Evaluating Mechanism Trust Model Based on Behavior Result under Cloud Computing

Lanying Huang , Zenggang Xiong , guangwei Wang

School of Computer and Information Science, Hubei Engineering University, Xiaogan ,Hubei,China

***Abstract* — An evaluating mechanism-based cloud computing trust model is raised to aim at the issue of how the cloud service user selects credible cloud service supplier. The trust model constitutes an evaluating system about service behavior between cloud service supplier and cloud service user. After formalized evaluation about entity achieved, certain algorithm would be used to get the trust and trust value of an entity to another one, and the research about the above trust value could be used to solve the issue of trust between cloud service user and cloud service supplier. Secondary, in order to settle the problem, e.g. the unreal and vicious entity which is trusted in the trust model, a trust management measure is formed based on curve fitting. The measure could help determine truth degree and accuracy degree of trust value after dynamic analysis and judgment and analyze the behavior intent of entity for the purpose to assure accuracy and stability of trust model. The simulation result shows that the evaluation result of the model is more close to real credibility and cloud service supplier, at the same time, could effective resist the attack from the vicious cloud service user, assure safety of cloud service environment and help improve cloud service quality.**

Keywords - information security; cloud computing; evaluation mechanism; user behavior

I. INTRODUCTION

The progress in the fields of computer software and hardware and communication technology contributes a new computing model, i.e. cloud computing. By cloud computing, the people could enjoy a variety of cloud services which call for cloud computing management center to provide effective security mechanism by which the supplier and user of cloud service is safe. In 1996, in order to settle the issue of security for Internet service, M.Blaze and others [1] for the first time used the concept of Trust Management to connect the research on trust model with the research field of distributed system. Following the initiation by M.Blaze and others, A.Adbul-Rahman and others[2-3] introduced the mathematic mode which functions measuring trust. Since then, the trust model was widely studied by the scholar home and abroad in the field of computer. As an effective traditional solution for security of network service, the trust mechanism has been popularly applied to the distributed computing, e.g. grid computing and pervasive computing, etc. However, the current trust model is not perfect. It consists of four branches with respective shortcoming:

(1)Probability-based trust model [4-6], where probability is used to describe trust value and at the same time, trust has two divisions of direct one and indirect one. The probability of the entity able to fulfil the task would be achieved by computing based on positive and negative experience. Then, the probability achieved would be used to measure credibility of entity. At the same time, what could be given includes computation formula for credibility derivation and synthesis given by experience recommendation. However, the model fails in defining concrete impact factors for trust and default status of trust, etc.

(2) Fuzzy logic-based trust model [7-9], where the trust level existent in entities could be expressed as more than one fuzzy subset in relevant domain. For example, fuzzy subsets, T1, T2, T3 and T4, could be respectively used to express “Absolute trust”, “General trust”, “Critical trust” and “Distrust”. The degree of membership is calculated of certain entity to each fuzzy subset. The vector of degree of membership is used to mean trust value of entity. Such a fuzzy logic-based representation method for trust valuve is able to solve the exclusion relation wich features one or the other and better work out the fuzziness issue for the trust. Its shortcoming mainly lies in the fact that relatively less consideration is paid to time variability of entity behavior and computing of indirect trust valuve is not taken into account, etc.

(3)Entropy theory-based trust model [10-12], it reflects trust expression with cloud model on the base of trust relation and characteristic of descriptive approach, with the form of one triple (Ex,En,He) wherein Ex means basic trust degree, En uncertainty of trust relation, He uncertainty of trust entropy. Its shortcoming is no building concrete mathematic model, which means study is difficult to be launched. Meanwhile, its definition about behavior is also fuzzy, lack of flexibility.

(4)Evidence theory-based trust model [13-15], it divides trust degree into “credible degree”, “not-credible degree” and “uncertain degree”. It uses basic trust function of the evidence theory to express three trust degrees. Then, the study on the influence of each element of trust to trust could effectively resolve the issue in the probability-based trust model that it only express trusted binary relation and fails in expressing trust-uncertain relation. Its shortcoming is mainly that it is unable to grasp behavior course of trust and only judge and execute trust decision-making from the angle of trust result, and meanwhile, it lacks dynamics.

In conclusion, though the trust model could assure security of cloud computing, when an entity in cloud service faces such issues as poor service quality, unreal service and vicious service, how to judge and recognize these conditions, how to assure security of cloud computing, especially in the course of service, and how to assure the accuracy and reliability of the trust generated by the cloud entity in the trust model would become the hotspot and difficulty of the cloud security field and also one study focus for the trust model.

On the base of the above discussion about the weakness of a variety of trust models, e.g. lack of dynamics, lack of concrete mathematic model, lack of study on behavior course and result, lack of comprehensive validation to behavior and identity, the paper puts forward to a trust model based on mutual evaluation between service entity and request entity, which resolves the issue of the trust to behavior course, behavior result and identity validation; the model introduces trust management which is of curve fitting to dynamically analyze and judge truth degree and accuracy degree of trust valuve, solve the dynamics of the trust model against cloud computing, update and judge trust in order to assure accuracy and reliability of trust model.

II. RELEVANT THEORY AND KNOWLEDGE

A. Classification of trust

In the literatures [16-18], from the ange of entity, trust has three divisions, i.e. Identity validation-based trust, behavior result-based trust and behavior course-based trust (Fig.1).

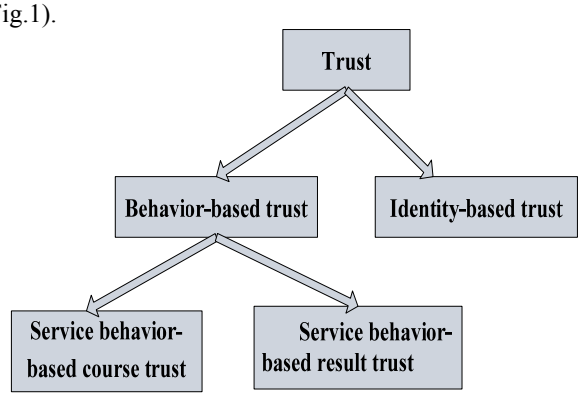

Fig.1 Classification of trust

Identity-based trust validation mechanism lacks real understanding and mastering of entity condition, which is easy to cause trust cheating problem present among entities. Behavior-based trust mechanism could effectively eliminate the problem of trust defect present in identity-based trust. However, an effective trust recording and trust updating strategy is necessary to match the dynamic evolution of the trust relation. The service behavior-based trust is such a trust mechanism as depends on service course. A variety of network behaviors exercised by the entity could be used to judge whether the entity is credible. Such a form of trust could make a kind of relation formed between entities via behavior course. Each service would generate such a trust relation as only aims at the service. Such a form of trust features independence and no needing entity trust initialization course. On the other hand, it is unable to update the trust generated by the service behavior result, too much relies on network behavior and lacks accuracy; in the course of behavior result-based trust trust dependence service, the information about the service behavior result generated by the entity could be used to judge whether the entity is credible. Such form of trust could make a relation directly formed between entities via service behavior result. Each service has its continuity. Because it depends on result of historic service to judge entity credibility, such a form of trust is of totality and able to depend on result of service behavior to accordingly update the trust.

B. Evaluation mechanism

Evaluation mechanism is a kind of behavior concept which could be understood as a kind of cognition and description about certain relation between the entity which performs the function of evaluating and the entity which is evaluated. The evaluation mechanism includes content, standard and method, etc. Evaluating means judging and cognizing risk and security. Trust in the trust model means a kind of description about entity-entity relation. Therefore, it is feasible to connect trust model with evaluation mechanism [11].

The evaluation mechanism studied in the paper is such an evaluation as based on service behavior result. Trust would be formed by evaluation, as shown as Fig.2.

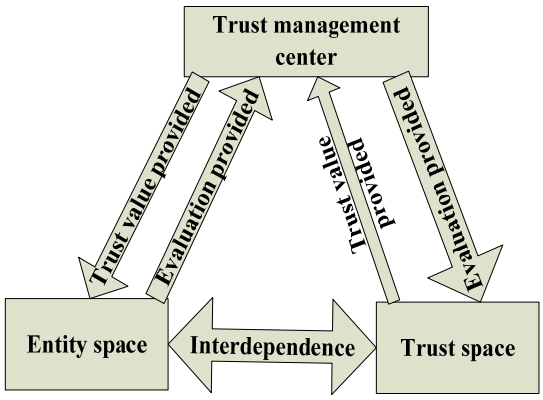

Fig.2 Trust and evaluation mechanism

Such an evaluation mechanism-based trust model would judge the trust value of two parties in order to decide whether current trust degree of two parties is suitable for service once before the service starts. Such an arrangement eliminates the issue of identity judgment in identity-based trust; in the course of service, trust model collects service experience of entity and express the service experience with digital form of evaluation. So, the entity could control the course of the service applied to two entities by controlling the evaluation. User experience plus conclusion about practice course would form evaluation, which solves the

issue of whether behavior course-based entity is credible; meanwhile, after service termination, trust model would follow two kinds of trust management mechanisms which are different to judge authenticity of current trust evaluation for the purpose to control truth degree of trust and avoid unreal trust.

III. EVALUATION MECHANISM-BASED TRUST MODEL UNDER CLOUD COMPUTING ENVIRONMENT

A. *Framework of evaluation mechanism-based trust model*

Evaluation mechanism-based trust model present in the paper (Fig.3) is such a kind of evaluation as based on service behavior result. The trust model consists of entity space, i.e. request entity, service entity, evaluation space, trust space and trust management center. Trust management center is core of trust model.

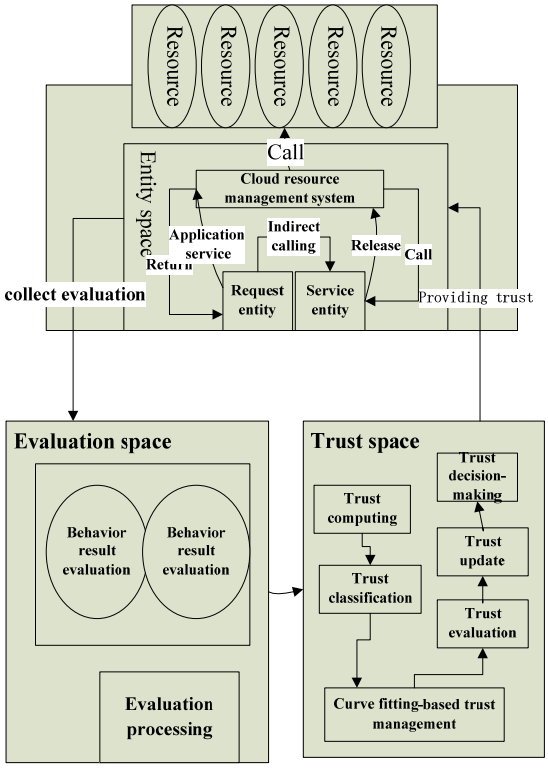

Fig.3 Evaluation mechanism-based trust model

Fig.3 basically illustrates its working principle. The relation among three entities briefed as follows: Rrequest entity and service entity respectively submit evaluation to trust management center; and trust management center translates evaluation value into trust value and meanwhile effectively judges trust value. If trust value meets requirement, it would be listed in trust space. After new addition comes here, new trust space would be under dynamic management and update; at the same time, when request entity and service entity perform their function of service, trust management center would provide two parties direct or indirect trust value of entity. After service terimination, entity space would deliver trust and evaluation to trust management center. Continual interaction and update makes trust model gradually optimized and approach to self-management.

B. *Formalized definition of trust evaluation model*

Definition 1: Abstract request entity as U = {U_1, U_2, …U_n}, and abstract service entity as S = {S_1, S_2, …S_n}. Define behavior between request entity and service entity as (U_i , S_j), and define service manager entity as *K*.

Definition 2: Define service evaluation E. After termination of each service behavior, generate a service evaluation E. Herein, service evaluation contains evaluation of request entity $E(U_i , S_j)$ and evaluation of service entity $E_s(U_i , S_j)$. And evaluation of request entity and evaluation of service entity respectively contain different parameter, with following formalized expression:

$$(U_i , S_j) = \{E|E_u(U_i , S_j), E_s(U_i , S_j)\} \quad (1)$$

$$E(U_i , S_j) = (t, q_u, v_u , p_u, T_s, T_e) \ \ q_u, v_u , p_u \in [0, 1] \quad (2)$$

Wherein, t means time spent by service behavior, and T_s and T_e respectively means description given by request entity about service quality; $v_u$means description given by request entity about truth degree of service; p_u means evaluation given by request entity about service behavior.

Definition 3: Relevant factors in trust model is expressed as follows: Rule for trust decision-making, Update for trust update; Visit for access; Get for resource acquisition; and Refuse for resource request rejected. Then, there is the following expression about whether the condition of the request entity is met or not in the course of service.

When trust value is in trust decision-making, service request given out by request entity is met:

$$(P(U_i , S_j) \in Rule) \rightarrow (Visi(U_i, K) \wedge Get(U_i , K, S_j) \wedge Update(U_i , S_j\, j) \quad (3)$$

When trust value is not in trust decision-making, service request given out by request entity is not met and condition to reject is returned.

$$(P(U_i , S_j) \notin Rule) \rightarrow (NotVisit(U_i , K) \wedge NotGe(U_i , K, S_j) \wedge Refuse(U_i , S_j) \quad (4)$$

Definition 4: Classification of trust relation. The trust relation among entities has two divisions, direct trust and recommended trust (indirect trust). Direct trust means direct service relation once present between two entities. Therefore, a direct trust relation has been formed between both. trust degree comes from direct experience formed for historic transaction between two parites. Recommended trust means there is no direct service provision and service

reception between two entities and is such a trust relation formed based on recommendation by other entity.

Definition 5: The trust value is defined as *T*. For convenient study, define trust degree between two entities as a numerical value between 0 and 1, which makes it possible to use probability theory to compute trust value. Therefore, $T \in [0, 1]$. Then, there are various trust degrees respectively for different request entity and service entity in trust space TS in cloud computing model. These trust degrees constitute space for trust degree TD.

Definition 6: Trust rating is defined. The trust rating is subject to two factors: trust value of each trust level and number of service under trust level. The paper gives three levels to service trust space TS, wherein, TS = {"Not credible", "Relatively credible", "Absolutely credible"}. In the paper, the trust value respectively for Not credible and Absolutely credible is set up as [0.3，0.75], which means such a service with a trust value below 0.3 would be not credible, and that with a trust value would be absolutely credible.

Definition 7: Weight of evaluation value is defined. Because the parameter respectively in evaluation of request entity and service entity is of different importance, a weight parameter is defined to determine computing method for the parameter. The weight means its proportion in behavior evaluation for entity, i.e. Importance of each factor. It is feasible to use each parameter and weight to compute trust value generated by service behavior.

For request entity, its weight parameter set is:

$$\alpha=\{\alpha_1,\alpha_2,\alpha_3\ldots\alpha_i\} \quad i\in Z\ ; \tag{5}$$

For service entity, its weight parameter set is:

$$\beta=\{\beta1,\beta2,\beta3\ \ldots\beta i\} \quad i\in Z\ ; \tag{6}$$

Definition 8: Method to compute how to convert evaluation value into trust value. Trust value is a kind of formalized and numerical method to express the trust. In the evaluation mechanism-based trust model, the combination of evaluation factor and weight is used to acquire trust value. For an evaluation $E_u(U_i\ ,\ S_j) = (t,\ q_u,\ v_u\ ,\ p_u,\ T_s,\ T_e)$ and $\alpha=\alpha\{\alpha_1,\alpha_2,\alpha_3\ldots\alpha_i\}$, trust value $T(U_i\ ,\ S_j)$ means the trust value of the evaluation made by the request entity U_i*S*to the service entity $S_j$and, trust value $T(S_j,\ U_i)$ means the trust value of the evaluation made by the service entity $S_j$to the request entity Ui.

$$(U_i\ ,\ S_j)=q_u\cdot\alpha_1+\ v_u\cdot\alpha_2+\ p_u\cdot\alpha_3 \tag{7}$$

$$(S_j,\ U_i)=p_s\cdot\beta_1 \tag{8}$$

Wherein, the evaluation to all the trust values in one entity $S_j$is kept in the trust value set *T* of S_j, with $TT=\{T(U_k,\ S_j)|k=1,2,3,\ldots\ldots\}$, which means all the evaluations to the entity S_j.

Definition 9: Computing method for direct and indirect trust value. The trust relation between entities has two types, direct trust and recommended trust (indirect trust). The difference between both is whether there is service behavior present between entities. Define the trust relation between service entity and request entity *R* as follows.

$R(U_i\ ,\ S_j)$ includes trust relation between entities and mutual evaluation between request entity $U_i$and service entity S_j, i.e. $T(U_i\ ,\ S_j)$,$T(S_j,\ U_i)$，and direct trust value $DT(U_i\ ,\ S_j)$,$DT(S_j,\ U_i)$ given by request entity $U_i$to service entity S_j, and indirect trust value $IT(U_i\ ,\ S_j)$,$IT(S_j,\ U_i)$ given by request entity U_i to service entity S_j:

$$R(U_i\ ,\ S_j)= (T(U_i\ ,\ S_j),T(S_j,\ U_i),DT(U_i\ ,\ S_j),DT(S_j,\ U_i),IT(U_i\ ,\ S_j),IT(S_j,\ U_i)) \tag{9}$$

If there is service behavior once present between certain request entity and service entity, it would be available to compute the trust value of the historic service once present between both to get the direct trust value. The direct trust value given by the request entity U_i to the service entitySS_j is expressed as $DT(U_i\ ,\ S_j)$,which is the mean value of all the historic trust values given by equest entity U_i to the service entityS_j, expressed as follows:

$$D(U_i\ ,\ S_j)=(T_1(U_i\ ,\ S_j)+ T_2(U_i\ ,\ S_j)+\cdots+Tn(U_i\ ,\ S_j))/n \tag{10}$$

Wherein, $T_1(U_i\ ,\ S_j)$，$T_2(U_i\ ,\ S_j)$ and others respectively mean once evaluation made by request entity $U_i$to service entity S_j , *n* meaning evaluation total.

If there is no service behavior present between certain request entity and service entity, there would be no trust evaluation made by request entity to service entity in the truststore. Thus, it is necessary to get an indirect cognition to the service entity with the evaluation to the historic trust value of the current entity given by other entity. The above indirect cognition could be expressed as indirect trust value of service entity. The indirect trust value of the service entity $S_j$as expressed as $I(S_j)$，which is mean value of all the trust evaluations given to the service entityS_j expressed as:

$$IT(U_i\ ,\ S_j)=(\sum_{n=1}^{a} T_n(U_1,S_j) + \sum_{n=1}^{a} T_n(U_2,S_j +\cdots+ \sum_{n=1}^{a} T_n(U_n,S_j)/total \tag{11}$$

Where in $\sum_{n=1}^{a} T_n(U_1,S_j)$ means the set of the evaluations made by the request entity U_1 to the service entity S_j, and $total$ means the total of all the evaluations given to the service entity S_j.

C. Flow to judge and achieve trust value

The evaluation mechanism trust model in Fig.3 is based on direct and indirect trust acquisition. Trust acquisition

consists of two sections, trust generation and trust extraction. Trust generation is such a course where trust is generated by evaluation. In the course, trust, which is an nonobjective concept, could be quantified by formalized trust value converted; the extraction section of the trust, at the stage where the actual trust of each entity is acquired, could depend on whether the direct trust relation is available to determine whether the direct trust value is available. If yes, it would be adopted; if not, it would depend on other trust value in the truststore to get the indirect trust value of the current entity.

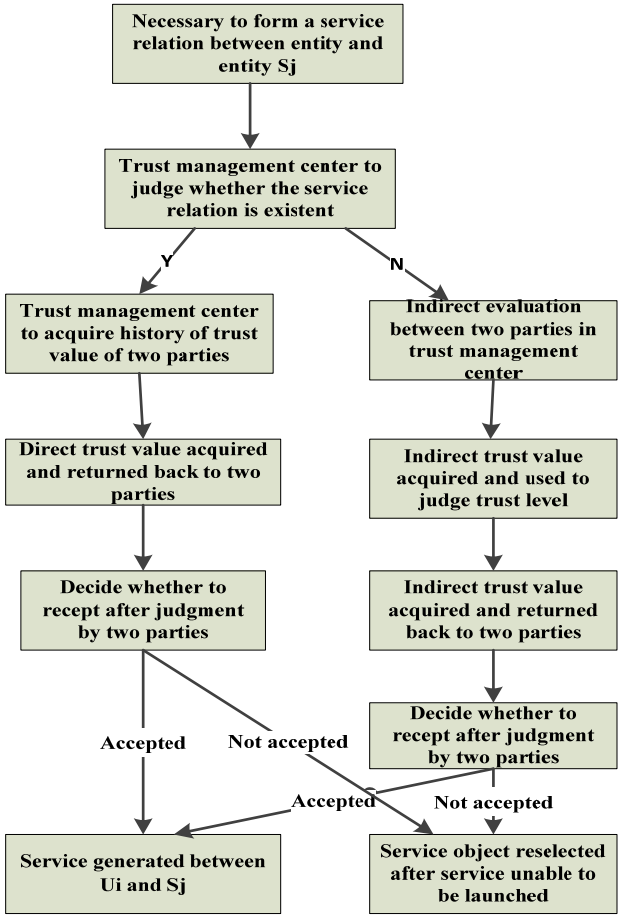

Fig.4 Flow to judge and acquire trust value

In the operating course of the trust model, when one request entity needs getting the trust value of a service entity to determine whether the service entity would be selected to act as the object which it serves, and when one service entity needs getting the trust value of a request entity to determine whether the request entity would be selected to act as the object which it serves, the flow is shown in Fig.4 to judge and get the trust value.

The trust management system could examine whether there have been service relation present between two parties. If yes, trust value would be acquired from the historic records about the trust value of two parties, and a direct trust value $DT(U_i , S_j)$ would be returned back to U_i, a direct trust value $DT(S_j, U_i)$ returned back to SSj. If two parties accept current trust value, the service would exceed; otherwise, the service would be unable to exceed. The entity would reselect the service object.

If there is no service relation present between two parties, the trust management center would get the history of the trust value of the service entity $S_j$from the history of the trust value and use it to compute and get an indirect trust value. Meanwhile, because there is no service relation formed between two parties, it would be necessary to make a judgement to the indirect trust value acquired about credibility interval. And return the indirect trust value $I(U_i , S_j)$ and the trust level of the trust evaluation together back to U_i.In the same way, return the indirect trust value

$I(S_j,U_i)$and the trust evaluation of the trust degree together back to S_j.Then, two parties would depend on the indirect trust value to judge and determine whether a service relation should be formed with the opposite entity.

C. Trust management

In order to assure stability and accuracy of cloud computing trust model and eliminate the problems of unreal entity and vicious entity present during entity evaluation, and the problem of the dynamic management and update of the trust value. The paper introduces the trust management which uses curve fitting function. Its total thought is as follows: Fit the trust value to the function, and analyze the function range and then depend on the function range to judge whether it is possible to accept new trust value against current trust distribution situation; First of all, for a request entity or service entity, it may be thought that there is a group of evaluations, i.e. set of trust value $\{T(U_k,S_j)|k=1,2,3,\ldots n\}$, called as the set T, made by the request entity to the service entity. Call the group of trust value as the sample of trust value of the entity. For the update method for the trust value which is based on curve fitting, first of all, these trust values would be ranked from small to large. After being ranked, number would be given to these trust values, with minimum trust value numbered 1, maximum one numbered n which is total of evaluation made. Therefore, the corresponding relation for a group of trust values would be acquired, i.e. $\{(k,(U_k,S_j))|k=1,2,3,\ldots n\}$. In the paper, it is called trust point, with the expression of the set *TP*. When these trust points are placed in the coordinate system, a group of trust point hash would be acquired which rise gradually. Then, fit these trust point into a proper and relatively right fitting function, which means fitting these scattered points to form a curve. If it is assumed that the curvilinear equation acquired is (x), It would be available to determine the max. and min. range of the trust value acquired with sample of current trust value on the base of the max. and mini value

$[fmin,fmax]$ which are able to be acquired for the curve in number of times of current evaluation.

Formation of fitting function (x) shown as follows:

$(x)=\varepsilon_1x^3+\varepsilon_2x^2+\varepsilon_3x+\varepsilon_4\sin x+\varepsilon_5$ Wherein, ε_1、ε_2、ε_3、ε_4、ε_5 are all constant. (12)

After the range of trust value $[fmin,max]$ is acquired based on curve fitting of trust value update mechanism, the first is to judge whether there is trust value beyond current range of trust value in the sample of the current trust value. If yes, it means that the trust value is inaccurate and not suitable to act as sample of trust value. After the inaccurate trust value is deleted, the trust update mechanism completes self-adaption adjustment of trust value and eliminating the unreal trust evaluation value.

If the service entity here receives a new evaluation, i.e. a new trust value $T(U_{\text{new}},S_j)$, the update method for trust value based on curve fitting would first judge whether the trust value $T(U_{\text{new}},S_j)$ is within the range of the current trust value $[fmin,fmax]$. If not, it means the trust value $T(U_{\text{new}},S_j)$ too high or too low and may be vicious or unreal evaluation, and the trust value would be rejected; if yes, it means that there is a relatively small gap between the trust value and the sample of trust value. Alternatively, the evaluation is relatively accurate and would be accepted. The trust value accepted would be added into the sample of trust value $\{(U_k, S_j)|k=1,2,3,\ldots n+1\}$. And then, new sample of trust value would be fit again and the step mentioned above would be repeated.

IV. RESULT OF EXPERIMENT

In order to know the accuracy and reliability of the trust model and validate the security of the trust model, the tester used CloudSim[19] simulator to validate the evaluation mechanism-based trust model. In the environment created with CloudSim simulator, the parameters of the cloud computing trust model used is listed in Table I.

The trust update mechanism of curve fitting used in the paper features as follows: first of all, rank the trust values and then, convert the ranked trust values into the points in the curve, and these points would be fitted into a fitting function which would function determining other trust value. By the trust update mechanism of curve fitting, it would be available to form a logic trust evaluation mechanism which is of self-adaption and self-adjustment to solve the problem of unreal evaluation.

The following data are used to test and analyze the trust update mechanism based on curve fitting. First of all, there are a group of sample set $T=\{T(U_k,S_j)|k=1,2,3,\ldots n\}$ about n trust values to the service entity S_j. The sample means the trust evaluation made by all the request entities in cloud computing space to the trust entity, as shown as Table II and a group of set $Tnew$ about new trust evaluation value given by the request entity $Ui$to the service entity S_j, as shown as Table III.

TABLE I. PARAMETERS USED BY SIMULATION EXPERIMENT

	Parameter	Description	Value
Parameter of trust model	u_1	Trust degree against absolute trust level	0.75
	u_2	Trust degree against general trust level	0.3
	$\alpha 1$	Weight parameter of request entity	1.0
	$\beta 1$	Weight parameter of quality description	0.382
	$\beta 2$	Weight parameter of truth degree description	0.449
	$\beta 3$	Weight parameter of service description	0.169
	α	Significance level	0.01
	n	Initial value	16

TABLE II. A GROUP OF TRUST SAMPLE T

k=	1	2	3	4
$T(U_k,S_j)$	0.2094	0.4365	0.4556	0.5076
k=	5	6	7	8
$T(U_k,S_j)$	0.5136	0.5675	0.5980	0.6060
k=	9	10	11	12
$T(U_k,S_j)$	0.6270	0.6435	0.6761	0.7196
k=	13	14	15	16
$T(U_k,S_j)$	0.7212	0.7979	0.8273	0.9562

TABLE III. A GROUP OF NEW TRUST EVALUATION T_{NEW}

k=	1	2	3	4
$T(U_k,S_j)$	0.1272	0.5597	0.4992	0.4352
k=	5	6	7	8
$T(U_k,S_j)$	0.6831	0.7802	0.9221	0.8260

\

First of all, input program 1 in Matlab to get the fitting function (x) by Matlab fitting:

$(x)=0.0006x^3-0.0154x^2+0.1466x-0.0014\sin x+0.1256$
$\Rightarrow$The range of (x) in [1,16] is [0.2628,0.9472]

It would be known via the range of (x) that there are data in trust sample T whic are not within range, respectively 0.2094 and 0.9562. Therefore, two values should be deleted in the course of self-adaption. After above deletion, new trust sample T_{adap} would be formed, as shown as Table IV.

TABLE IV.SAMPLE T_{adap} AFTERSELF-ADAPTION ADJUSTMENT

k=	1	2	3	4	5
$T(U_k,S_j)$	0.4365	0.4556	0.5076	0.5136	0.5675
k=	6	7	8	9	10
$T(U_k,S_j)$	0.5980	0.6060	0.6270	0.6435	0.6761
k=	11	12	13	14	
$T(U_k,S_j)$	0.7196	0.7212	0.7979	0.8273	

Fit new trust sample T_{adap} with Matlab and get new fitting function $f_{ada}(x)$:

$f_{ada}(x)$=0.0002x^3−0.0041x^2+0.0515x−0.0002sin$x$+0.3801
⇒The range of (x) in [1,14] is [0.4275,0.8301]

Now, all the trust sample values are in the range, which means adjustment unnecessary. The real range of the sample is [0.4275,0.8301]. For new trust value in a $Tnew$set, judge whether it belongs to the range, with result shown in Table V.

If a new trust value is beyond the range, e.g. 0.1273, it would be considered as vicious evaluation. At the same time, the value would be rejected. If a new trust value is in the range, it would be considered acceptable, e.g. 0.5598, and add the trust value to the sample of trust value T_{adap}, and use T_{adap} of the fifteen trust values as the sample of trust value T for next judgment. From the simulated data, using the trust update mechanism based on curve fitting realizes judgment about unreal or vicious trust value and update of trust value.

TABLE V. JUDGMENT ABOUT T DATA AND REJECTION REGION

i=	1	2	3	4
$ST(S_j, U_{new})$	0.1273	0.5598	0.4994	0.4353
Range	[0.4275,0.8301]			
Wether in range or not	No	Yes	Yes	Yes
Wether to accept or not	Reject	Accept	Accept	Accept
i=	5	6	7	8
$ST(S_j, U_{new})$	0.6832	0.7803	0.9221	0.8362
Range	[0.4275,0.8301]			
Wether in range or not	Yes	Yes	No	No
Wether to accept or not	Accept	Accept	Reject	Reject

V. CONCLUSION

The paper researched the hot issue of cloud security in cloud computing and used evaluation mechanism and curve fitting mechanism to constitute a kind of trust model and trust management method which could solve the issue of cloud computing security. The mutual evaluation assures trust among entities in cloud computing and provides better foundation for service selection by cloud user and cloud service supplier among entities. At the same time, it urges the cloud service supplier to provide better service and avoids appearance of more and more vicious users and entities.

On the other hand, due to limitation in terms of academic level and theory vision, it is inevitable that some shortage is present in the course of problem solving. Thus, in future study, we hope the following breakthrough achieved in the evaluation mechanism-based trust model:

(1)First of all, in the trust model, the evaluation factors should be further perfected, and the much better weight setting should be necessary. The paper sets up relevant evaluation factors in the formalized evaluation about the cloud computing service. However, because the cloud computing business mode is becoming more and more complicated, the description about cloud computing service is also becoming more and more difficult. The future study would focus on perfecting and establishing much better setting for evaluation factor and weight.

（2）In the curve fitting-based trust management method, the fitting function is key factor. And it should be denied that a more scientific form than that described in the paper is certain about selection and definition of fitting function. It also shows the future direction we should improve further.

ACKNOWLEDGMENT

This work is partly supported by National Natural Science Foundation of China(No.61370092), Natural Science Foundation of Hubei Province of China(No.2014CFB188),Hubei Provincial Department of Education Humanities and Social Science Research Foundation of China(No.15Y141).

REFERENCES

[1] BLAZE M,MFEIGENBAUM J,LACY J." Decentralized Trust Management", Proceedings of 1996 IEEE Symposium on Security and Privacy, Oakland, CA,**(1996)**, May 6-8 .

[2] Abdul-Rahman,A.,Hailes,S. "A distributed trust model-In:Proceddings of the 1997 New Security Paradigms Workshop", A Abdul-Rahman and S Hailes,Cumbria,UK:ACM Press**,(1998)**,pp.48-60.

[3] Abdul-Rahman,A.,Hailes,S. "Using recommendations for managing trust in distributed systems -in:Proceedings of the IEEE Malaysia International Conferenceon(MICC'97)" ,Kuala Lumpur:IEEE Press**,(1997).**

[4] CQ Tian,"A New Trust Model Based on Recommendation Evidence for P2P Networks", Chinese Journal of Computers, ,vol. 31,no.2,(**2009**),pp.270-281.

[5] Xuan Wang and Lei Wang,"P2P Recommendation Trust Model",Intelligent Systems Design and Applications**,2008**,2: 591-595.

[6] Ping Wang, Jing Qiu," Trust and probability analysis in P2P network",Fuzzy Systems and Knowledge Discovery(FSKD),**2011**,4: 2645-2649.

[7] TangWen, Chen Zhong,"Subjective Trust Management Model Based on fuzzy set theory ",Journal of Software, **2003**,14 (8): 1401-1408.

[8] Liu Sifeng, Xie Shiyi,"Fuzzy trust grid access control model", Computer Engineering and Design, **2011**,32 (8): 2604-2607.

[9] Schmidt S,Steele R,Dillon TS,et al,"Fuzzy trust evaluation and credibility development in multi-agent systems",Applied Soft Computing Journal,**2007**,7(2) 492-505.

[10] Zhaoxiong Zhou, Xu He, Suo-ping Wang,"A Novel Weighted Trust Model based on Cloud",Advances in Information Sciences and Services Sciences,**2011**,3: 115-124.

[11] Wang Shouxin, Zhang Li, Li Hesong,"Subjective trust evaluation method based on cloud model", Journal of Software, **2010**,6: 1341-1352.

[12] Gu Xin, Xu zhengquan, Liu Jin," Based on credible research on cloud theory and Prospect" Journal of Communications, **2011**,32 (7): 176-181.

[13] Kai Wei, Shaohua Tang," A Multi-level Trust Evaluation Model Based on D-S Theory for Grid",Computational Intelligence and Security,**2009,**2: 411-415

[14] Yanchun Zhu, Wei Zhang," A novel trust model based on D-S evidence reasoning and Fuzzy Cognitive time Map",IT in Medicine and Education(ITME 2008),**200**8: 76-79.

[15] Fang En-guang, Wu Qing,"Trust model based on cloud computing research evidence theory". Computer Applications and software, **2012**,29 (4): 68-70.

[16] Paul D Manuel,S.Thamarai Selvi,Mostafa Ibrahim Adb-EI Barr,"Trust Management System for Grid and Cloud Resources",The First International Conference on Advanced Computing 2009: 176-180.

[17] Xiaodong Sun, Guiran Chang, Fengyun Li,"A Trust Management Model to Enhance Security of Cloud Computing Environments",The Second International Conference on Networking and Distributed Computing **2011**: 244-248.

[18] Cha caiwang,"Cloud computing environment behavior trust model", Dalian Maritime University Master Thesis **,2011.**

[19] Zhou Qian,"Trust Model and Application of Mobile Ad Hoc Network Environment", University of Electronic Science and Technology master's degree thesis. 2008.4.