The Application of Personalized Cloud Service and Grey System Theory in Network Platforms

Ying Wang*, Mengying Yang
School of Business Wuchang University of Technology, Wuhan 430223, Hubei, China

*Corresponding author: yingwang@wut.edu.cn

Abstract. In order to better practice the purpose of cloud computing to provide users with cheap on-demand services and meet the personalized needs of service requesters, a dynamic trust model for personalized cloud services is proposed. Personalized cloud service is defined based on the idea of fine-grained service. The direct trust value is modified by introducing time decay factor and establishing an efficient incentive mechanism. The evaluation similarity between entities is calculated based on the grey system theory, and the evaluation similarity and the recommender's recommendation credibility are important factors to synthesize the recommendation trust value, At the same time, a method of self-confidence factor assignment based on Evaluation similarity is proposed to improve the accuracy of synthetic trust value. The experimental results show that, compared with GM-Trust model and CCIDTM model, the interaction success rate of this model is increased by 4% and 11% respectively.

Keywords: Personalized cloud services, Incentive mechanism, Recommendation credibility, Evaluation of similarity, Grey system theory, Self confidence regulator.

1. Summary
Cloud computing is based on the grid, P2P and virtualization technology developed a kind of new mode of Shared resources, IT embodies the thought of "network computers" [1], will link together a large number of software and hardware resources, a huge size of the Shared virtual IT resource pool, elastic as computing ability, the user dynamic customization service, etc. Cloud computing is about providing cheap on-demand services to businesses and other end users.

Although cloud computing brings convenience to users, user data is transferred to the hands of cloud computing service providers, and cloud computing center has no trust mechanism related services, there is a crisis of trust, therefore, the establishment of a trusted cloud computing environment is an important guarantee for the application of cloud services. Literature [2] divides information security into "hard security" and "soft security". Soft security takes service requestor as the object of protection and examines whether the service requestor is satisfied with the service provided by the service provider. In order to improve the success rate of interaction between service requestors and service providers in the cloud environment, the soft security of cloud computing - the trust relationship between service requestors and service providers has practical research value. Therefore, this paper proposes a dynamic trust model for personalized cloud services.
2. Related work
At present, in the P2P network, the research of trust model has been relatively mature, domestic and foreign researchers based on different mathematical theories, refer to the characteristics of trust such as subjective, fuzzy and other characteristics, put forward a series of trust model. The existing typical trust models in P2P networks include: Beth trust model [3] and Josang trust model [4], both of which use probability theory to build the trust model, ignoring the subjective characteristics and time-related characteristics of trust, and having a high computational complexity. Literature [5] proposed a global trust model based on similarity weighted recommendation of node rating behavior, which can contain a wider range of malicious node attacks. Literature [6] starts from the subjective characteristics of trust and constructs a trust model using grey system theory.

In the cloud computing environment, the research of trust model is still in the primary stage. The existing models include: the service selection strategy based on trust evolution and collection in cloud environment proposed in Literature [7], which solves the deficiency of simple weighting of trusted parameters. The trust model for cloud computing proposed in literature [2] is based on two-layer incentive and spoof detection, which can effectively resist attacks of various malicious behaviors. However, the calculated trust value cannot accurately reflect the real trust relationship between service requestors and service providers, which affects the success rate of interaction between service requestors and service providers. In order to help users, choose trusted cloud services, literature [8-9] built a trust model oriented to cloud computing by combining service level agreement and user evaluation. However, the reputation value measurement method ignored the subjective characteristics of trust evaluation. Literature [10] proposes a general trust model based on the related characteristics of trust. To solve the problem that it is difficult for cloud service requestors to obtain cloud services that meet their interests and preferences, literature [11] proposed a trust evaluation model of cloud service behavior based on membership theory, which enables requestors to evaluate trust according to their interests and preferences and improves the accuracy of trust evaluation. In order to describe the dynamic characteristics of trust, a dynamic trust model is proposed in literature [12-13], but its practicability needs to be improved. Literature [14] proposed a trust model based on spatiotemporal variation, but it ignored the existence of malicious recommenders in the scenarios it considered.

With more and more information on the Internet, how can users be more accurate to obtain interesting and useful services is a research hotspot. Therefore, the study of cloud service personalization cannot be ignored in the research of trust model. According to the characteristics of cloud computing and the shortage of the existing trust models, this paper proposes a personalized cloud service oriented dynamic trust model, by adopting the idea of fine-grained services provided by the service provider to refine, using the grey correlation degree evaluation, to reflect the subjective characteristics of trust, and establish incentive/punishment mechanism, encourage good service provider, Punish bad service providers. In addition, an assignment method of confidence and in moderator based on evaluation similarity is proposed, which makes the comprehensive trust value more scientific and improves the accuracy and universality of the calculated value.

3. Model of this paper

3.1. Trust relationship
Trust relationship is essentially the subjective affirmation of the trusted entity to the trusted entity [2], which has the characteristics of subjectivity, ambiguity and uncertainty, etc., and cannot be accurately measured. So far, there is no standard definition of trust. In the cloud computing environment, the service provider maximizes the satisfaction of the personalized cloud service demand proposed by the service requester, which is called the service requester trusts the service provider. The trust value is used to measure the level of trust, and the trust value changes dynamically over time.

Trust is divided into direct trust and recommendation trust, as shown in Fig. 1. Direct trust represents the direct interaction experience between service requester S and service provider O, and DT so represents the direct trust value. The recommendation trust represents the trust relationship of the service provider
O obtained by the service requester S through the recommendation of the neighbor node R, and the recommendation trust value is represented by RTso. The service requestor can obtain the comprehensive trust value of the service provider from the perspective of the whole network by integrating the historical direct interaction experience and the recommendation information of the neighbor nodes. The comprehensive trust value is represented by Tso, and the service requestor selects the service provider according to Tso.

Figure 1. Trust relationship diagram

3.2. Definition and representation of model

In different environments, the needs of service requesters are not necessarily the same. Similarly, the fields that service providers are good at are not necessarily the same [11, 15]. According to each cloud service has several service attributes, this paper subdivides the cloud service in order to more accurately reflect the behavior of service requesters and service providers, as shown in Fig. 2. Among them, O is the i-th service provider, \( V(O_i) = (V_{i1}, V_{i2}, \ldots, V_{in}) \), \( V_{ij} \) is the j-th service of \( O_i \), and each service contains multiple attributes. The weight vector of service attribute is \( A(V_{ij}) = (i_1, i_2, \ldots, i_K) \), \( i_k \) is the weight of the k-th service attribute of \( V_{ij} \), forming personalized cloud service.
Therefore, the personalized demand matrix of service requester is as follows:

\[
Q = \begin{bmatrix}
q_{111} & q_{112} & \cdots & q_{11k} \\
q_{121} & q_{122} & \cdots & q_{12k} \\
\vdots & \vdots & \ddots & \vdots \\
q_{y1} & q_{y2} & \cdots & q_{yk}
\end{bmatrix}
\]

For example, assuming that the service provider provides download service, collaborative computing service and storage service, each service can be subdivided into response time attribute, download speed attribute and file quality attribute. The personalized demand matrix of Alice and Bob service requesters is:

\[
Q_{\text{Alice}} = \begin{bmatrix}
0.2 & 0.4 & 0.4 \\
0.4 & 0.3 & 0.3 \\
0.2 & 0.4 & 0.4
\end{bmatrix},
Q_{\text{Bob}} = \begin{bmatrix}
0.5 & 0.3 & 0.2 \\
0.3 & 0.4 & 0.3 \\
0.8 & 0.1 & 0.1
\end{bmatrix}
\]

It means that different service requesters have different emphases for the same service, and different weights are given to each service attribute, which represents the personalized demand of their service request. After each transaction, the service requester \( s \) evaluates the service, and the evaluation vector \( E(V_j) = (e_{j1}, e_{j2}, \ldots, e_{jk}) \), \( w_{jm} \) represents the number of transactions between the \( j \)-th service provider and the \( m \)-th requester. Before service request, service requester \( s \) requests the information copy of service provider from the administrator as historical evidence. The structure of information copy is shown in Table 1.
3.3. Design of trust model

The goal of building a dynamic trust model in the cloud environment is: service requesters use the trust model to dynamically evaluate the trust relationship between them and service providers, and select the appropriate service providers to trade according to the evaluation results to meet their personalized service needs.

3.3.1. Direct trust value. After a transaction is completed, service requester S directly evaluates O and calculates the direct trust value based on the historical interaction experience $DT_{so(n-1)}$ and the satisfaction of the direct transaction $A_{ijk} \times E(A_{ijk})^T$ with the service provider O, providing a basis for the next interaction. In order to improve the accuracy of direct trust evaluation, based on the literature [6], this paper considers the time-related characteristics of direct trust value, establishes an effective incentive/punishment mechanism, and constructs the following direct trust model for personalized cloud service:

$$DT_{so}^{(n)} = (1-\eta) \times DT_{so}^{(n-1)} \times e^{\frac{(t-t_f)}{\lambda}}$$

$$\eta \times \delta \times [A_{ijk} \times E(A_{ijk})]^T$$

According to the property of $\lim_{x \to 0^+} e^x = 0$, $e^{-\frac{(t-t_f)}{\lambda}}$ As a time decay function, reflects the time-dependent characteristics of trust, $\lambda$ It is a time regulator; $\eta$ It is the influence weight of this satisfaction; $\delta$ Is the excitation coefficient, and its value is:

$$\delta = \begin{cases} 
A_{ijk} \times E(A_{ijk})^T > 0 \\
0 & A_{ijk} \times E(A_{ijk})^T = 0 \\
b & A_{ijk} \times E(A_{ijk})^T < 0 
\end{cases}$$

Among them, $b >= 0$ indicates that if O provides satisfactory service, it can increase the trust value slightly; if O provides malicious service, it can decrease the trust value greatly. This method can effectively punish O's malicious behavior and encourage O to provide good service. Compared with the existing incentive / punishment mechanism [2], it has the advantage of low computational complexity.

---

**Table 1. Trust relationship files among members**

| Service provider | Service collection | Service attribute weight | Interactive evaluation weight | Number of transactions | Last transaction time | Comprehensive trust value |
|------------------|--------------------|--------------------------|-------------------------------|-----------------------|----------------------|--------------------------|
| 1                | $V(O_1)$          | $A(V_{1j})$              | $E(V_{1i})$                   | $w_{1m}$              | $t_f^{(1)}$          | $T_1$                    |
| 2                | $V(O_2)$          | $A(V_{2j})$              | $E(V_{2i})$                   | $w_{2m}$              | $t_f^{(2)}$          | $T_2$                    |
| ...              | ...               | ...                      | ...                           | ...                   | ...                  | ...                      |
| $k$              | $V(O_k)$          | $A(V_{kj})$              | $E(V_{ki})$                   | $w_{km}$              | $t_f^{(k)}$          | $T_k$                    |
3.3.2. **Recommended trust value.** In order to obtain the trust value of the service provider from the perspective of the whole network, when comprehensively evaluates the services provided by O, it not only depends on the historical interaction experience, but also asks the recommender $R_i$ evaluation of O. Therefore, recommendation trust is an important part of the trust model.

(1) Composition of recommended trust values

Composition of the recommendation trust is a complex process, as shown in Fig. 3. Where, $\text{Sim}_{SR_i}$ is the evaluation similarity between service requester S and the ith recommender $R_i$; $DT_{R_iO}$ is the trust value of the $i$ recommender $R_i$ to the service provider $O$; $T_{R_i}$ represents the trustworthiness of the $i$ recommender $R_i$.

![Figure 3. Composition diagram of recommended trust value](image)

Firstly, this paper takes $DT_{R_iO}$, the historical interaction experience between $R_i$ and $O$, as the recommendation evidence for $R_i$, reflecting the historical direct transaction between the recommender and the service provider. Secondly, due to the subjective characteristics of evaluation, $\text{Sim}_{SR_i}$, the evaluation similarity between S and $R_i$, was used as one of the weights of its recommendation evidence. Similarly, the credibility of $R_i$ recommendation information cannot be ignored. In this paper, $T_{R_i}$, the global credibility of $R_i$, is used as the recommendation credibility of $R_i$ and as one of the weights of recommendation evidence. Finally, the recommended trust value is synthesized according to Formula (3):

$$RT_{SO} = \frac{1}{k} \sum_{i=1}^{k} \left( \text{Sim}_{SR_i} \times T_{R_i} \times DT_{R_iO} \right)$$

(2) Recommendation credibility

In the cloud computing environment, due to the selfishness of service requester, service provider and recommender $R_i$, $R_i$ may provide untrue recommendations. Therefore, malicious behaviors such as collusion, fraud and malicious recommendation often occur.

In order to effectively suppress the occurrence of collaborative cheating malicious behavior, the recommendation credibility of $R_i$ plays a crucial role in recommendation trust calculation. In the whole network, $R_i$ global trust value $T_{R_i}$ can reflect $R_i$ behavior credibility. Therefore, this paper uses $T_{R_i}$ to represent $R_i$ recommendation credibility to improve the accuracy of recommendation trust evaluation.
(3) Evaluation similarity
When the recommender $R_i$ recommends the service provider to $S$, $S$ is more willing to accept the recommender $R_i$ recommendation which is consistent with its own evaluation. Therefore, this paper takes the evaluation similarity between $S$ and $R_i$ as one of the recommendation evidences to improve the accuracy of calculating the recommendation trust value.

Grey system is a system that contains both known information and unknown or unascertained information. Reference [16] points out that subjective trust has subjectivity, uncertainty and imprecision. Its essence lies in its grey nature, which is the external manifestation of grey system.

Referring to the literature [17], this paper uses the grey relational degree to represent the evaluation similarity of $S$ and the recommender $R_i$, that is, the degree of consistency of their evaluation of the same behavior. It is assumed that the subject is more willing to believe the nodes similar to its own evaluation, that is, the more similar the evaluation is, the higher the evaluation similarity $Sim_{SR_i}$ will be; otherwise, the lower the evaluation similarity $Sim_{SR_i}$. The calculation process of evaluation similarity is shown in Fig. 4.

![Figure 4. Calculation diagram of evaluation similarity](image)

Let $O^\prime = \{O^{\prime}1, O^{\prime}2, \cdots, O^{\prime}n\}$ be the set of cloud service providers that have direct interaction with $S$ and $R_i$, and the direct trust vector of $S$ to $O^\prime$ is denoted as $XS (DTSO^\prime) = (DTSO^\prime1, DTSO^\prime2, \cdots, DTSO^\prime n)$, which is called the reference vector set; The direct trust vector of $R_i$ to $O^\prime$ is denoted as $XR (DTR, O^\prime) = (DTR. O^{\prime}1, DTR. O^{\prime}2, \cdots, DTR. O^{\prime} n)$, which is called the comparison vector set.

1) Using the absolute correlation degree of grey system theory [18], the grey correlation coefficients of $XS (DTSO^\prime)$ and $XR (DTR, O^\prime)$ can be obtained, which are denoted as $\gamma_i (XS (DTSO^\prime), XR (DTR, O^\prime))$ respectively, and their calculation formula is as follows:

$$Z_i(X_S(DTSO^\prime), X_R(DTR.O^\prime)) = \frac{\Delta_{\min} \eta \rho \Delta_{\max}}{\Delta \eta \rho \Delta_{\max}}$$

(4)

Where, $\rho$ is the resolution coefficient, usually 0.5; $\Delta_{\min}$ is the minimum difference between $XS (DTSO^\prime)$ and $XR (DTR.O^\prime)$, and $\Delta_{\max}$ bar is the maximum difference between $XS (DTSO^\prime)$ and $XR (DTR.O^\prime)$. $\Delta$ is the absolute difference between $XS (DTSO^\prime)$ and $XR (DTR.O^\prime)$. 


2) $r_{SR_i}$ is defined as the grey correlation degree of $X_S(DT_{SO})$ and $X_i(DTR_iO')$, and the calculation formula is:

$$r_{SR_i} = \frac{1}{k} \sum_{t=1}^{k} \rho(X_S(DT_{SO}), X_i(DTR_iO'))$$

(5)

3) The calculation formula of similarity $Sim_{SR_i}$ of $S$ and $R_i$ is defined as follows:

$$Sim_{SR_i} = \frac{r_{SR_i}}{\sum_{i=1}^{n} r_{SR_i}}$$

(6)

3.3.3. **Comprehensive trust value.** Synthesis of comprehensive trust value and confidence factor based on Evaluation similarity $\alpha$ the assignment method is as follows:

(1) Synthesis of comprehensive trust value

When service requester $S$ requests service from service provider $O$, it first requests historical transaction information such as historical direct trust value $T_{SO}(n-1)$, last transaction time $t_f$ and so on from the group administrator. Secondly, the recommended trust value $RT_{SO}(n)$ is calculated, and the comprehensive trust value $T_{SO}(n)$ is synthesized based on formula (7), which is used as the basis for this transaction. Finally, the group administrator updates the copy of information to provide the basis for the next request for service.

$$T_{SO}(n) = \alpha T_{SO}(n-1) + \beta RT_{SO}(n)$$

(7)

Where, $\alpha$ and $\beta$ represent the weight of direct trust and recommendation trust respectively, $0 \leq \alpha, \beta \leq 1$ and $\alpha + \beta = 1$, $\alpha$ represents the degree of confidence.

(2) Confidence factor based on Evaluation similarity $\alpha$ Assignment method

In the existing trust model, $\alpha$ and $\beta$ Most of the values are subjective, they are set as a fixed value, and they pay more attention to their own historical direct interactive experience $\alpha$ And $\beta$ The relationship for is set to $\alpha > \beta$. However, when the evaluation similarity between the service requester and the recommender is very high, users should combine the historical interaction experience with the weight of recommendation trust $\alpha$ And $\beta$ The relationship for is set to $\alpha \approx \beta$. Therefore, in order to improve the scientficity and objectivity of calculating the comprehensive trust value, and make the comprehensive trust value more reflect the real behavior of service providers, this paper proposes a self-confidence factor based on the evaluation similarity $\alpha$ The calculation method is as follows:

$$\alpha = 1 - \frac{Sim_{SR_i}}{\varepsilon}, \beta = 1 - \alpha = \frac{Sim_{SR_i}}{\varepsilon}$$

(8)

Among them* $\varepsilon (\varepsilon \in Z$ and $\varepsilon \neq 1)$ was the moderator of self-confidence. If $Sim_{SR_i}$ is larger, then $\alpha$ and $\beta$ the closer the $Sim_{SR_i}$ is, the smaller The SRI SIM is $\alpha$ and $\beta$ There is a big difference, but there is always $1 \geq \alpha \geq \beta \geq 0$. The significance of this method is: according to the evaluation similarity of service requester $S$ and recommender $R$, the weight of historical interaction experience and recommendation trust is reasonably allocated, so that the result of comprehensive trust value is more in line with the actual situation.

4. **Simulation experiment and comparative analysis**

In this section, the accuracy and effectiveness of the model in this paper are verified through simulation experiments, and the experimental results of the CCIDTM [2] model and GM-TRUST [6] model are compared with the results of the model in this paper.
4.1. Experimental environment
The simulation hardware environment is Intel Core2 Quad 2.83 GHz, 2.00 GB, and the simulation software environment is Windows XP, MATLAB 7.0 simulation platform. The evaluation index is the success rate of interaction between service requester and service provider with the increase of interaction times $\eta$, take $\eta$ It is defined as:

$$\text{Interaction success rate } \eta = \frac{T_{so} \geq 0.6 \text{Number of interactions for } \eta}{\text{Total number of interactions}}$$

The experimental parameters are shown in Table 2.

| Parameter name and symbol | Parametric treatment | Parameter name and symbol | Parametric treatment |
|---------------------------|----------------------|---------------------------|----------------------|
| Self confidence regulator $e$ | 2 | Provider size | 100 |
| Initial trust value $\omega$ | 0.6 | Types of providers | 4 |
| Historical action coefficient $\eta$ | 0.5 | Types of interest | 2 |
| Time adjustment factor $\lambda$ | 50 | Requester size | 2000 |
| Incentive factors $\gamma$ | 0.003 | Neighbor ratio % | 20 |
| Penalty factor $b$ | 0.005 | Proportion of malicious neighbors % | 2 |

In the real situation, there are many kinds of neighbor nodes. In this paper, two kinds of neighbor nodes are set:

1. Honest neighbor. When recommending service providers, such neighbors always provide true and credible recommendation information according to the actual situation.
2. Malicious neighbors. Such neighbors provide false and inaccurate recommendation information when recommending service providers.

4.2. The experimental results
In the scenario where the proportion of malicious neighbors is set to 2%, the curve of interaction success rate with the number of interactions obtained by the model in this paper, GM-Trust model and CCIDTM model is shown in Fig. 5.
Figure 5. The change of transaction success rate with the number of interactions

As can be seen from Figure 5:

(1) With the increase of interaction times, the interaction success rate $\eta$ of the three models converges to a fixed value. The interaction success rate between the proposed model and the GM-Trust model is higher than that of the CCIDTM model, for the following reasons: In this paper, model and GM-TRUST model by adopting the idea of fine-grained to subdivide the needs of the service requester, formed to service requesters interest embodies in the personalized services, make TRUST evaluation object from service requesters to service requesters personalized service, so as to more accurately assess the TRUST relationship between service requesters and service providers. However, CCIDTM does not take into account the personalized service requirements of service requestors, and the results of its trust evaluation cannot fully and truly reflect the trust relationship between service requestors and service providers, thus affecting their interaction success rate.

(2) As the number of interactions increases, the success rate of the proposed model is always higher than that of the GM-Trust model, and when the number of transactions is about 1,000, the success rate of the proposed model is still stable at $\geq 0.92$. The reasons are as follows: the GM-Trust model ignores the existence of malicious neighbor nodes, and the confidence factor assignment is too subjective; Model on the correction, this paper recommended the credibility of neighbor node, as an important factor synthesis of recommendation trust, and on the basis of evaluation of similarity to dynamically adjust the confidence factor, to better reflect the subjective characteristics, dynamic characteristics of trust, the trust evaluation results more effectively reflect the trust relationship between service requestors and service providers, improve the success rate of interaction.

5. Concluding remarks
This paper proposes a dynamic trust model for personalized cloud services. According to the personalized needs of the requester, the model uses the idea of fine-grained to refine the service provided by the service provider, so that the obtained trust value is more accurate, and uses the gray correlation degree to express the evaluation similarity. At the same time, according to the evaluation similarity, a dynamic adjustment method of self-confidence and trust factor is proposed to make the comprehensive trust value more scientific. In addition, an efficient incentive / punishment mechanism is proposed to motivate or punish service providers. The experimental results show that the evaluation results of the model can more accurately reflect the trust relationship between the service requester and the service provider, and help the service requester to obtain personalized cloud services.

References
[1] Feng Dengguo, Zhang Min, Zhang Yan, et al. Research on Cloud Computing Security [J]. Journal of Software, 2011, 22 (1): 71 - 83.
[2] Xie Xiaolan, Liu Liang, Zhao Peng. Journal of Electronics & Information Technology, 2012, 34 (4): 812 - 817. (in Chinese).
[3] Beth T, Borcherding M, Klein B. Valuation of Trust in Open Networks[C]//Proc. of European Symposium on Research in Security. Brighton, UK: Springer-Verlag, 1994: 1 - 18.
[4] Uncertainty of $\phi$
sang A. A Logic for Uncertain Probabilities [J]. International Journal of
Uncertainty, Unsharpness and Knowledge-Based System, 2001, 9 (3): 279 - 311.

[5] Li Jingtao, Jing Yinan, Xiao Xiaochun, et al. Trust model in P2P environment based on similarity
weighted recommendation [J]. Journal of Software, 2007, 18 (1): 157 - 167.

[6] Chen Wei, Ou Yangdan, Tang Guangming. A fine-grained P2P trust model based on grey
relational degree. Computer System Applications, 2010, 19 (6): 153 - 157.

[7] Hu Chunhua, Liu Jibo, Liu Jianxun. Service selection in cloud computing environment based on
trust evolution and collection [J]. Journal of Communications, 2011, 32 (7): 71 - 79.

[8] Gao Yunlu, Shen Beijun, Kong Huafeng. A trust model for cloud computing based on SLA and
user evaluation [J]. Computer Engineering, 2012, 38 (7): 28 - 30.

[9] Pawar P S, Rajarajan M, Nair S K, Advancement of Cloud Services[C]//Proc. Of the 6th IIP
WG 11.11 International Conference. Surat, 6th India, [s. n.], 2012: 97 - 112.

[10] Abassi R, El- Atmi S G. Towards a Generic Trust Management Model[C]//Proc. of the 19th
International Conference on Telecommunication. Jounieh, Lebanon: [s. n.]: 2012: 1 - 6.

[11] Xie Lijun, Zhu Zhiqiang. Application Research of Computers, 2013, 30(4): 1051-1054. (in
Chinese).

[12] Ren Wei, Lei Min, Yang Yu. DRT: A general dynamic evolution robust trust model for trusted
software services in cloud computing [J]. Small Microcomputer System, 2013, 33 (4): 679 -
683.

[13] Prajapati S K, Changder S, Sarkar A. Trust Management Model for Cloud Computing
Environment[C]//Proc. of International Conference on Computing Communication and
Advanced Network. Chennai, India: [s. n.], 2013: 1 - 5.

[14] Guo Q, Sun D, Chang G, et al. Modeling and Evaluation of Trust in Cloud Computing
Environments[C]//Proc. of the 3rd International Conference on Advanced Computer Control.
Harbin, China: [s. n.], 2011: 112 - 116.

[15] Tian Huirong, Zou Shihong, Wang Wendong. Journal of Electronics & Information Technology,
2007, 29 (11): 2560 - 2563. (in Chinese).

[16] Wang Lei, Huang Mengxing. Research on supplier trust evaluation based on grey AHP in cloud
computing environment. Application Research of Computers, 2013, 30 (3): 742 - 745.

[17] Xu Lanfang, Hu Huaifei, Sang Zixia, et al. Reputation reporting mechanism based on grey system
theory. Journal of Software, 2007, 18 (7): 1730 - 1737.