24]. The trust management is also called the access control based on competence [25]. It could not establish a dynamic trust relationship with strange entities because it requires issuing a credential for users in advance by providers. Li et al provided a simple role-based trust management [26]. It combined with the role-based access control into the trust management. At present, the trust management systems represented by roles describe and deal with trust relationships between entities in an accurate and rational way. It is over-rigorous and difficult to describe the extent of the trust relationship between entities. It is necessary to make it flexible for the balance between security and convenient access and individuation. Beth et al [27] presented a method for the valuation of trustworthiness which can measure the extent of trust in a relative way from the standpoint of the subjective trust and non-rational. This model of the valuation of trustworthiness makes use of the recommendation of similarity entities and themselves experiences to automatically compute the trust degree with the mathematical models. The computing results are used to make the authority decision. This trust negotiation mechanism can be used as an application base in the environment of cloud services.

In summary, the above researches about trust management provide a substantial basis for trust measurement and control. This paper will extend the present research achievements to study the trust evolution process and trends based on the trust degree calculation.

III. A Trust Evolution Model Construction

A. A Trust Evolution Model Discription

There can be differing phases in a trust relationship process such as building trust, a stable trust relationship and declining trust. Trust can be lost quickly: as Nielsen states [28]: "It [trust] is hard to build and easy to lose: a single violation of trust can destroy years of slowly accumulated credibility". During building up trust stage, users provide service requests and access candidates (cloud service providers) through computing trust degrees. The candidate is selected and added to the list of the reliable cloud service providers when the trust value is more than the threshold that the user had set up in advance. In the same time, cloud service providers also access users with the same way. As long as the user and the provider all satisfied a trust relationship has been established. That means they have a trade relationship. After that the trust enters a development stage. During this stage the user and the provider continue to access if their trust degrees are more than their setting the thresholds in service quality, use behavior, and the degrees of satisfaction after every deal. If satisfaction the trust relationship maintains and continues to trade, otherwise trust declines and enters demise as shown in Fig. 1.

B. Trust Degree Computation

The key issue is to calculate the trust degree in the trust evolution model. Trust degree computation includes direct trust degree when the user and the provider have trades and indirect trust degree when the user and the provider have no trade.

Direct trust degree is calculated in terms of the degree of trade satisfaction along with the trading volume and the time horizon.

$$TD_{ab} = \sum_{i=1}^{n} C(i) SD_i \cdot \quad (1)$$

where TD_{ab} is the direct trust value and SD_i is the value of the degree of trade satisfaction. Among (1)

$$C(i) = A(i)M(i) = \frac{\sqrt{t_i - t_0}}{\sum_{j=1}^{n} \sqrt{t_j - t_0}} \times \frac{D_i}{\sum_{j=1}^{n} D_j} \times \frac{m_i^2}{\sum_{j=1}^{n} m_j^2} \cdot \quad (2)$$

Indirect trust degree is computed based on the method of the user behavior similarity (UBS). In the sparse data condition the sparse user information results in incorrect computing outcomes with the traditional similarity algorithms (Pearson correlation coefficient). UBS method can effectively solve this problem.

Suppose the cloud trade entity a and the target entity b have n trades. An independent evaluation set is represented by { v_{i1}, v_{i2}, ..., v_{ik}} after ith trade and k means the number of evaluating indicators (in this research k=4). The behavior feature vector of ith trade evaluation is presented by

$$\overline{L_{abi}} = (v_{i1}, v_{i2}, \ldots, v_{ik}), \qquad 1 \le i \le n \tag{3}$$

The total behavior similarity vector can be measured with (2) and (3)

$$\overline{U_{ab}} = (u_1, u_2, \ldots, u_k), \quad u_j = \sum_{j=1}^{n} C(i) v_{ij}, \quad 1 \le i \le n, \quad 1 \le j \le k. \tag{4}$$

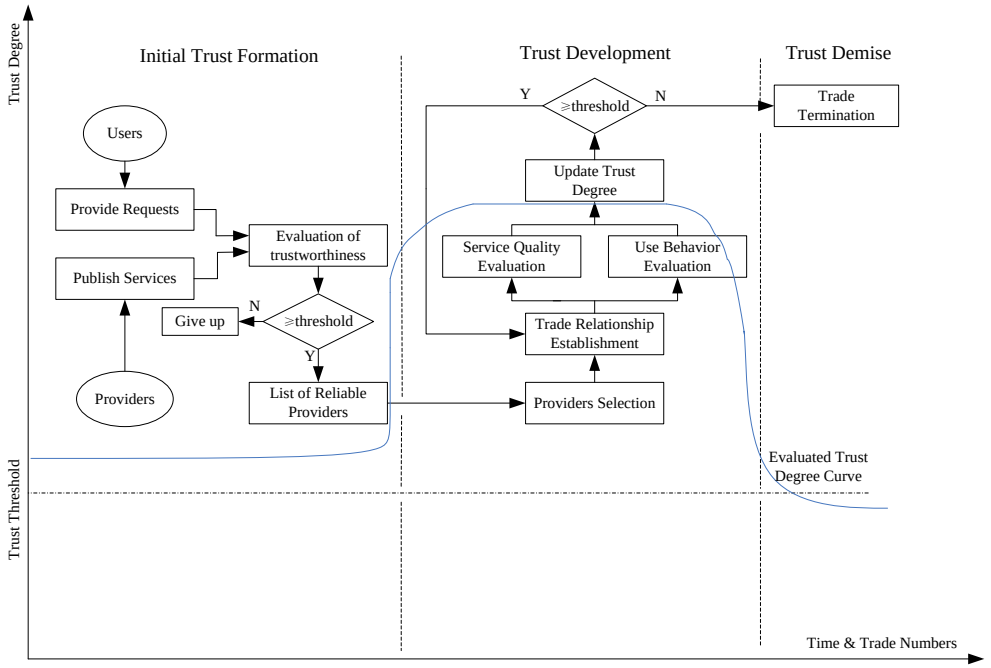

Figure 1. A trust evolution model.

Suppose S_{XY} is the behavior similarity of the trade entity X and Y to the target entity Z.

$$S_{XY} = \frac{\sum_{i=1}^{k} u_{Xi} \times u_{Yi}}{\sqrt{\sum_{i=1}^{k} u_{Xi}^2} \times \sqrt{\sum_{i=1}^{k} u_{Yi}^2}}. \tag{5}$$

When $\sqrt{\sum_{i=1}^{k} u_{Xi}^2} = 0$ or $\sqrt{\sum_{i=1}^{k} u_{Yi}^2} = 0$ define $S_{XY} = 0$.

There are two situations to calculate UBS under the condition of cloud services.

The trade entity a and the target entity b had trades happened.

Define r is the left trade entities except a. $\overrightarrow{U_{a_j b}}$ $(1 \le j \le r)$ is the total behavior similarity vector. The behavior similarity of a and a_j can be calculated based on (4), (5)

$$S_{aa_i} = \frac{\sum_{i=1}^{k} u_{ai} \times u_{aji}}{\sqrt{\sum_{i=1}^{k} u_{ai}^2} \times \sqrt{\sum_{i=1}^{k} u_{aji}^2}}. \tag{6}$$

The trade entity a and the target entity b had no trade record.

In this situation $\overrightarrow{U_{ab}}$ could not be computed. We must select a reference entity whose reputation value (RV) is the greatest among the same entities. Suppose a_l is a reference entity, we define $RV_{a_l} = \max RV_A$. Here A means a class of all the same entities except a. In this way we have

$$S_{aai} = RV_{al} \times S_{alai} = RV_{al} \times \frac{\sum_{i=1}^{k} (u_{ali} \times u_{aji})}{\sqrt{\sum_{i=1}^{k} u_{ali}^2} \times \sqrt{\sum_{i=1}^{k} u_{aji}^2}}. \tag{7}$$

Combined with (1) and (7) the indirect trust degree can be calculated by

$$TI_{ab} = \sum_{i=1}^{r} S_{aa_i} TD_{a_i b}. \tag{8}$$

Finally we can get a total trust degree

$$TC_{ab} = \varepsilon_1 \times TD_{ab} + \varepsilon_2 \times TI_{ab}. \tag{9}$$

where $\varepsilon_1 + \varepsilon_2 = 1$, $\varepsilon_1 \succ \varepsilon_2$, they represent direct trust degree and indirect trust degree weights respectively.

C. The Best Service Provider Selection Algorithm

When a list of the reliable cloud service providers is got the best provider should be chosen. We design an algorithm based on the rule of TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) [29] with the service capacity indicators.

An initial evaluation matrix is constructed in Table I.

TABLE I. AN INITIAL EVALUATION MATRIX

TCS / A	a_1	a_2	a_3	a_4
tcs1	A11	A12	A13	A14
…	…	…	…	…
tcs_m	Am1	Am2	Am3	Am4

A list of the reliable cloud service providers can be represented by a vector TCS={tcs_1,tcs_2,…,tcs_m}, m means the length of the vector. The evaluation indicators is represented by A={a_1,a_2,a_3,a_4}, they represent reliability, bandwidth, cost, and performance respectively [30]-[32].

Constructing the decision matrix with the entropy-weight method

Suppose the decision matrix $R=(r_{ij})_{m\times 4}$ is normal. We have

$$r_{ij}=\frac{a_{ij}}{\sqrt{\sum_{i=1}^{m}a_{ij}^2}},\quad (1\le i\le m,\quad 1\le j\le 4) \tag{10}$$

among them $A=(a_{ij})_{m\times 4}$ acting as the initial decision matrix.

Computing entropy e_j

$$e_j=-k\sum_{i=1}^{m}r_{ij}\ln r_{ij},\qquad (k=1/\ln m,\quad e_j\ge 0)\cdot \tag{11}$$

Computing the divergent coefficient g_j

$$g_j=1-e_j. \tag{12}$$

Computing weights w_j

$$w_j=\frac{g_j}{\sum_{j=1}^{4}g_j}. \tag{13}$$

Constructing the decision matrix $X=(x_{ij})_{m\times 4}$

$$x_{ij}=w_j\times r_{ij},\qquad (1\le i\le m,\quad 1\le j\le 4)\ . \tag{14}$$

Calculating the ideal solution and the negative ideal solution

The best value and the worst value in the decision matrix are used to construct the ideal solution and the negative ideal solution.

$$x_j^+=\max x_{ij},\qquad x_j^-=\min x_{ij},\qquad (1\le i\le m,\quad 1\le j\le 4) \tag{15}$$

Computing the distance measure

The distance measure represents the adjacent extent between the ideal solution and the reliable provider solution. It can be calculated by the Euclid distance.

$$d_i^+=\sqrt{\sum_{j=1}^{4}(x_{ij}-x_j^+)^2},\quad d_i^-=\sqrt{\sum_{j=1}^{4}(x_{ij}-x_j^-)^2},\qquad (1\le i\le m,\quad 1\le j\le 4) \tag{16}$$

Calculating the relative distance measure

Suppose the relative distance measure C_i represent the distance between the candidate solution and the ideal solution. We have

$$C_i=d_i^-/(d_i^-+d_i^+),\qquad (1\le i\le m) \tag{17}$$

Sorting the relative distance measures

Sort the relative distance measures C_i. The biggest value represents the best provider among them.

D. Satisfaction Degree Computation

Satisfaction degree computation includes both the user to the provider and vice versa.

The satisfaction degree of the user to the provider is calculated by the four evaluation indicators.

$$SD_{us}=\sum_{i=1}^{4}w_i\times a_i,\qquad \sum_{i=1}^{4}w_i=1\cdot \tag{18}$$

where w_i is the weight of the a_i indicator.

The satisfaction degree of the provider to the user is calculated by the user use behavior evaluation indicators as shown in Table II.

TABLE II. THE USE BEHAVIOR EVALUATION INDICATORS

Indicators	Standard	Values
b_1: Operation Normalization	Violating Rule Times	0～5
b_2: Contract Compliance	Grading	0～5
b_3: Payment On Time	Grading	0～5

$$SD_{su}\sum_{i=1}^{3}b_i,\qquad (0\le b_i\le 5,\quad i=1,2,3) \tag{19}$$

E. Dynamic Update of Trust Degree and Reputation Degree

Trust degree and reputation degree are dynamic change with the trade increase in the environment of cloud services. We adopt an increment update method. When satisfaction degree SD is less than the set threshold ST, a punishment function P is added to calculate the increment of trust degree ΔTV.

$$\Delta TV=[(SD-ST)/SD_{\max}]\times TV\times(m/m_{av})+P \tag{20}$$

where TV is the trust degree, m is the trade volume, and m_{av} is the average value of all the trade volumes.

$$P=f\times[1/(l+e^{-h})] \tag{21}$$

where f=0 if the trade is successful; f=1 otherwise. $1/(l+e^{-h})$ is the accelerating factor; h is the amount of the trade failures and l is the number related the trade volume.

The trust degree update formula is

$$TV_{i+1}=TV_i+\Delta TV\qquad i=1,2,\cdots,n \tag{22}$$

Similarly the reputation degree update formula is

$$RV_{i+1} = RV_i + \Delta RV \qquad i = 1,2,\cdots,n \tag{23}$$

IV. Simulation Results and Analysis

A. Indicators and Parameters Selection

We set up three indicators to measure the trust evolution based on the related researches [33].

Proposition 1 An average trust density ρ of the trust system equals to

$$\rho = \sum_{i \in Node} RV / n \tag{24}$$

where $Node = \{e_i \mid 1 \le i \le n\}$, n means the trade number of times. ρ represents the trust level of the system.

Proposition 2 A collaboration success ratio θ equals to

$$\theta = S / n \times 100\% \tag{25}$$

where S is the number of the trade success. θ reflects the reliability of the trust evolution model.

Proposition 3 An average trust value $\overline{TV}$ of the cloud service provider equals to

$$\overline{TV} = \sum_{TV_{ik} \in R} TV_{ik} / N \tag{26}$$

where the user class is $N_{CU} = \{CU_i \mid 1 \le i \le N\}$(N is the number of the users), the cloud service provider set is $N_{CS} = \{CS_k \mid 1 \le i \le M\}$ (M is the number of the providers), the trust relationship set is $R = \{(CS_k, CU_i, TV_{ik}) \mid CU_i \in N_{CU}, CS_k \in N_{CS}\}$. $\overline{TV}$ reflects the variation trend of the trust relationship of the provider.

TABLE III. The Classification of the Providers and Users

Entities	Service promise/ assignment	Promise performing/ assignment
CS_1	high/high initial trust degree	good/high evaluation value
CS_2	high/high initial trust degree	poor/low evaluation value
CS_3	low/low initial trust degree	good/high evaluation value
CS_4	low/low initial trust degree	poor/low evaluation value
CU_A	High quality	
CU_B	Low quality	

Before simulation it is necessary to classify the providers and users (to see Table III).

B. Simulation Results

Two kinds of simulation were carried out in this study on the Netlogo platform based on the principle of the multi-agent simulation. One is to verify the reliability of the trust evolution model. The other is to explore the trust evolution development trends with the model. The entities of providers and users are represented by agents. The trade between agents is simulated by the interaction of agents.

Before simulation the initial parameters had been set up as shown in Table IV after many trials.

TABLE IV. The Initial Parameters

Parameters	Assignment	Parameters	Assignment
M	3	Wgt. of reliability	0.1
N	50		
Trust thr.	0.50	Wgt. of bandwidth	0.3
Satisfaction thr.	0.50		
Ratio of baleful nodes	10%, 20%, 30%, 40%	Wgt. of cost	0.4
		Wgt. of performance	0.2
		No. of trades	2000

pro. = providers; thr. = threshold; wgt.=weight

where the ratio of baleful nodes means the ratio of CU_B in all the users.

The simulation results are show in Fig. 2 to Fig. 9.

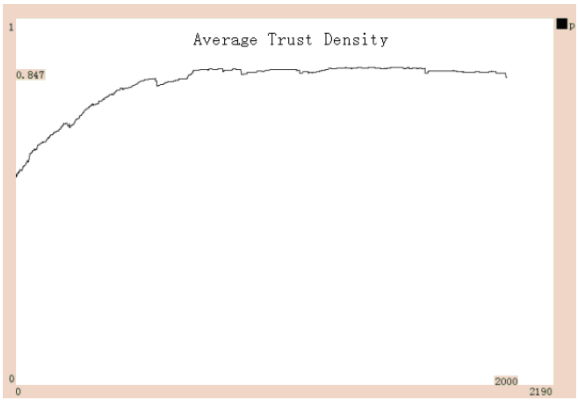

Figure 2. ρ change trend in 10% baleful nodes

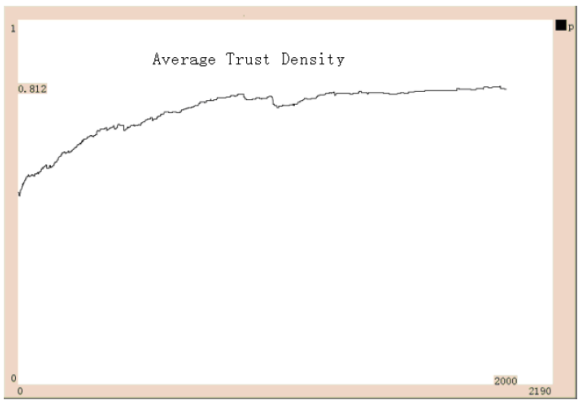

Figure 3. ρ change trend in 20% baleful nodes

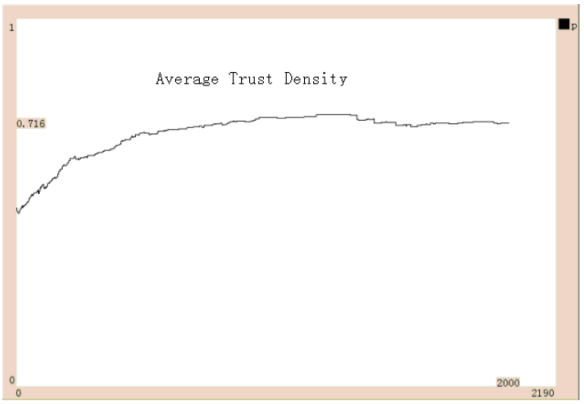

Figure 4. ρ change trend in 30% baleful nodes

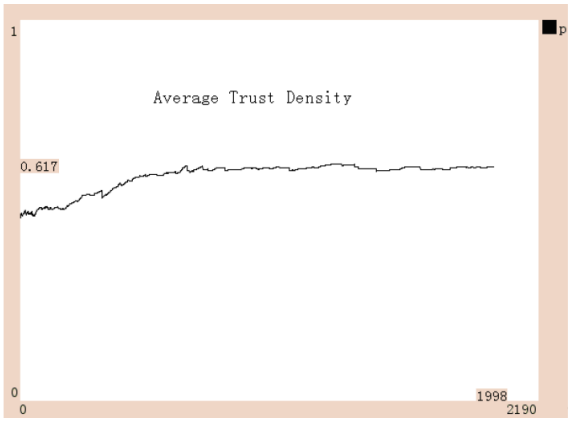

Figure 5. ρ change trend in 40% baleful nodes

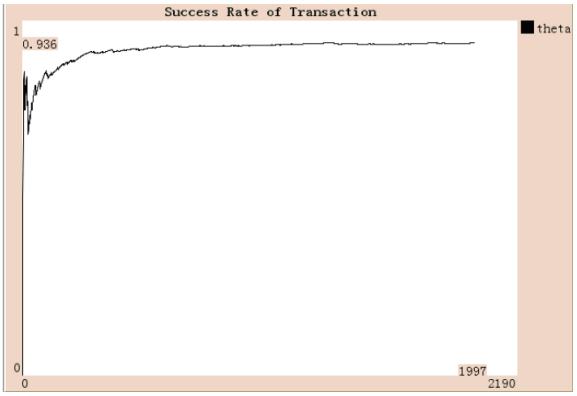

Figure 6. θ change trend in 10% baleful nodes

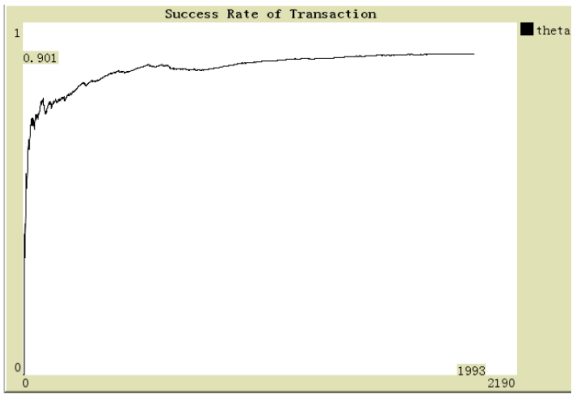

Figure 7. θ change trend in 20% baleful nodes

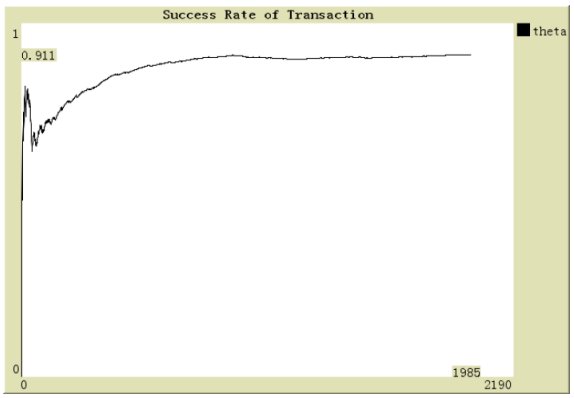

Figure 8. θ change trend in 30% baleful nodes

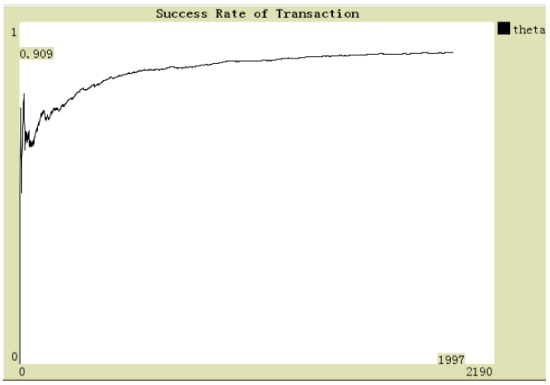

Figure 9. θ change trend in 40% baleful nodes

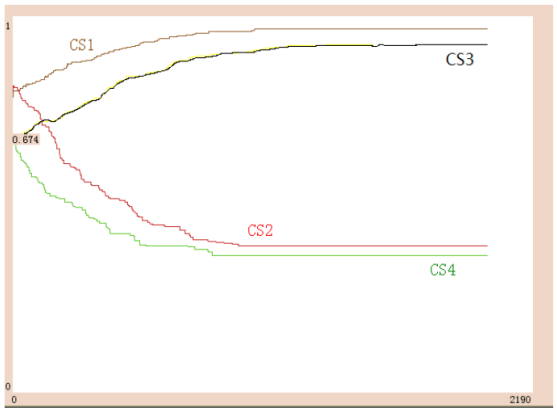

Figure 10. $\overline{TV}$ change trend in 10% baleful nodes

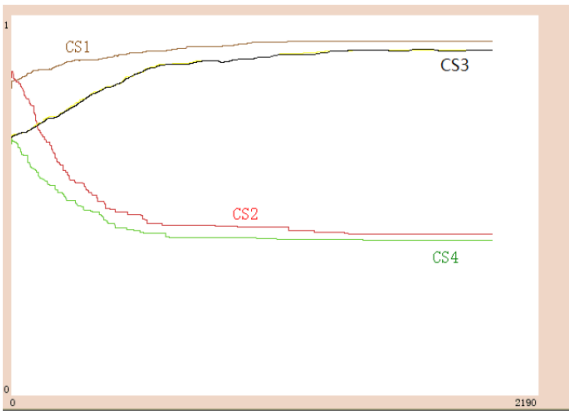

Figure 11. $\overline{TV}$ change trend in 20% baleful nodes

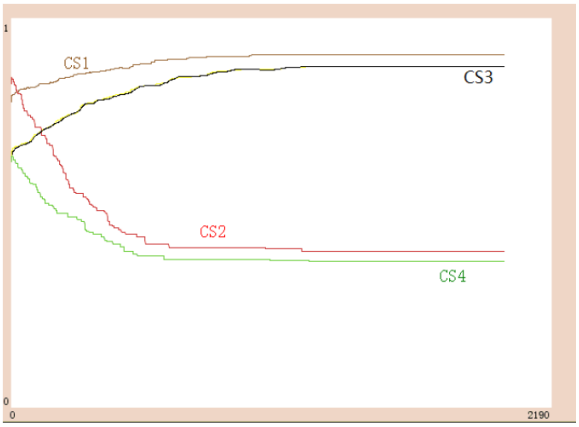

Figure 12. $\overline{TV}$ change trend in 30% baleful nodes

In order to explore the evolution trends of trust four kinds of providers were set up (to see Table III) to conduct four times of simulation with the four different baleful nodes respectively. The simulation results are show in Fig. 10 to Fig. 13.

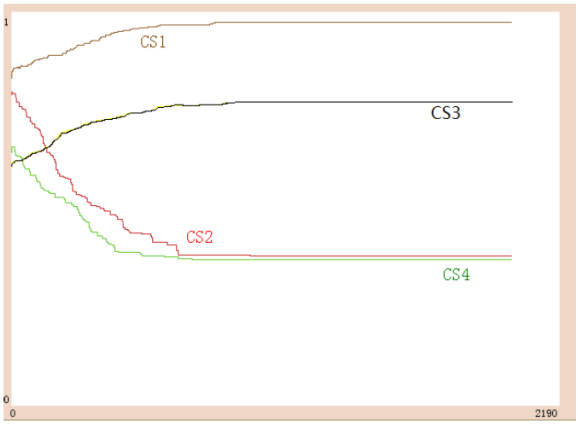

Figure 13. $\overline{TV}$ change trend in 40% baleful nodes

C. Simulation Results Analysis

We found that the average trust density ρ is more than 80% when the ratio of baleful nodes is less than 20% from the Fig. 2 and Fig. 3. This result proved that the simulation model we designed is more reliable than other dynamic trust models. With the increase of the ratio of the baleful nodes ρ has the lower value from the start (to see Fig. 4 and Fig. 5). However with the increase of trade number of times ρ goes up gradually and keeps stable finally. It also indicates our model is very reliable.

θ has the same change trends no matter the ratios of baleful nodes are different or not. It is because a punishment function P is added in our trust model to ensure a high trade successful ratio when the worst users are eliminated.

Four experiments have been done with the four different ratios of baleful nodes (that means CU_B ratio), 10%, 20%, 30%, and 40% respectively from Fig. 10 to Fig. 13. The CS_1 and CS_2 have the same initial trust degrees but the development trends are dramatically different with the increase of the trade number of times. The trust degree of CS_2 goes down quickly to a lower level but the trust degree of CS_1 goes up to a higher level because of the different promise performing. Although CS_3 has the lower initial trust degree its average trust value goes up stably because of good promise performing. Distinctly, the average trust value of CS_4 goes down gradually because of its low initial trust degree and poor promise performing.

V. Conclusions and Discussions

A. Conclusions

The paper describes a mutual assessment trust evolution model based on the theory of interpersonal society trust relationship and cloud service characteristics. The model has been verified by simulation. Simulation results proved that the model is reliable and effective. It provides a novel reference model for solving cloud service security issue.

The main contributions of the paper include putting forward the concept of the mutual assessment between trustors and trustees under the condition of cloud services; constructing a dynamic evolution model with the increase of the trade number of times based on the characteristics of cloud services; designing a set of algorithms to measure the trust degree and the reputation degree in terms of the theory of interpersonal society trust relationship and the theory of the behavior similarity; verifying the reliability and correctness of the model and algorithms through simulations; the simulation results can be used to specify the behavior of the providers and users to maintain a longer trust relationship.

B. Discussions

The model and the simulation results indicate: the trust relationship is mutual. Both cloud services providers and users' behavior all influence the variation of the trust values; in order to maintain a higher trust degree both sides of the cloud services must present good behavior; a punishment must be given when the trade is failure. In addition the trade time and volume also must be considered.

The future study will focus on two aspects. One is to revise and extend the model itself to make it adapt to more general situations. The other is experiment design and parameters selection, such as the punishing function design, the assignment of the initial trust degree, and so on must be considered carefully and experimentally.

References

[1] P. Mell and T. Grance, The NIST Definition of Cloud Computing, NIST Special Publication 800-145, National Institute of Standards and Technology (NIST), September, 2011.
[2] C. Baun, M. Kunze, J. Nimis, and S. Tai, *Cloud Computing: Web-Based, Dynamic IT Services*, Heidelberg, Germany: Springer, 2011, ch. 1, pp. 1.
[3] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011.
[4] P. G. Dorey and A. Leite, "Commentary: Cloud computing - A security problem or solution?" *Information Security Technical Report*, vol. 16, pp. 89-96, Aug-Nov 2011.
[5] D. Rousseau, S. Sitkin, R. Burt, and C. Camerer, "Not so different after all: A cross-discipline view of trust," *Academy of Management Review*, vol. 23, no. 3, pp. 393-404, 1998.
[6] D. E. Zand, "Trust and managerial problem solving," *Administrative Science Quarterly*, vol. 17, no. 2, pp. 229-239, 1972.
[7] D. L. Kegan and A. H. Rubenstein, "Trust, effectiveness, and organizational development: A field study in R&D," *Journal of Applied Behavioral Science*, vol. 9, no. 4, pp. 495-513, 1973.
[8] A. K. Cohen, *Deviance and Contro*l, Englewood Cliffs, NJ: Prentice-Hall, 1966, ch. 1, pp. 3.
[9] J. B. Rotter, "Interpersonal trust, trustworthiness, and gullibility," *American Psychologist*, vol. 35, no. 1, pp. 1-7, 1980.
[10] J. Scanzoni, "Social exchange and behavioral interdependence," in *Social Exchange in Developing Relationships*, R. L. Burgess & T. L. Huston Ed., New York: Academic Press, 1979, pp. 61-98.
[11] B. Barber, *The Logic and Limits of Trust*, New Brunswick, NJ: Rutgers University Press, 1983, ch. 1, pp. 2.
[12] C. Johnson-George and W. C. Swap, "Measurement of specific interpersonal trust: Construction and validation of a scale to assess trust in a specific other," *Journal of Personality and Social Psychology*, vol. 43, no. 6, pp. 1306-1317, 1982.

[13] J. D. Lewis and A. J. Weigert, "Trust as a social reality," *Social Forces*, vol. 63, no. 4, pp. 967-985, 1985.
[14] S. P. Shapiro, "The social control of impersonal trust," *American Journal of Sociology*, vol. 93, no. 3, pp. 623-658, 1987.
[15] J. K. Rempel, J. G. Holmes, and M. P. Zanna, "Trust in close relationships," *Journal of Personality and Social Psychology*, vol. 49, no. 1, pp. 95-112, 1985.
[16] R. Mayer, J. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Academy of Management Review*. vol. 20, no. 3, pp. 709-734, 1995.
[17] D. Gambetta, "Can we trust?" in *Trust: Making and Breaking Cooperative Relations*, D. Gambetta Ed. electronic edition, Department of Sociology, University of Oxford, 2000, ch. 13, pp. 213-237.
[18] J. H. Dyer and W. Chu, "The role of trustworthiness in reducing transaction costs and improving performance: Empirical evidence from the United States, Japan, and Korea," *Organization Science*, vol. 14, no. 3, pp. 57-68, 2003.
[19] H. Nissenbaum, "Can trust be secured online? A theoretical perspective," *Eticae Politica*, no. 2, Dec 1999.
[20] P. Blau, *Exchange and Power in Social Life*, Wiley, New York, 1964, ch. 1, pp. 4.
[21] R. L. Oliver, "A cognitive model of the antecedents and consequences of satisfaction decisions," *Journal of Marketing Research*, vol. 17, no. 4, pp. 460-469, November 1980.
[22] S. J. Tan, "Strategies for reducing customer's risk aversion and internet shopping," *Journal of Consumer Marketing*, vol. 16, no. 2, pp. 163–180, 1999.
[23] M. Fishbein and I. Ajzen, *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, Reading, MA: Addison-Wesley, 1975, ch. 1, pp. 5.
[24] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," in *Proc. IEEE Symp. on Security and Privacy*, Washington, IEEE Computer Society Press, 1996, pp. 164−173.
[25] W. H. Winsborough, K. E. Seamons, and V. E. Jones, "Automated trust negotiation," in *Proc. DARPA Information Survivability Conf. and Exposition*, S. C. Hilton Ed. New York: IEEE Press, 2000, pp. 88-102.
[26] N. H. Li, W. H. Winsborough, and J. C. Mitchell, "Distributed credential chain discovery in trust management," *Journal of Computer Security*, vol. 1, no. 11, pp. 35-86, 2003.
[27] T. Beth, M. Borcherding, and B. Klein, "Valuation of trust in open networks," in *Proc. 3rd European Symposium on Research in Computer Security*, London, UK: Springer-Verlag, 1994, pp. 3-18.
[28] J. Nielsen. (1999). Trust or bust: Communicating trustworthiness in web design, Jacob Nielsen's Alertbox. [Online]. Available: http://www.useit.com/alertbox/990307.html.
[29] D. L. Olson "Comparison of weights in TOPSIS models," *Mathematical and Computer Modeling*, vol. 40, pp. 721-727, October 2004.
[30] J. Hassan, L. X. Hung, U. Kalim, A. Asjjad, S. Y. Lee, and Y. K. Lee, "A trust model for ubiquitous systems based on vectors of trust values," in *Proc. 7th IEEE Int'l Sump on Multimedia*, Washington: IEEE Computer Society Press, 2005, pp. 674−679.
[31] R. He, J. W. Niu, and G. W. Zhang. "CBTM: A trust model with uncertainty quantification and reasoning for pervasive computing," *Parallel and Distributed Processing and Applications*, vol. 3758, pp. 541−552, 2005.
[32] W. J. Li and L. D. Ping. "Trust model to enhance security and interoperability of cloud environment," *Cloud Computing*, vol. 5931, pp. 69–79, 2009.
[33] S. Marsh, "Formalizing trust as a computational concept," Ph.D. dissertation, Dept. Computing Science and Mathematics, University of Stirling, Scotland, UK, 1994.

Y. J. Zhou is a Professor of Industrial Engineering at the Nanjing University, P. R. China. He was born in Oct. 1958 in Nanjing City, Jiangsu, P. R. China. He got his Ph.D. from the City University of Hong Kong in 2002.

He has over 28 years working and research experience. He conducted a post-doctoral research at Florida Atlantic University, U.S.A. during 2000-2002. He is the author of 5 books and over 70 journal and international conference papers. Articles published in the International Journal of Manufacturing Technology Management, the International Journal of Industrial Ergonomics, the International Journal of Operations and Production Management, the International Journal of Advanced Manufacturing Technology, and so on. His previous research focused on Computer Integrated Manufacturing. His present interest research areas including cloud service supply chain management, management information systems, and logistics and supply chain management.

Prof. Zhou is a senior member of Chinese Mechanical Engineering Society and a fellow of Chinese Industrial Engineering Institution. He was awarded a second prize and a third prize of the minister's science and technology.

