Hindawi
Security and Communication Networks
Volume 2019, Article ID 2437062, 11 pages
https://doi.org/10.1155/2019/2437062

Research Article

A Cloud Service Trust Evaluation Model Based on Combining Weights and Gray Correlation Analysis

Yubiao Wang[1,2], **Junhao Wen**[2], **Xibin Wang**[3], **Bamei Tao**[4] and **Wei Zhou**[2]

[1] *Huxi Campus of Network Information Center, Chongqing University, Chongqing 400030, China*
[2] *School of Big Data & Software Engineering, Chongqing University, Chongqing 400030, China*
[3] *School of Big Data, Guizhou Institute of Technology, Guiyang 550003, China*
[4] *School of Construction Management and Real Estate, Chongqing University, Chongqing 400030, China*

Correspondence should be addressed to Junhao Wen; wjhcqu@cqu.edu.cn

Received 21 December 2017; Revised 2 September 2018; Accepted 18 October 2018; Published 1 January 2019

Academic Editor: Jiankun Hu

Cloud services are cloud computing resources and applications deployed on the Internet or cloud computing platform, and users can access the required cloud services at any time. However, users face the diversity and complexity of quality of service (QoS) when evaluating and selecting cloud services. Therefore, it is important to study and establish an effective and objective trust model to improve user satisfaction and interaction success rate. In this paper, a model based on combining weights and gray correlation analysis is proposed. Firstly, direct trust, recommendation trust, and reputation together form a comprehensive trust, resulting in a more accurate overall trust. Second, rough set theory and analytic hierarchy process (AHP)-based method are used for the direct trust. Meanwhile, the degree of similarity recommendation trust is calculated by a gray relational analysis method. In order to ensure the accuracy of direct trust, this paper proposes a dynamic trust update mechanism. Finally, the simulation experiment is carried out to verify that the cloud services trust evaluation model (CSTEM) is more robust than the other three methods. It protects against malicious entities; at the same time, it can increase user satisfaction and interaction success rate.

1. Introduction

Google introduced the concept of cloud computing in 2006. The cloud computing center uses virtualization technology to organize a large number of idle resources, forming a huge "virtual resource pool", and users can request personalized cloud services through the network. As the scale of cloud services continues to expand, more and more service providers provide services with similar functions and different quality of services. Users select the most suitable cloud services from among many cloud services. In a cloud environment, trust is subjective and dynamic and is influenced by many factors. In today's increasingly competitive environment, the highly scalable technology of cloud services brings vitality to enterprises, and it also challenges users' trust in cloud services. At present, the trust problem of cloud computing is the most concerned issue of most enterprises, and it is difficult to select cloud services. Therefore, it is important to study and establish an effective and objective trust model to improve user satisfaction and interaction success rate.

At present, home and foreign scholars have conducted research on the trustworthiness evaluation and selection of cloud services. A multidimensional trust evaluation system based on compliance is proposed [1]. Ding et al. [2] analyzed the security issues facing cloud computing and defined trusted cloud services. Tang et al. [3] proposed a trustworthiness cloud service selection framework and developed corresponding evaluation middleware. Wu et al. [4] proposed a custom choice decision based on reputation. Therefore, the reputation evaluation and selection research of cloud services has a good theoretical basis.

It is important to study and establish an effective and objective trust model to improve user satisfaction and interaction success rate. We propose a CSTEM based on combining weights and gray correlation analysis. The contributions of this paper are as follows:

(1) Direct trust, recommendation trust, and reputation together form a comprehensive trust, resulting in a more accurate overall trust. The direct trust also considers transaction time and transaction amount, so the final direct trust is very accurate and effective.

(2) We propose a gray correlation analysis method used to calculate the degree of similarity recommendation trust.

(3) In order to ensure the accuracy of direct trust, a dynamic trust update mechanism is proposed.

After this Introduction, Section 2 introduces some related works; Section 3 describes the system model and its trust evaluation process; Section 4 presents the proposed trust evaluation algorithm and trust dynamic updating mechanism; Section 5 describes simulation experiment results and analysis. Finally, Section 6 presents conclusions and possible future works.

2. Related Work

There are many evaluation methods for cloud service: service transactions [5], cloud storage [6, 7], cloud application [8], and cloud security [9, 10]. A trust mining model for identifying trusted cloud services when negotiating a Service-Level Agreement (SLA) is proposed [11]. Wang et al. [12] proposed a dynamic cloud service selection strategy named DCS. Shaikh et al. [13] identified some of the available checklists to evaluate and select the parameters of the service provider to select the optimal service. Yang et al. [14] proposed a QoS-aware cloud service selection strategy, using AHP to help cloud customers choose the appropriate cloud service. Lartigau et al. [15] proposed a method based on intuitionistic fuzzy sets, which can perform similarity evaluation.

For trust evaluation of cloud services, scholars at home and abroad have relevant research in this field. Li et al. [16] proposed a multiattribute service quantization algorithm that uses information entropy and rough set theory to evaluate service quality. Na S H and Huh E N [17] proposed an SLA-based evaluation model, analyzing security threats based on service types and a cooperative model for achieving universal consensus. Wang et al. [18] proposed the CTDSS method, which divided the trust into different communities and finally selected the appropriate cloud services. A CCIDTM (Cloud Computing Incentive and Detection Trust Model) proposed by paper [19] does not consider the user's demand preference and direct trust update problem. Li et al. [20] proposed a trust-based selection scheme, and users can select cloud services through trust values. Wang et al. [21] proposed a dynamic cloud service selection strategy called DCS (Dynamic Cloud Service, DCS). Fan et al. [22] proposed a new model based on evidence reasoning. Ding et al. [23] proposed a CSTrust model, which can evaluate cloud service credibility by combining QoS prediction and customer satisfaction.

Compared to other selection methods, the CSTEM in this paper considers subjective weight and objective weight in the calculation of direct trust degree, and the calculated trust degree is more accurate. For the dynamic update of trust degree, the recommended trust degree is calculated by the gray correlation method. However, the methods in [16, 17] are not perfect for the malicious evaluation of users and the feedback of users after using cloud services. The CCIDTM does not consider the user's demand preference and direct trust update problem [19]. Hu et al. [24] proposed a novel method; it does not consider the level of service and the accuracy of credible services span tree. There is no guarantee that the recommended service is the best service. The EigenRep trust model is a global reputation calculation model. There is no reputation penalty correction for node malicious behaviour. Even if the service with the best reputation is selected, the service is not guaranteed to be true and is the most suitable for users. At the same time, the EigenRep model requires an iterative calculation of the global reputation in the entire network for each transaction, and the system overhead is large.

In this paper, we propose an evaluation model that is based combining weights and gray correlation analysis, it introduces the direct trust dynamic update mechanism. Meanwhile, the model can dynamically evaluate the comprehensive trust of cloud services, and obtain the cloud service with the highest comprehensive trust, effectively helping users to choose the best cloud service.

3. Trust Evaluation Model

3.1. Model Definitions

Definition 1 (entity). This paper defines the ability of an entity to have self-behavior. Define cloud users CSU= $\{User_1, User_2, User_i \cdots User_n\}$. Cloud service provider is defined as CSP= $\{CSP_1, CSP_2 \cdots CSP_i, CSP_n\}$ [9].

Definition 2 (scoring matrix). After the user uses the cloud service, the user scores the cloud service, and the evaluation of the cloud service indicates that the article uses E(Q) to indicate the trust evaluation.

3.2. Model Framework. The CSTEM is composed of five modules: service requestor, cloud service registration center [9], CSP, CSTMC, and trust feedback monitoring, shown in Figure 1. The CSTMC is composed of direct trust, recommended trust, reputation, and trust dynamic update mechanism. It performs the evaluation and selection of cloud services.

3.3. Trust Evaluation Process. The comprehensive trust consisted of the direct trust, recommendation trust, and reputation. The direct trust relationship means that both sides have historical interaction experience. Recommended trust has no historical interaction of both interactive experiences; relevant factors include the degree of similarity recommendation respondents and the level of the respondents. The reputation represents the evaluation of all the cloud service users.

This trust evaluation process is as shown in Figure 2.

The specific steps of the trust evaluation are as follows.

Step 1 (register). Cloud service provider resources are registered by CSAPI.

Step 2. Request.

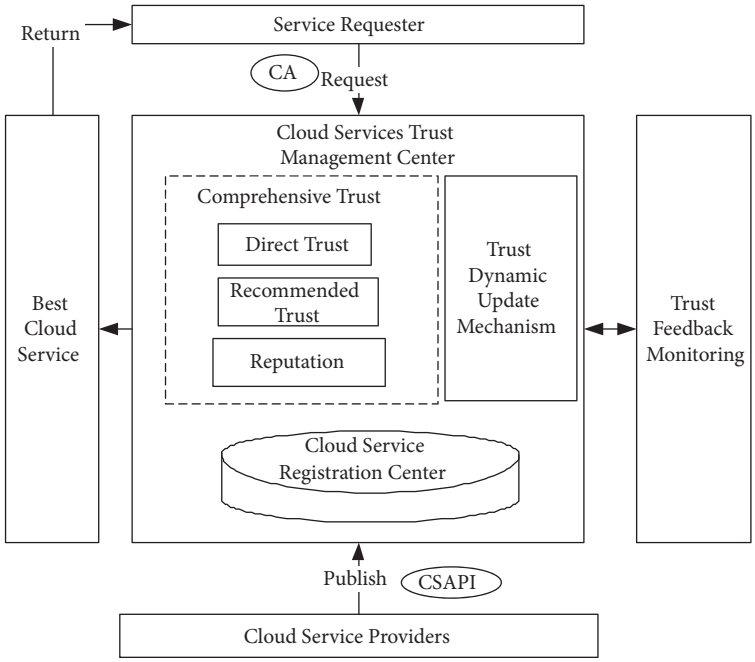

Figure 1: Cloud service trust evaluation model.

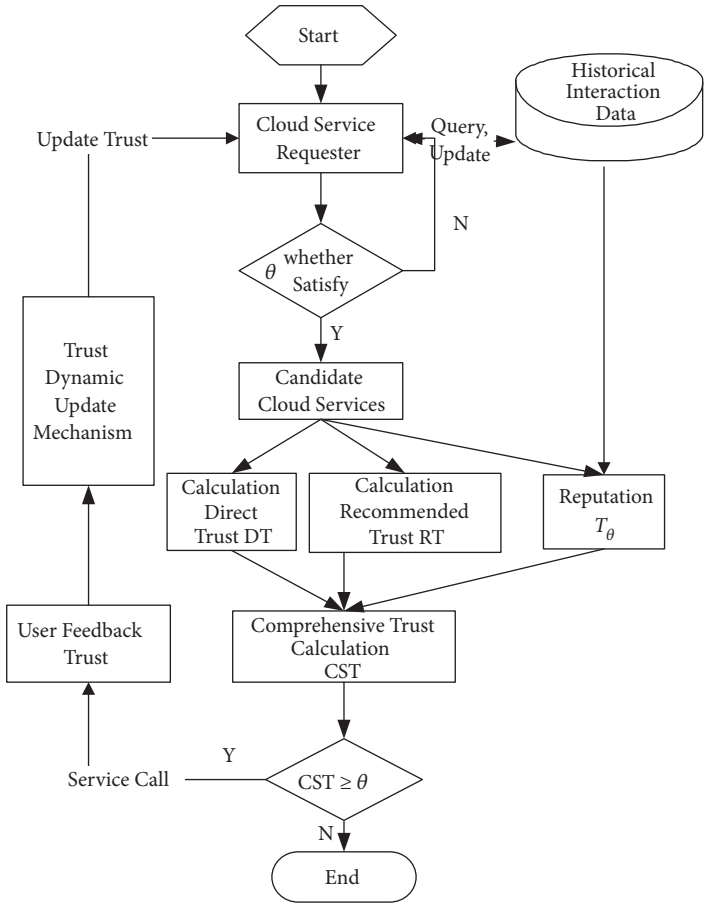

Figure 2: Trust evaluation process.

Step 3 (calculate the comprehensive trust CST). History interaction records are inquired by the cloud trust management center. A gray relational analysis method is used to calculate the similarity recommended trust and get the recommended trust RT, and the reputation of T_θ is calculated by all users of the cloud service. Meanwhile, three different types of trust are assigned different weights for evaluation.

Step 4. If CST≥θ, indicating that the service meets the requirements of the user, go to Step 5; otherwise, if the cloud service does not meet the user requirements, please go to Step 2.

Step 5. Users select the cloud service with the highest CST.

Step 6. Update the direct trust according to formula (30).

4. Trust Evaluation Algorithm

4.1. Direct Trust Calculation. In order to guarantee the weight of evaluation is right, evaluation data should be adjusted to a uniform interval, the data preprocessing of this paper with a minimum-maximum normalization method, and it is calculated by paper [25].

4.1.1. Objective Weight. Rough set theory is founded by Polish Scientist Z. Pawlak [26]; it is a treatment imprecise, inconsistent, incomplete information and other effective tools.

Set S = (U, A, V, f) as an information system, the definition of fuzzy relation R, V represents an attribute value, V_{ij}(i = 1, 2, · · ·n; j = 1, 2, · · ·m) represents an attribute value for the object i in the j-th attribute, and f : U × A ⟶ V is a knowledge representation function, for each x∈U, q∈A, f (x, q) ∈V.

Definition 3 (set R as the equivalent relation on U). It is defined as follows: $\forall x_r, x_t \in U; \forall q_j \in A; r, t = 1, 2, \cdots n; j = 1, 2, \cdots m$. The similarity of the object x_r and the object x_t is defined as $1 - \alpha$, and $V_{ij}{}'$ represents a property value of data preprocessing.

$$x_r R x_t = \left\{ (x_r, x_t) \in U \times U \mid \frac{1}{m} \sum_{j=1}^{m} \left| V_{rj}{}' - V_{tj}{}' \right| \le \alpha \right\} \quad (1)$$

Definition 4 (S = (U, A, V, f)). FR(x_i) represents the fuzzy similarity class of the x_i,$\forall x_r, x_t \in U$, they are expressed as

$$\mathrm{FR}(x_i) = \left\{ x_i \in U \mid \frac{1}{m} \sum_{j=1}^{m} \left| V_{rj}{}' - V_{tj}{}' \right| \le \alpha \right\} \quad (2)$$

Definition 5 (S = (U, A, V, f)). The equivalence class of x is represented by I(x), x∈U, x represents the fuzzy relationship of U, R ⊆ A, $\overline{\mathrm{Apr(x)}}$ represents the upper approximation set, and $\underline{\mathrm{Apr(x)}}$represents the lower approximation set.

$$\overline{\mathrm{Apr}(x)} = \bigcup \{ x \in U : I(x) \cap X \neq \Phi \quad (3)$$

$$\underline{\mathrm{Apr}(x)} = \bigcup \{ x \in U : I(x) \subseteq X \quad (4)$$

For a given threshold $\beta \in (0.5, 1)$, the definition upper approximation set of variable precision rough set is

$$\overline{\mathrm{Apr}_\beta(x)} = \bigcup \left\{ x \in U \mid \frac{X \cap FR(x)}{FR(x)} > 1 - \beta \right\} \quad (5)$$

The under approximation set of β is

$$\underline{\mathrm{Apr}_\beta(x)} = \bigcup \left\{ x \in U \mid \frac{X \cap FR(x)}{FR(x)} \ge \beta \right\} \quad (6)$$

Definition 6. Set R∈A, X as a division of property, X = {$X_1, X_2, \cdots X_t$}, and the approximate classified quality γ_R(X) is defined as

$$\gamma_R(X) = \sum_{1}^{t} \frac{\underline{\mathrm{Apr}_\beta(x)}}{|U|} \quad (7)$$

Definition 7. Set S = (U, A, V, f), and sig(A_i) represents the importance of A_i properties:

$$\mathrm{sig}(A_i) = 1 - \gamma_{A-\{A_i\}}(X) \quad (8)$$

Definition 8. Set S = (U, A, V, f), A = {$A_1, A_2, A_j, \ldots, Am$}, and $W_j(A_j)$ represents the weight of attribute A_j in A:

$$W_j(A_j) = \frac{\mathrm{sig}(A_j)}{\sum_{j=1}^{m} \mathrm{sig}(A_j)} \quad (9)$$

4.1.2. Subjective Weight. Analytic Hierarchy Process (AHP) is put forward a qualitative and quantitative combination of decision analysis method by A.L.Saaty in the 1970s [27]. AHP model for cloud service selection is as shown in Figure 3.

The process of calculating subjective weights using AHP is as follows.

Step 1. It clears a problem, and then establish hierarchical structure.

According to the important attribute index summarized by the cloud service, the relationship between the influencing factors of the cloud service selection process is analyzed, and the hierarchical model is established.

(1) Target Layer G. It chooses a most suitable cloud service from multiple cloud services.

(2) Criterion Layer B. It analyzes the factors that affect the choice of cloud service and the three basic elements of cloud service: cost, performance, and reputation.

(3) Attribute Layer C (Including Subattribute Layer).

(4) Object Layer.

The evaluation indicators $B_1, B_2 \cdots B_n$ have an effect on the target G. We use a pairwise comparison method to determine their impact in the proportion of G. The results of all the comparisons are expressed by the matrix B = (b_{ij}) n ∗ n.

$$B = \begin{Bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{Bmatrix} \quad (10)$$

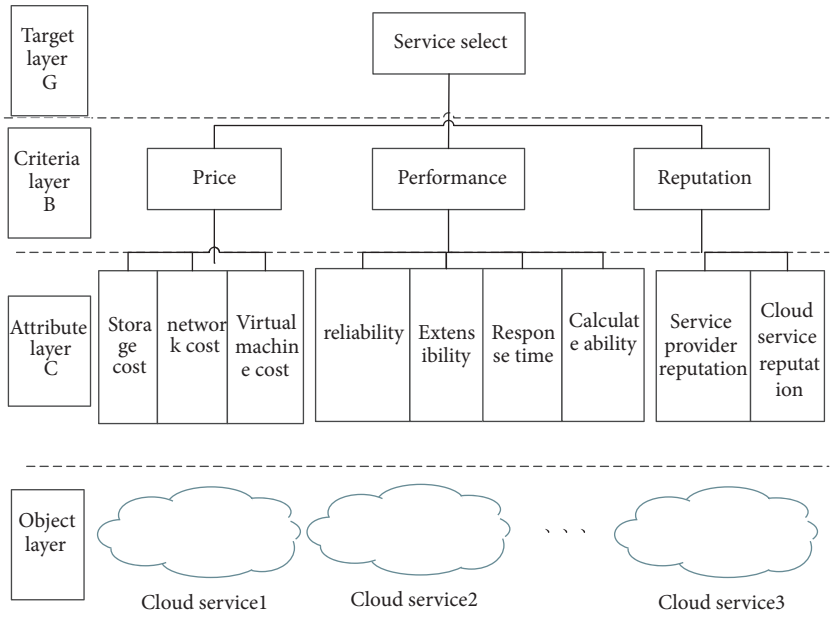

Figure 3: AHP model for cloud service selection.

Step 2. Set up the comparison matrix of the two pairs.

Step 3. Hierarchy Single Sort.

As shown in Figure 3, we use the judgment matrix B and then get a single ordering vector of the attribute index in the criterion layer B with respect to target G. It is a feature vector that satisfies $BW = \lambda_{\max} W$, it represents $W = (w_1, w_2 \cdots w_n)^T$, and w_i is represented by the corresponding position element.

(1) We normalize each column element of the judgment matrix, and the general term of the element is

$$\overline{b}_{ij} = \frac{b_{ij}}{\sum_1^n b_{ij}} \tag{11}$$

(2) Each column is normalized after the judgment matrix, and the line added is

$$\overline{w}_i = \sum_1^n \overline{b}_{ij} \quad (i = 1, 2, \ldots n) \tag{12}$$

(3) $w_i = \overline{w}_i / \sum_1^n \overline{w}_i, W = (w_1, w_2 \cdots w_n)^T$ is the approximate solution of the required eigenvector.

(4) $\lambda_{\max} = \sum_{i=1}^n ((BW)_i / w_i)$.

Step 4 (consistency check). Since matrix B is subjectively determined, it is necessary to check satisfaction consistency.

(1) Judgment matrix consistency index CI (consistency index):

$$CI = \frac{\lambda_{\max} - n}{n - 1} \tag{13}$$

(2) Random consistency index RI.

(3) Consistency ratio CR (it is used to determine the permissible range of B's inconsistency).

When n<3, the judgment matrix is always completely consistent. The random consistency ratio CR (consistency ratio) is as shown in the following equation.

$$CR = \frac{CI}{RI} \tag{14}$$

Step 5 (hierarchical sorting). The hierarchical total sort vector is a relative weight vector that calculates the importance of the target layer for all factors at a certain level; the process is carried out from high level to low level. As shown in Figure 3, if the level B has m influencing factors $B_1, B_2, \cdots, B_m$, the total ranking weights for the target layer G are $w_{B_1}^G, w_{B_2}^G, \cdots, w_{B_m}^G$. The next level C of the influencing factor Bj contains the n attribute indices $C_1, C_2, \ldots, C_n$, and their hierarchical single order weights are $w_{C_{1j}}^{B_j}, w_{C_{2j}}^{B_j}, \cdots, w_{C_{nj}}^{B_j}$, and the C level attribute C_{ij} is given the total ordering weight of the target layer G:

$$w_{C_i}^G = w_{B_j}^G w_{C_{ij}}^{B_j}, \quad i = 1, 2, \cdots, n, \ j = 1, 2, \cdots, m \tag{15}$$

4.1.3. Combining Weights. In this paper, the rough set theory is used to calculate the user's objective weight, the AHP is used to calculate the subjective weight of the user, and finally their combined weights are calculated. The objective weight calculation formula is as shown in (9), and the subjective weight calculation formula is as shown in (15). W_i^* represents the combined weight, m is the number of attributes, and the combined weights values are shown in the following equation:

$$W_i^* = \frac{W_i W_i'}{\sum_{i=1}^m W_i W_i'} \tag{16}$$

4.1.4. Attenuation Factor

(1) Transaction Time. The user's preference will decay with time. According to the Ebbinghaus forgetting curve, the time

decay factor is established. The time decay factor is shown in the following equation.

$$T(\mathrm{i}) = \exp\left(\frac{time\left(\mathrm{U}_i, CS_j\right) - \min\left(\mathrm{U}_i\right)}{\max\left(\mathrm{U}_i\right) - \min\left(\mathrm{U}_i\right)}\right) \tag{17}$$

When the user U_i requests the service and interacts with the cloud service CS_j, $time(\mathrm{U}_i, CS_j)$ represents the evaluation time after the user uses the cloud service CS_j, and the latest evaluation time after the user U_i uses the cloud service is represented by $\min(\mathrm{U}_i)$. The earliest evaluation time after the user U_i uses the cloud service CS_j is represented by $\max(\mathrm{U}_i)$.

(2) Transaction Amount. The transaction amount is a more important factor. p_i indicates the transaction amount between the user and the cloud service at the i-th transaction. As shown in (18), it indicates attenuation factor P(i).

$$\mathrm{P}(\mathrm{i}) = \frac{{p_i}^{\tau}}{\sum_{j=1}^{n} {p_j}^{\tau}}$$
$$\text{and } \sum_{i=1}^{n} \mathrm{P}(\mathrm{i}) = 1 \tag{18}$$

τ is a constant greater than 1, which is used to adjust the intensity of the change in the amount of different transactions. It can produce discrete effects and better distinguish between the effects of different transactions, when $\tau = 2$ can achieve a good discrete effect, so we set $\tau = 2$ in this model.

$$\mathrm{P}(\mathrm{i}) = \frac{{p_i}^{2}}{\sum_{j=1}^{n} {p_j}^{2}}$$
$$\text{and } \sum_{i=1}^{n} \mathrm{P}(\mathrm{i}) = 1 \tag{19}$$

ϕ represents the final attenuation factor, and $\sum_{i=1}^{n} \phi(\mathrm{i}) = 1$.

$$\phi(\mathrm{i}) = T(\mathrm{i})\,\mathrm{P}(\mathrm{i}) \tag{20}$$

4.1.5. Final Direct Trust. E(Q) represents a trusted evaluation matrix of the user for the cloud service, combined with (16) and (19), and the final direct trust values are shown in the following equation:

$$DT^{t_i} = \sum_{i=1}^{n} \mathrm{E}(\mathrm{Q})\, {W_j}^{*T} \phi(\mathrm{i}) \tag{21}$$

4.2. Recommended Trust. Professor Deng Julong proposed a grey system theory [28]; it is a new method for less data and poor information uncertainty. In this paper, it is used to calculate the degree of similarity of the requester with other user's recommendation. By the geometry of the column reference data and comparison data columns similarity, it is used to determine their similarity tightness.

Requester u_r and recommender u_i are for common use a set CS, $CS = \{\mathrm{CS}_1, \mathrm{CS}_2, \cdots CS_n\}$, m is the number of recommenders, u_r and u_i trust evaluation for CS are $DT_{CS_k,u_r} = \{DT_{CS_1,u_r}, DT_{CS_2,u_r}, \cdots DT_{CS_n,u_r}\}$and $DT_{CS_k,u_i} = \{DT_{CS_1,u_i}, DT_{CS_2,u_i}, \cdots DT_{CS_n,u_i}\}$, the gray correlation analysis method is used to calculate the similarity of the evaluation of requesters u_r and u_i, and the step is as follows:

(1) $\xi_i(DT_{CS_k,u_r}, DT_{CS_k,u_i})$ represents gray correlation coefficient of the requester u_r and recommender u_i.

$$\xi_i\left(DT_{CS_k,u_r}, DT_{CS_k,u_i}\right) = \frac{\Delta_{\min} + \rho\Delta_{\max}}{\Delta + \rho\Delta_{\max}} \tag{22}$$

ρ means the resolution factor. ρ is smaller, the greater of the resolution, the general value $\rho \in (0, 1)$. Set $\rho = 0.5$, and $\Delta_{\max}$, $\Delta_{\min}$, and Δ represent the poles that are maximum difference, minimum difference, and absolute difference for DT_{CS_k,u_r} and DT_{CS_k,u_i}.

(2) Gray correlation of DT_{CS_k,u_r} and DT_{CS_k,u_i} is

$$\gamma_{u_r,u_i} = \sum_{1}^{n} \xi_i\left(DT_{CS_k,u_r}, DT_{CS_k,u_i}\right) \tag{23}$$

(3) Sim_{u_r,u_i} represents the similarity, and m is the number of recommenders.

$$Sim_{u_r,u_i} = \frac{\gamma_{u_r,u_i}}{\sum_{1}^{m} \gamma_{u_r,u_i}} \tag{24}$$

DT_{CS_k,u_i} represents the trust relationship between recommender and service provider, Sim_{u_r,u_i} represents the evaluation similarity, T_{u_i} is a global trust of recommender, and recommendation trust value is as shown in the following equation.

$$RT = \frac{1}{m}\sum_{i=1}^{m} Sim_{u_r,u_i} \times T_{u_i} \times DT_{CS_k,u_i} \tag{25}$$

4.3. Comprehensive Trust. $DT^{t_i}_{u_r,cs_k}$ represents a direct trust, $RT^{t_i}_{u_r,cs_k}$ represents a recommendation trust, and ${T_\theta}^{t_i}$ represents cloud service itself reputation in time t_i, the initial value is 0.6, and the value with user interaction will be updated. α represents the weight of direct trust. The weight of the recommended trust is indicated by β, and the weight of the cloud service credibility is represented by χ. In time t_i, the comprehensive trust degree of the user u_r to the cloud service cs_k can be represented by $CST^{t_i}_{u_r,cs_k}$, and the final comprehensive trust degree calculation formula is shown as (26). The pseudocode of trust evaluation process is shown in Algorithm 1.

$$CST^{t_i}_{u_r,cs_k} = \alpha * DT^{t_i}_{u_r,cs_k} + \beta * RT^{t_i}_{u_r,cs_k} + \chi {T_\theta}^{t_i} \tag{26}$$

4.4. Trust Dynamic Updating Mechanism

Customer Satisfaction. ${W_j}^*$ represents each attribute trust preferred weight of cloud service, S represents service vector, maybe a single cloud service or multiple cloud services, E(Q) represents trust evaluation feedback, and ST(i) represents the

Input: Requester u_r, Provider CS
Output: CST (u_r,CS,Time).
D=Find(u_r,CS,Time);
Public Void CSTrust_Eval( )
D=Find(u_r,CS,Time);
C=Count(CSr,CSp,Time); // History interaction records are inquired by cloud trust management center
If C≥1;
Calculate$W_j^* = W_j W_j' / \sum_{j=1}^{m} W_j W_j'$;/
Calculate $\phi(\mathrm{i}) = T(\mathrm{i})\mathrm{P}(\mathrm{i})$
Calculate $DT^{t_i} = \sum_{i=1}^{n} \mathrm{E}(\mathrm{Q}) W_j^{*T} \phi(\mathrm{i})$;
else
DT=CST_0 //CST_0 is a trust value that is published by cloud service
Then
Calculate $Sim_{u_r,u_i} = \gamma_{u_r,u_i} / \sum_1^m \gamma_{u_r,u_i}$
$RT = (1/m) \sum_{i=1}^{m} Sim_{u_r,u_i} \times T_{u_i} \times DT_{CS_k,u_i}$
Then
Calculate the comprehensive trust in t_i
$CST_{u_r,cs_k}^{t_i} = \alpha * DT_{u_r,cs_k}^{t_i} + \beta * RT_{u_r,cs_k}^{t_i} + \chi T_\theta{}^{t_i}$//$\alpha$=0.7, β=0.15, χ=0.15
If CST ≥ θ Send service request to CS, then user feedback trust
else
Return request failed

Algorithm 1: The pseudocode of trust evaluation process.

satisfaction on the cloud service i. Customer satisfaction is shown in (28).

$$Q = \left(W_j^*\right)^{\mathrm{T}} * \mathrm{S} = \begin{bmatrix} q_{11}, q_{12}, \cdots q_{1k} \\ q_{21}, q_{22}, \cdots q_{2k} \\ \cdots \\ q_{j1}, q_{j2}, \cdots q_{jk} \end{bmatrix} \tag{27}$$

$$\mathrm{ST}(\mathrm{i}) = Q * \mathrm{E}(\mathrm{Q})^{\mathrm{T}} \tag{28}$$

Penalty Factor. The user's preference will decay with time, and trust will drop quickly. Therefore, the direct trust update of this paper introduces a penalty mechanism. Once the transaction fails, that is, the cloud service does not satisfy the user, the service party will be punished. Setting φ is a penalty factor after the transaction.

$$\varphi = f * \left[\frac{1}{(k + e^{-n})}\right] \tag{29}$$

If the transaction is successful, it is $f = 0$, the transaction failure is $f = -1$, and the number of failures is indicated by n. In order to prevent the problem of small amount of transaction fraud, the transaction amount is considered. The trust value will be decreased rapidly in the transaction failures by the acceleration factor, so that once the main trading promises to each other, their trust values will decline rapidly.

Dynamic Trust Updates. Trust relationship will be updated by the trust manager center, μ represents the weight of transaction history ($0 < \mu < 1$), $T(\mathrm{i})$ is calculated by (17), and P(i) is calculated by (18).

Finally, the direct trust value update formula (30) of the penalty factor is considered.

$$DT' = \mu DT + (1 - \mu)\,\mathrm{ST}(\mathrm{i}) * T(\mathrm{i}) * \mathrm{P}(\mathrm{i}) + \varphi \tag{30}$$

DT' is a direct trust value, trust needs to be updated, through this service to meet the user set basic satisfaction threshold ξ, and it is used to determine whether the transaction is successful. Rewrite the Cloudsimlet class in Cloudsim, add variables to identify cloudletPrice for the user in the interaction provided by the resources of the cost, and meanwhile, increase the variable cloudletTime, customer satisfaction ST, and penalty factor φ. Pseudocode of direct trust update is shown in Algorithm 2.

5. Simulation Experiment Results

The model is analyzed and implemented on the Myeclipse 2014 platform, its integrated simulation package CloudSim 3.0.3, its hardware environment for the CPU Core i7-3770 3.4GHz, RAM 8.00 GB. CloudSim is a new, universal, and extensible simulation framework.

The number of nodes in the cloud computing network is very large, the relationship between nodes is also very complex, and in this simulation, the experimental process is divided into many rounds: each round has the same nodes, and the trust mechanism is similar. There are 50,100,150,200,250,300 experiments of different sizes, the comprehensive average of the rounds of experiments as the average satisfaction, and the value of the success rate. It is successful to meet the certain threshold of customer satisfaction as a criterion for judging the success of the

Algorithm: direct trust update;
Input: direct trust degree DT; user satisfaction threshold ξ; user satisfaction evaluation E (q); penalty factor φ
Output: The direct trust of this transaction.
(1) public void UpdateDirectValue(int cloudletId. int vmId);
(2) { ;
(3) double P(i)=Cloudletlist.getById(cloudletId.vmId).getcloudletPrice();
(4) double T(i)=Cloudletlist.getById(cloudletId.vmId).getcloudletTime();
(5) this. ST(cloudletId. vmId. E(q));
(6) if(ST > ξ);
(7) double φ=Cloudletlist.getById(cloudletId.vmId).getcloudlet Penalty ();
(8) this. IncrementalDirectValue(cloudlet. vmId. P(i). T(i).φ);
(9) int t=DirectTable.getById(cloudletId,vmId).getTime;
(10) DirectTable.getById(cloudletId,vmId).getTime(t.K);// K is the time period
(11) DirectTable.getById(cloudletId,vmId).updateDirectValue(DT, IncrementalDirectValue);
(12) }

Algorithm 2: Pseudocode of direct trust update.

interaction: when the satisfaction reaches 0.7, the interaction is successful.

In this paper, CSTEM was compared with other CCIDTM, EigenRep, and RSS methods; the first method is a random service selection (RSS), and RSS only randomly selects a service that satisfies the basic functions of the user. It does not perform feedback after the user uses the service. The EigenRep is a global reputation calculation model. There is no reputation penalty correction for node malicious behaviour. The third method is the CCIDTM proposed by paper [19].

5.1. Customer Satisfaction. CSTEM was compared with other CCIDTM, EigenRep, and RSS methods. The average satisfaction of the different methods is shown in Figure 4. The customer satisfaction of different proportions of malicious cloud service entities is shown in Figure 5.

RSS only randomly selects a service that satisfies the basic functions of the user. It does not perform feedback after the user uses the service, and the satisfaction is the lowest. The EigenRep trust model is a global reputation calculation model. There is no reputation penalty correction for node malicious behaviour. Even if the service with the best reputation is selected, the service is not guaranteed to be true and is the most suitable for users. At the same time, the EigenRep model requires an iterative calculation of the global reputation in the entire network for each transaction, and the system overhead is large. The CCIDTM does not consider the user's demand preference and direct trust update problem, so the user satisfaction is low. The CSTEM in this paper considers subjective weight and objective weight in the calculation of direct trust degree, and the calculated trust degree is more accurate. The dynamic update of trust degree, the recommended trust degree, is calculated by the gray correlation method, so the user satisfaction is the highest, CSTEM> CCIDTM> EigenRep> RSS.

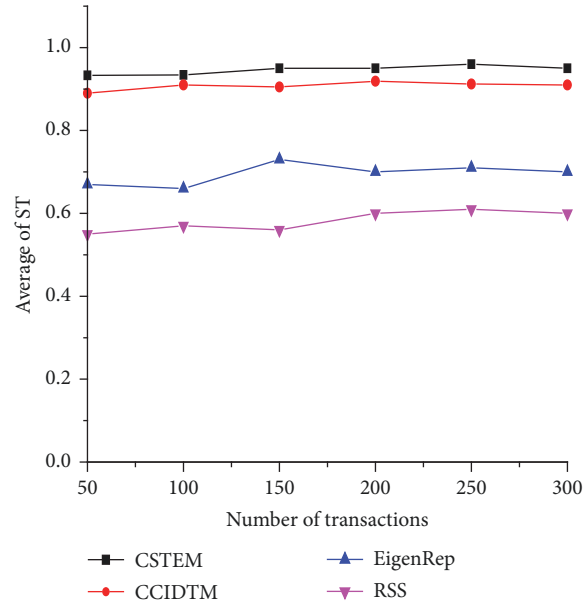

Figure 4: The average satisfaction of different methods.

5.2. Success Rate of Cloud Services Selections. RSS only randomly selects a service that satisfies the basic functions of the user. It does not perform feedback after the user uses the service, and the satisfaction is the lowest. The EigenRep trust model is a global reputation calculation model. There is no reputation penalty correction for node malicious behaviour. Even if the service with the best reputation is selected, the service is not guaranteed to be true and is the most suitable for users. At the same time, the EigenRep model requires an iterative calculation of the global reputation in the entire network for each transaction, and the system overhead is large. As shown in Figure 6, the success rate of CSTEM and CCIDTM is higher than EigenRep model. The CCIDTM does not

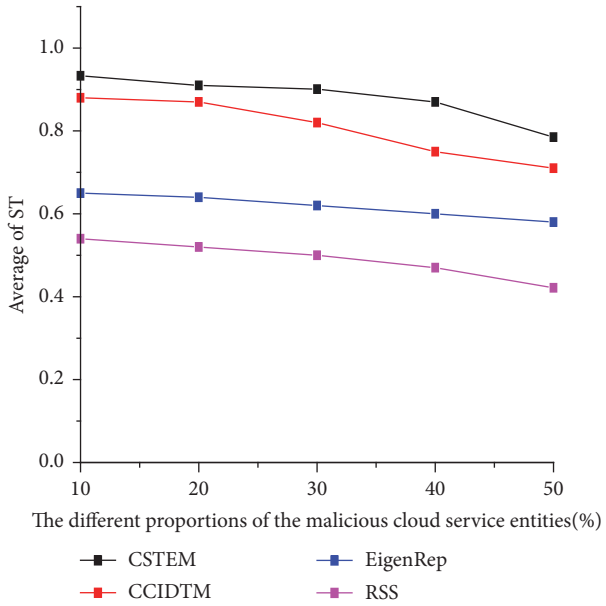

Figure 5: The customer satisfaction of the malicious cloud service entities.

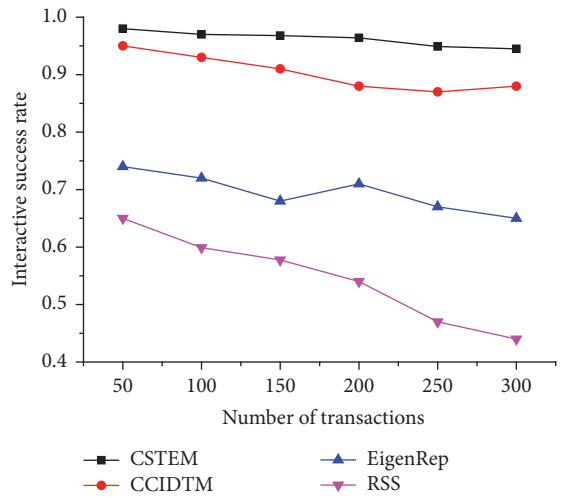

Figure 6: The interactive success rate.

consider the user's demand preference and direct trust update problem, so the user satisfaction is low. The EigenRep trust model is a global reputation calculation model. There is no reputation penalty correction for node malicious behaviour. Even if the service with the best reputation is selected, the service is not guaranteed to be true and is the most suitable for users. At the same time, the EigenRep model requires an iterative calculation of the global reputation in the entire network for each transaction, and the system overhead is large. The CSTEM considers the time decay of direct trust, using feedback density factor to reduce the impact of malicious trust feedback, and dynamic trust updating mechanism, so the interactive success rate is highest. The interactive success ranking is CSTEM>CCIDTM>EigenRep>RSS.

In order to validate the model, there are malicious cloud service entities ranging from 10% to 40% evaluated. Different proportions and success rates of malicious cloud service entities are shown in Figure 7, and CSTEM is more better than CCIDTM, EignRep, and RSS. The success rates of CSTEM and CCIDTM is higher than that of EigenRep model. RSS only randomly selects a service that satisfies the basic functions of the user. It does not perform feedback after the user uses the service, and the satisfaction is the lowest. The CSTEM considers the time decay of direct trust, using feedback density factor to reduce the impact of malicious trust feedback, and dynamic trust updating mechanism, so the success rate of interaction is higher than the other three methods, CSTEM > CCIDTM >EigenRep> RSS.

6. Conclusion

The CSTEM is based on combining weights and gray correlation analysis. In order to improve user satisfaction and interaction success rate, direct trust, recommendation trust, and reputation together form a comprehensive trust, resulting in a more accurate overall trust. The direct trust also considers transaction time and transaction amount, the objective weight is calculated by rough set theory, and the subjective weight is calculated using AHP, so the final direct trust is very accurate and effective. A gray relational analysis method is used to calculate the degree of similarity recommendation trust, make the recommendation trust become more reasonable, combine with the service provider's own reputation, and then get the comprehensive trust. This paper proposes a dynamic direct trust update mechanism. Finally, simulation experiments show that the CSTEM performs better than CCIDTM, EignRep, and RSS.

This paper is subject to the following limitations:

(1) The CSTEM could be further improved by considering more trust dynamic update factors of the cloud services evaluation. Considering the trust dynamic update factor of cloud service evaluation, cloud service providers can classify and evaluate and select cloud service trustworthiness in specific environments such as mobile environment and heterogeneous environment.

(2) In order to improve interaction success rate, the future cloud service selection performance, and security, we can further expand the scale of the experiment, build the actual cloud prototype system, and deploy this strategy to verify and improve the model which is the main work of the future.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Science Foundation of China under Grant No. 61672117 and No. 61602070 and the Medical Research Project of Chongqing Health and Family Planning Commission of China (No. 20142124).

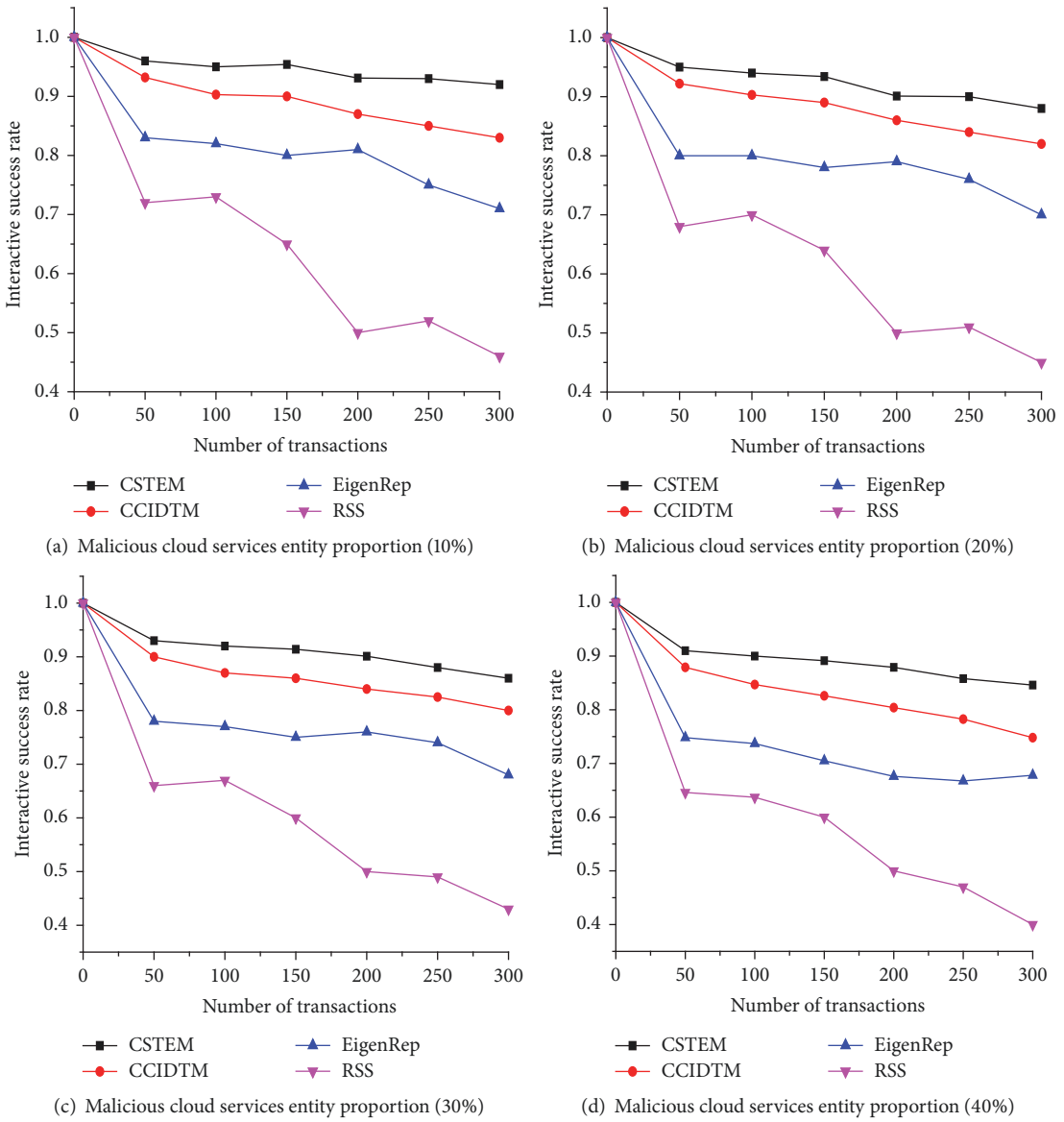

Figure 7: Different proportions and success rates of malicious cloud service entities.

References

[1] S. Singh and J. Sidhu, "Compliance-based Multi-dimensional Trust Evaluation System for determining trustworthiness of Cloud Service Providers," *Future Generation Computer Systems*, vol. 67, pp. 109–132, 2017.

[2] Y. Ding, H. M. Wang, P. C. Shi, Q. Wu, H. D. Dai, and H. Y. Fu, "Trusted cloud service," *Chinese Journal of Computers*, vol. 38, no. 1, pp. 133–149, 2015.

[3] M. Tang, X. Dai, J. Liu, and J. Chen, "Towards a trust evaluation middleware for cloud service selection," *Future Generation Computer Systems*, vol. 74, pp. 302–312, 2017.

[4] Z. Wu and Y. Zhou, "Customized Cloud Service Trustworthiness Evaluation and Comparison Using Fuzzy Neural Networks," in *Proceedings of the 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, pp. 433–442, Atlanta, GA, USA, June 2016.

[5] Y. Kouki, T. Ledoux, and R. Sharrock, "Cross-layer SLA selection for cloud services," in *Proceedings of the 2011 1st IEEE Symposium on Network Cloud Computing and Applications, NCCA 2011*, pp. 143–147, France, November 2011.

[6] Q. Liu, G. Wang, and J. Wu, "Secure and privacy preserving keyword searching for cloud storage services," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 927–933, 2012.

[7] X. Li, J. Li, and F. Huang, "A secure cloud storage system supporting privacy-preserving fuzzy deduplication," *Soft Computing*, vol. 20, no. 4, pp. 1437–1448, 2016.

[8] Y. Zhao and L. Zhu, *Service Evaluation-Based Resource Selection in Cloud Manufacturing, Cooperative Design, Visualization, and Engineering*, Springer International Publishing, 2014.

[9] Y. Wang, J. Wen, X. Wang, and W. Zhou, "Cloud service evaluation model based on trust and privacy-aware," *Optik - International Journal for Light and Electron Optics*, vol. 134, pp. 269–279, 2017.

[10] S. K. Garg, S. Versteeg, and R. Buyya, "A framework for ranking of cloud computing services," *Future Generation Computer Systems*, vol. 29, no. 4, pp. 1012–1023, 2013.

[11] R. Buyya, R. Ranjan, and R. N. Calheiros, "InterCloud: Utility-oriented federation of cloud computing environments for scaling of application services," in *Proceedings of the International Conference on Algorithms and Architectures for Parallel Processing*, pp. 13–31, Springer, Heidelberg, Berlin, Germany, 2010.

[12] X. G. Wang, J. Cao, and Y. Xiang, "Dynamic cloud service selection using an adaptive learning mechanism in multi-cloud computing," *The Journal of Systems and Software*, vol. 100, pp. 195–210, 2015.

[13] R. A. R. Shaikh and M. Sasikumar, "Dynamic parameter for selecting a cloud service," in *Proceedings of the 3rd IEEE International Conference on Computation of Power, Energy, Information and Communication, ICCPEIC 2014*, pp. 32–35, India, April 2014.

[14] Y. Yang, X. Peng, and D. Fu, "A framework of cloud service selection based on trust mechanism," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 25, no. 3, pp. 109–119, 2017.

[15] J. Lartigau, X. Xu, L. Nie, and D. Zhan, "Similarity evaluation based on intuitionistic fuzzy set for service cluster selection as cloud service candidate," in *Enterprise Interoperability*, pp. 36–49, Springer, Heidelberg, Berlin, Germany, 2013.

[16] X. Li, J. He, and Y. Du, "Trust based service optimization selection for cloud computing," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 10, no. 5, pp. 221–230, 2015.

[17] S.-H. Na and E.-N. Huh, "A broker-based cooperative security-SLA evaluation methodology for personal cloud computing," *Security and Communication Networks*, vol. 8, no. 7, pp. 1318–1331, 2015.

[18] Y. Wang and J. Zhou, "Community trust driven service selection method for cloud computing," *Journal of Huazhong University of Science and Technology (Natural Science Edition)*, vol. 43, no. 5, pp. 11–16, 2015.

[19] X.-L. Xie, L. Liu, and P. Zhao, "Trust model based on double incentive and deception detection for cloud computing," *Journal of Electronics and Information Technology*, vol. 34, no. 4, pp. 812–817, 2012.

[20] X. Li, J. He, B. Zhao, J. Fang, Y. Zhang, and H. Liang, "A method for trust quantification in cloud computing environments," *International Journal of Distributed Sensor Networks*, vol. 12, no. 2, Article ID 5052614, 2016.

[21] R.-Z. Du, J.-F. Tian, and H.-G. Zhang, "Cloud service selection model based on trust and personality preferences," *Journal of Zhejiang University (Engineering Science Edition)*, vol. 47, no. 1, pp. 53–61, 2013.

[22] W. Fan, S. Yang, and J. Pei, "A novel two-stage model for cloud service trustworthiness evaluation," *Expert Systems with Applications*, vol. 31, no. 2, pp. 136–153, 2014.

[23] S. Ding, S. Yang, Y. Zhang, C. Liang, and C. Xia, "Combining QoS prediction and customer satisfaction estimation to solve cloud service trustworthiness evaluation problems," *Knowledge-Based Systems*, vol. 56, pp. 216–225, 2014.

[24] C. H. Hu, J. B. Liu, and J. X. Liu, "Services selection based on trust evolution and union for cloud computing," *Journal of China Institute of Communications*, vol. 32, no. 7, pp. 71–79, 2011.

[25] Y. Wang, J. Wen, W. Fang, W. Zhou, and X. Wang, "A model of web service evaluation based on grey theory and combining weights," *Journal of Computational Information Systems*, vol. 11, no. 17, pp. 6497–6508, 2015.

[26] Z. Pawlak, "Rough classification," *International Journal of Man-Machine Studies*, vol. 20, no. 5, pp. 469–483, 1984.

[27] T. L. Saaty, "A scaling method for priorities in hierarchical structures," *Journal of Mathematical Psychology*, vol. 15, no. 3, pp. 234–281, 1977.

[28] J. L. Deng, *Grey System Theory Tutorial*, Huazhong University of Science and Technology Press, Wuhan, China, 1990.