A Method for Service Evaluation Based on Fuzzy Theory for Cloud Computing

Liangmin Guo*, Yonglong Luo, Xiaokang He, Guiyin Hu and Yan Dong

School of Mathematics and Computer Science, Anhui Normal University

Wuhu, 241003 - China

[e-mail: lmguo@ustc.edu.cn]

*Corresponding author: Liangmin Guo

Received October 12, 2016; revised January 11, 2017; accepted February 3, 2017; published April 30, 2017

Abstract

Aiming at the phenomenon of false information issued by service providers in cloud computing environment, a method for service evaluation based on fuzzy theory is put forward in this paper. According to the quality of services provided by cloud service providers and their behavior during interactions, a trust relationship between cloud service providers and cloud service consumers is established, which can be quantified by using fuzzy theory. The quality of services is evaluated by drawing on the trust relationship. In our method, the recommendation credibility of a cloud service consumer is determined through behavior similarity with evaluators and a praise factor. The introduction of the praise factor better suits the phenomenon of a high-quality service getting more repeat customers. The negative impact of dishonest customers is reduced, and the accuracy of trust and cloud service quality evaluation is improved by introducing a confidence factor that can be dynamically adjusted. The experimental results show that our method can effectively and accurately evaluate the trust value and service quality of providers, while weakening the influence of dishonest consumers, and quickly detect dishonest service providers. This is beneficial for consumers trying to find high quality service providers for similar services.

Keywords: Cloud service evaluation; trust; fuzzy theory; confidence factor

This work was supported by the National Natural Science Foundation of China (No. 61370050, No. 61672039, No. 61602009), Natural Science Foundation of Anhui Province (No. 1508085QF133, No. 1608085MF145), Research Program of Anhui Province Education Department (No. KJ2014A088).

https://doi.org/10.3837/tiis.2017.04.001 **ISSN : 1976-7277**

1. Introduction

Cloud computing is a relatively new pattern for business computing, which is supported by data centers usually based on virtualization technology, and where the cloud infrastructure, development platform and software can all be delivered as a paid service [1-2] (i.e., IaaS, PaaS, and SaaS), as shown in **Fig. 1**. As the number of cloud service providers (CSPs) increases and the cloud environment becomes more and more complex, cloud service consumers (CSCs) will face many challenges [3] such as privacy, security, availability, and other sensitive issues. One of the principal challenges is how a CSC can be sure of a CSP's honesty (i.e., identification of reliable CSPs), and know that they get what a CSP is promising. Some CSPs may provide false QoS (Quality of Service) information. This false information will have an effect on the selection of CSPs by CSCs, making it more difficult to find services that can satisfy their requirements. In this service-oriented environment, there is a need to know whether a CSP can be trusted or not (i.e. the credibility of CSPs). Therefore, to ensure smooth operation of service-oriented systems, the CSCs must establish trust with CSPs, and evaluate the service quality of these CSPs. Although some trust-based evaluation methods of QoS have been proposed, the problem of evaluation of QoS still warrants further research. On one hand, the accuracy of evaluation is vitally important. If it is done well enough, high quality services will be selected by CSCs, and poor quality services will be weeded out. On the other hand, dishonest CSPs need to be detected very quickly to reduce their impact on CSCs.

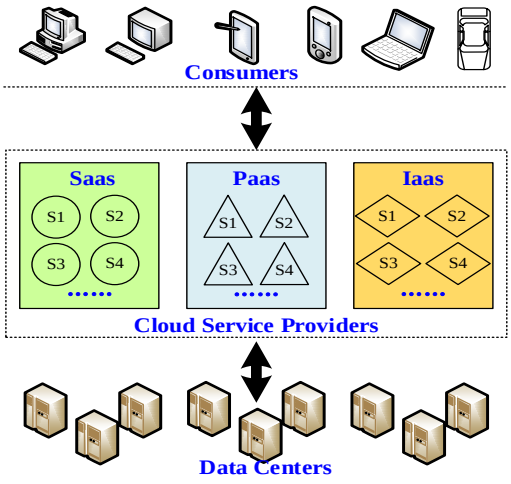


Fig. 1. Cloud service infrastructure

Therefore, in this paper, we propose a method for service evaluation based on fuzzy theory. It adopts fuzzy theory to compute direct trust value and recommendation trust value according to consumer ratings of different service attributes. Then, in terms of announced QoS and actual QoS provided by CSPs and their final trust values, the overall QoS is evaluated. In our method, a confidence factor is introduced and used to dynamically adjust weights corresponding to the values of direct and indirect evaluation, which are derived from a praise factor and a credibility factor. The praise factor reflects QoS according to the corresponding CSP's past behavior, and the credibility factor represents the credibility of all recommendations. When the value of the praise factor or the credibility factor is small, direct experience is considered more important, i.e., the value of the confidence factor should be larger. By dynamically adjusting the confidence factor, the negative impact of indirect evaluation from dishonest customers can be weakened to improve the accuracy of comprehensive evaluation, and dishonest cloud service providers can be detected quickly.

The main contributions of this paper include: (1) a trust model based on fuzzy theory for evaluating the trust relationship between cloud service providers and cloud service consumers, (2) a new evaluation method for effectively and accurately evaluating the QoS of providers, and (3) experimentation to validate this new method.

The remainder of this paper proceeds as follows. Section 2 explores the related works. Section 3 introduces the description of our model. A cloud trust evaluation model based on fuzzy theory is presented in Section 4. Section 5 proposes an evaluation method for cloud service quality. In section 6, we analyze our trust model and its time complexity, followed by an experimental evaluation of our method in Section 7. Finally, section 8 summarizes all of our research.

2. Related Work

In this section, we review relevant literature on evaluation of cloud service quality and trust.

2.1 Evaluation of Cloud Service Quality

In recent years, a few scholars have performed research in the field of evaluation of cloud service quality. Huang [4] proposed an evaluation model for cloud services aimed only at establishing an evaluation model from the service perspective and service characteristics, which can help CSCs choose the same or a similarly functioning cloud service. Choi et al. [5] presented a service quality evaluation method for cloud computing based on the preferences of consumers and attributes weighted by using the analytic network process. A QoS evaluation method for cloud computing has been presented by Wang et al. [6], which uses fuzzy synthetic decision to evaluate CSPs according to consumer preferences, and computes

the uncertainty of cloud services through the use of a cloud model based on monitored QoS data. However, the methods described above do not consider the credibility of entities. To resolve this problem and help CSCs to select the trustworthy CSPs, some researchers have proposed various solutions. Ma et al. [34] proposed a novel recommendation approach for trustworthy services with user preference awareness, which identifies user usage preference, trust preference and cost preference, then uses dynamic fuzzy clusters to select the most suitable services to recommend to new users. However, the malicious evaluations and false evaluations from consumers are not considered in [34], which leads to the inaccuracy of evaluation (or even recommend dishonest service providers to new users). Specifically, aiming at the problem of CSPs providing some false QoS information, Hu et al. [7-9] proposed a method of service evaluation based on trust reasoning, which uses a probability density function to represent the credibility of entities and correct QoS information using this credibility.

2.2 Trust

The concept of trust, which is well understood in everyday life, comes from the social sciences [10]. As it can serve as the basis for making decisions in many complex situations, it has been successfully applied in many fields such as information technology, commerce, and economics. Many scholars have proposed different evaluation methods for deriving trust values, including evaluation based on simple calculations [11], probability-based trust evaluation [7-9, 12-14], trust evaluation using fuzzy mathematics [15-19], and evaluation based on cloud models [20]. Some other methods have been proposed specifically for use in cloud environments. Alhamad et al. [21] and Chakraborty et al. [22] presented SLA-based trust models for evaluating the trust of CSPs, which are mainly based on QoS parameters defined in the SLA, and do not consider security. Habib et al. [23] and Noor et al. [24-25] proposed trust models to evaluate the trust of CSPs based on CSCs feedback. Xie et al. [26] proposed a dual incentive system, based on trust and deception detection models, to reflect the true service behavior of CSPs. Sato et al. [27] proposed a trust model that enhances existing clouds with internal and contracted trust to manage the quality of cloud service. Wang et al. [28] proposed a measurement model for evaluating the trustworthiness of cloud services, which considers trust factors provided by multiple trust dimensions. Fan et al. [29] also proposed a multi-dimensional trust model, which is based on an evidential reasoning approach. Similarly, Chiregi et al. [30] proposed a model that determines trust values based on attributes such as availability, reliability, data integrity, identity, and capability, and considers the influence of opinion leaders and removing the effects of troll entities. Tang et al. [31] proposed a trust evaluation method that combines objective and subjective trust, where objective trust and subjective trust are based on direct experience and indirect experience respectively. Rajendran et al. [32] also proposed a hybrid trust model for

evaluating CSPs by objective and subjective trust into consideration.

However, there is room for improvements regarding effective trust evaluation. For example, most of the evaluation methods depend on direct and indirect experience or multiple trust factors and lack sufficient weighting abilities. In references [28] and [31], though the weights are adjustable, both methods still suffer from deficiencies. In [28], the weights are determined by display level, visitation frequency and a custom-defined usefulness ratio, so this makes it vulnerable to malicious reviews. Reference [31] is based on the assumption that a majority of users are honest, and that a dishonest user gives more unfair ratings than fair ratings, and it does not consider attenuation of the ratings as time goes on.

Furthermore, CSC trust in CSPs is subjective, meaning fuzzy, random and uncertain [33]. It is difficult to describe and validate accurately. In methods based on probability, the subjectivity and fuzziness of trust is identical to true randomness. These methods based on probability and simple calculation do not reflect the facticity of trust relationships, and trust evaluations tend to be inaccurate. In this paper, we use fuzzy theory to evaluate trust and estimate quality of service accurately as possible. We also propose solutions for the problems mentioned above, including false QoS information and the adjustment of weights. Building upon the work of Hu et al. [7-9], we propose a method of service evaluation based on fuzzy theory, which can accurately and effectively evaluate trust and QoS of CSPs, while weakening the influence of dishonest consumers, and quickly detect dishonest CSPs.

3. Model Description

Suppose there are n_{csp} CSPs in a system, which are $csp_1, csp_2, ..., csp_{n_{csp}}$ respectively, and that there are n_{csc} CSCs, which are $csc_1, csc_2, ..., csc_{n_{\text{csc}}}$ respectively. The evaluation information of CSCs for CSPs is stored on a credible public platform and can be obtained by other CSCs. For convenience of description, we only consider four service attributes: price, security, reliability, and completion time. A CSP (csp_B) reports its QoS information vector $q^i_{csp_B}$ in the i-th interaction, expressed in Eq. (1).

$$q^i_{csp_B} = \left(q^i_{csp_B(1)}, q^i_{csp_B(2)}, q^i_{csp_B(3)}, q^i_{csp_B(4)}\right) \tag{1}$$

$q^i_{csp_B(j)}$ $\left(0.5 < q^i_{csp_B(j)} \le 1\right)$ is the j-th $\left(j = 1,2,3,4\right)$ dimensional of QoS information reported by csp_B. The first dimension is price, the second is security, the third is reliability and the fourth is completion time. Higher values in these dimensions indicate that the reported service quality is better.

After a CSC (csc_A) interacts with csp_B, it will have a QoS vector named $Q^i_{csc_A, csp_B}$ based to the interaction, which is defined in Eq. (2). $Q^i_{csc_A, csp_B(j)}$ $\left(0 < Q^i_{csc_A, csp_B(j)} \le 1\right)$ is the real value of the j-th $\left(j = 1,2,3,4\right)$ dimension of the QoS vector. Assume that only the evaluation information of the T most recent interactions is saved in the system.

$$Q^{i}_{csc_A,csp_B} = \left(Q^{i}_{csc_A,csp_B(1)}, Q^{i}_{csc_A,csp_B(2)}, Q^{i}_{csc_A,csp_B(3)}, Q^{i}_{csc_A,csp_B(4)}\right) \quad (2)$$

4. Trust Model based on Fuzzy Theory

For this model, we measure trust values from two different dimensions, the direct trust dimension, and the recommendation trust dimension. For the above csc_A and csp_B, direct trust comes from the evaluator csc_A's direct experience with csp_B, and recommendation trust (indirect trust) is generated from other CSCs' experience with csp_B. These other CSCs are referred to as recommenders. They can be quantified using the following method.

The following discussion is based on a nonempty set $U = \left\{csp_1, csp_2, ..., csp_{n_{csp}}\right\}$. Trust in U is divided into five trust grades (five fuzzy subsets $TR_i = Y(U)$, $i = 1,2,3,4,5$): *full distrust* (TR_1), *distrust* (TR_2), *basic trust* (TR_3), *trust* (TR_4), and *full trust* (TR_5). The trust grades, their meanings, and their quantificational indices are shown in **Table 1**. Every fuzzy subset TR_i ($i = 1,2,3,4,5$) is described by four dimensions: service price, security, reliability, and completion time, denoted $\left(TR_{i(1)}, TR_{i(2)}, TR_{i(3)}, TR_{i(4)}\right)$.

In general, the trust values of CSPs follow an approximately normal distribution, which can reflect the real application scenarios. This means that the number of CSPs with particularly high trust values and particularly low trust values is small. Therefore in this research we assume that every fuzzy subset is approximately a large partial normal distribution. Suppose the trust rating vector of a CSP csp_x is $\left(x_{(1)}, x_{(2)}, x_{(3)}, x_{(4)}\right)$, and the corresponding membership function can be approximated by Eq. (3), where $\overline{x_{i(j)}}$ and $\sigma_{i(j)}$ are the average and the standard deviation of the j-th component of a trust rating vector of grade i respectively. When we calculate direct trust value, the above trust rating vector is the direct trust rating vector. When we calculate recommendation trust value, it becomes the recommendation trust rating vector.

Table 1. Trust grade, meaning and quantificational index

Grade	Meaning	Value range
1	*full distrust*	$[0,0.2]$
2	*distrust*	$(0.2,0.4]$
3	*basic trust*	$(0.4,0.6]$
4	*trust*	$(0.6,0.8]$
5	*full trust*	$(0.8,1]$

$$\mathrm{P}_{i(j)}(x_{(j)}) = \begin{cases} 0 & , \quad \left|x_{(j)} - \overline{x_{i(j)}}\right| > \sigma_{i(j)} \\ 1 - \left(\dfrac{x_{(j)} - \overline{x_{i(j)}}}{\sigma_{i(j)}}\right)^2 & , \quad \left|x_{(j)} - \overline{x_{i(j)}}\right| \le \sigma_{i(j)} \end{cases} \quad (3)$$

The membership degree of csp_x in the i-th $(i=1,2,3,4,5)$ trust grade is defined in Eq. (4), where $\omega_{(j)}$ is the weight of the j-th dimensional evaluation, and $\sum_{j=1}^{4}\omega_{(j)}=1,\ 0\le\omega_{(j)}\le 1$.

$$P_i(x)=\sum_{j=1}^{4}\omega_{(j)}\,\mathrm{P}_{i(j)}(x_{(j)}) \tag{4}$$

According to the principle of maximum membership degree, if $P_i(x)=\bigvee_{k=1}^{5}\{P_k(x)\}$ for $\forall csp_x\in U$, then csp_x belongs to TR_i, we can calculate the trust grade for csp_x. For example, if $P_1(x)=0.1$, $P_2(x)=0.6$, $P_3(x)=0.9$, $P_4(x)=0.5$, and $P_5(x)=0.4$, then csp_x belongs to TR_3. According to the trust value ranges of the different grades, the trust value of a CSP (csp_x), named $t(x)$, is given by Eq. (5), where $\bar{x}$ is equal to $\sum_{j=1}^{4}\omega_{(j)}x_{(j)}$. $\bar{x}_{\max}$ is the upper limit of $\bar{x}$, and i is the trust grade.

$$t(x)=\begin{cases}0.4(\bar{x}+1) & ,\ i=1\\ 0.05(10\bar{x}+9) & ,\ i=2\\ 0.2\left(10\bar{x}+3\right) & ,\ i=3\\ 0.2\left(100\bar{x}+3\right) & ,\ i=4\\ 0.2\left(\dfrac{\bar{x}+4\bar{x}_{\max}-0.05}{\bar{x}_{\max}-0.01}\right) & ,\ i=5\end{cases} \tag{5}$$

5. Evaluation of Cloud Service Quality

In this section we discuss how to evaluate the trust value and QoS value of csp_B.

5.1 Trust Evaluation of CSPs

5.1.1 Direct Trust Evaluation

The direct trust of csc_A in csp_B is approximated by the difference ratio between the actual QoS vector and the reported QoS information vector. Because the most recent service interactions more accurately reflect the quality of service that csp_B provides, we introduce the time decay function defined by Eq. (6). In Eq. (6), i is used to indicate the i-th interaction, and $\theta\in[0,1]$ is a regulatory factor used to control the speed of attenuation. We can see that the closer θ is to one, the earlier attenuation occurs.

$$\mu(i)=1-\frac{1}{i}\theta \tag{6}$$

By combining the T interactions of csc_A with csp_B, we can drive the direct trust rating vector $\left(\Delta_{csc_A,csp_B}(1),\Delta_{csc_A,csp_B}(2),\Delta_{csc_A,csp_B}(3),\Delta_{csc_A,csp_B}(4)\right)$. $\Delta_{csc_A,csp_B(j)}$ is the difference ratio for the j-th dimension of the QoS vector, which can be computed using Eq. (7).

$$\Delta_{csc_A,csp_B(j)}=\frac{1}{T}\sum_{i=1}^{T}\mu(i)\left(\frac{Q^i_{csc_A,csp_B(j)}-q^i_{csp_B(j)}}{q^i_{csp_B(j)}}\right) \tag{7}$$

By using Eq. (4), we can compute the membership degree for direct trust to derive a trust grade, and then calculate the direct trust value DT_{csc_A,csp_B} using Eq. (5).

5.1.2 Recommendation Trust Evaluation

The recommendation trust of csc_A in csp_B is determined by all other CSCs not including csc_A, who have directly interacted with csp_B. In the real world, some consumers provide intentionally deceptive evaluations. For example, they can give unfairly negative evaluations for good CSPs, and unfairly positive evaluations for dishonest CSPs. The credibility of these recommendations will directly affect the recommendation trust evaluation. Suppose there are z recommenders $R_1, R_2, ..., R_z$, and that currently, the most recent actual QoS vectors of these recommenders for csp_B are $Q^i_{R_1,csp_B}, Q^i_{R_2,csp_B}, ..., Q^i_{R_z,csp_B}$ respectively. csc_A generally places greater trust in CSCs whose opinions are similar to their own. Thus, the recommendation credibility of R_k $(k = 1, 2, ..., z)$ in the j-th dimension of the QoS vector can be calculated from the similarity of evaluation results. In our research, this similarity is measured as the inverse of the difference of every dimensional real value weighted by a time decay factor. Furthermore, when the opinion of csc_A on csp_B is the same as R_k, i.e. $\sum_{i=1}^{m}\left(\mu(i)\left|Q^i_{csc_A,csp_B(j)} - Q^i_{R_k,csp_B(j)}\right|\right) = 0$, we consider its recommendation credibility equal to be one. This indicates that csc_A completely trusts the opinion of R_k. Therefore, the recommendation credibility of R_k $(k = 1, 2, ..., z)$, denoted $rc^{R_k}_{csc_A \to csp_B(j)}$, is computed as follows:

$$rc^{R_k}_{csc_A \to csp_B(j)} = \frac{1}{1 + \frac{1}{m}\sum_{i=1}^{m}\left(\mu(i)\left|Q^i_{csc_A,csp_B(j)} - Q^i_{R_k,csp_B(j)}\right|\right)} \tag{8}$$

where m $(m \le T)$ represents interactions. We use $rc^{R_k}_{csc_A \to csp_B(j)}$ as the weight of the direct trust rating of R_k for csp_B. The recommendation trust rating vector is denoted $\left(\Delta'_{csc_A,csp_B(1)}, \Delta'_{csc_A,csp_B(2)}, \Delta'_{csc_A,csp_B(3)}, \Delta'_{csc_A,csp_B(4)}\right)$, and $\Delta'_{csc_A,csp_B(j)}$ is calculated in Eq. (9).

$$\Delta'_{csc_A,csp_B(j)} = \frac{f_{csp_B}}{z}\sum_{k=1}^{z}\left(rc^{R_k}_{csc_A \to csp_B(j)} \times \Delta_{R_k,csp_B(j)}\right) \tag{9}$$

where $\Delta_{R_k,csp_B(j)}$ is the direct trust rating of the j-th dimension in the QoS vector of R_k for csp_B, $f_{csp_B} = \frac{n_{paise(csp_B)}}{n_{total(csp_B)}}$ is a praise factor, $n_{praise(csp_B)}$ is the amount of praise that csp_B gains, and $n_{total(csp_B)}$ is the total number of interactions for csp_B. Generally, when the quality of service that csp_B provides is equal to or better than its claim, it will gain praise. csp_B can also gain praise if the system can tolerate some deviation, such as if the difference $q^i_{csp_B(j)} - Q^i_{csp_A,csp_B(j)}$ of the j-th $(j = 1, 2, 3, 4)$ dimension is smaller than the threshold value δ_j. δ_j is derived from system tolerance and is typically close to zero. The reason for introducing the praise factor is to lessen the effect of dishonest evaluation from R_k on csp_B. If csp_B is dishonest, the f_{csp_B} of csp_B is typically low. Even though R_k already gave a high

evaluation to csp_B, f_{csp_B} can further adjust every dimension's value in the recommendation trust vector based on recommendation credibility, particularly when recommendation credibility is high. Similarly, f_{csp_B} can also further adjust every dimension's value if csp_B is an honest provider and can provide high quality services. In short, f_{csp_B} can more accurately represent the phenomenon of a high quality service attracting more repeat consumers.

Equations (4) and (5) can also provide the membership degree for recommendation trust, as well as the recommendation trust value IT_{csc_A,csp_B}.

5.1.3 Trust Value Integration

Combining the direct trust value and recommendation trust value, we gain the final trust value, shown in Eq. (10).

$$CT_{csc_A,csp_B} = \alpha DT_{csc_A,csp_B} + (1-\alpha) IT_{csc_A,csp_B} \tag{10}$$

where α is a confidence factor. α and 1-α are the weights corresponding to the values of direct trust and recommendation trust respectively. In many previous research literatures, the weights rely on user understanding of the importance of direct trust and recommendation trust to be assigned different values. But in our system, to adjust the weights dynamically, α is malleable and is determined by both f_{csp_B} and γ, specifically $\alpha = 1 - f_{csp_B} \times \gamma$. γ is a credibility factor for recommendations and reflects the importance of recommendations in the trust evaluation. It is an average of recommendation credibility of different recommenders, and is computed by using Eq. (11).

$$\gamma = \frac{1}{4z} \sum_{j=1}^{4} \sum_{k=1}^{z} rc_{csc_A \to csp_B(j)}^{R_k} \tag{11}$$

5.2 QoS Evaluation

Suppose that the real QoS values for csp_B from csc_A are $Q_{csc_A,csp_B}^1, Q_{csc_A,csp_B}^2, ..., Q_{csc_A,csp_B}^T$ respectively over the latest T interactions, where $Q_{csc_A,csp_B}^i = \left(Q_{csc_A,csp_B(1)}^i, Q_{csc_A,csp_B(2)}^i, Q_{csc_A,csp_B(3)}^i, Q_{csc_A,csp_B(4)}^i\right)$. Based on these T interactions between csc_A and csp_B, the direct QoS evaluation value DQ_{csc_A,csp_B} for csp_B from csc_A can be computed by using Eq. (12).

$$DQ_{csc_A,csp_B} = \frac{1}{T} \sum_{j=1}^{4} \sum_{i=1}^{T} \left(\omega_{(j)} \mu(i) Q_{csc_A,csp_B(j)}^i\right) \tag{12}$$

The indirect QoS evaluation value IQ_{csc_A,csp_B} is derived from CT_{csc_A,csp_B} and $q_{csp_B}^i$ $\left(i = 1,2,...,T\right)$, as shown in Eq. (13).

$$IQ_{csc_A,csp_B} = CT_{csc_A,csp_B} \cdot \frac{1}{T} \sum_{j=1}^{4} \sum_{i=1}^{T} \left(\omega_{(j)} \mu(i) q_{csp_B(j)}^i\right) \tag{13}$$

By combining DQ_{csc_A,csp_B} and IQ_{csc_A,csp_B}, we get the comprehensive QoS evaluation value, as shown in Eq. (14). The CSCs can then use this comprehensive value to select the best CSPs from those that offer the desired services.

$$CQ_{csc_A,csp_B} = \alpha DQ_{csc_A,csp_B} + (1-\alpha) IQ_{csc_A,csp_B} \tag{14}$$

Algorithm 1 summarizes the entire process of QoS evaluation for csp_B from csc_A.

Algorithm 1: QoS evaluation for csp_B from csc_A

Input: $q^i_{csp_B}$ $(i=1,2,...T)$; Q_{csc_A,csp_B}; $Q_{R_1,csp_B}, Q_{R_2,csp_B},..., Q_{R_z,csp_B}$

Output: CQ_{csc_A,csp_B}

1: Calculate $\Delta_{csc_A,csp_B(j)}$ to get direct trust rating vector;

2: Get DT_{csc_A,csp_B} using Eq. (4) and (5);

3: **for** each recommender R_k $(k=1,2,...,z)$ **do**

4: Calculate $rc^{R_k}_{csc_A \to csp_B(j)}$ and $\Delta_{R_k,csp_B(j)}$ using Eq. (8) and (9) separately;

5: **end for**

6: Get the recommendation trust value IT_{csc_A,csp_B};

7: $\alpha = 1 - f_{csp_B} \times \gamma$;

8: $CT_{csc_A,csp_B} = \alpha DT_{csc_A,csp_B} + (1-\alpha) IT_{csc_A,csp_B}$;

9: $DQ_{csc_A,csp_B} = \frac{1}{T}\sum_{j=1}^{4}\sum_{i=1}^{T}\left(\omega_{(j)}\mu(i)Q^i_{csc_A,csp_B(j)}\right)$, $IQ_{csc_A,csp_B} = CT_{csc_A,csp_B} \cdot \frac{1}{T}\sum_{j=1}^{4}\sum_{i=1}^{T}\left(\omega_{(j)}\mu(i)q^i_{csp_B(j)}\right)$;

10: $CQ_{csc_A,csp_B} = \alpha DQ_{csc_A,csp_B} + (1-\alpha) IQ_{csc_A,csp_B}$;

6. Theoretical Evaluation

6.1 Trust Model Analysis

In this section, we test if our trust model can accurately evaluate CSP behavior. We only consider direct trust evaluation here, because the method for calculating indirect trust is the same and would be redundant for testing purposes. We use 100 CSPs as a sample. The sample data set, meaning the QoS information and actual QoS of these CSPs, is generated by using a random function. The CSPs are then divided into five subsets according to the value of each component in the direct trust rating vector. The five subsets correspond to the five previously mentioned trust grades. **Table 2** shows the average and standard deviation of each component of the direct trust rating vector at each different trust grade. **Table 3** shows the direct trust rating vector of three of the sample CSPs from each trust grade. Of the three CSPs in each grade: one's direct trust value is near the minimum in the grade, another's is near the median, and the other's is near the maximum. By using Equations (4) and (5), we can calculate their direct trust grades and values, also shown in **Table 3**. When computing the direct trust value for csp_{13}, csp_{14} and csp_{15}, we suppose $\bar{x}_{\max} = 0.85$. From Table 3 we can see that the model can accurately evaluate direct trust. However, the accuracy is affected by the average and standard deviation of the sample data set. If sampling error is large, i.e., the average and standard deviation of every sampled grade cannot describe the corresponding real grade, we find that the model cannot judge the grade of a few evaluation

vectors, which are usually on the boundary of two adjacent grades. Thus, the error rate is very low even with moderate sampling error.

Table 2. Average and standard deviation of different trust grades

Grade	Price		Security		Reliability		Time	
	average	deviation	average	deviation	average	deviation	average	deviation
1	-0.711	0.194	-0.707	0.191	-0.704	0.195	-0.683	0.194
2	-0.262	0.148	-0.255	0.157	-0.303	0.138	-0.308	0.143
3	-0.046	0.037	-0.036	0.035	-0.052	0.039	-0.039	0.031
4	0.003	0.003	0.002	0.003	0.004	0.003	0.002	0.002
5	0.422	0.389	0.403	0.368	0.372	0.380	0.378	0.384

Table 3. Direct trust rating vector, trust grade, and trust value

CSP	Direct trust rating vector	Grade	Direct trust value
csp_1	(-0.80, -0.90, -0.90, -0.95)	1	0.05
csp_2	(-0.75, -0.60, -0.80, -0.50)	1	0.14
csp_3	(-0.50, -0.60, -0.50, -0.50)	1	0.19
csp_4	(-0.49, -0.48, -0.49, -0.45)	2	0.21
csp_5	(-0.30, -0.25, -0.40, -0.28)	2	0.30
csp_6	(-0.10, -0.10, -0.10, -0.10)	2	0.40
csp_7	(-0.09, -0.07, -0.09, -0.08)	3	0.44
csp_8	(-0.04, -0.05, -0.04, -0.03)	3	0.52
csp_9	(-0.01, -0.01, -0.01, -0.01)	3	0.58
csp_{10}	(0.00, 0.00, 0.00, 0.00)	4	0.60
csp_{11}	(0.00, 0.01, 0.00, 0.01)	4	0.70
csp_{12}	(0.01, 0.01, 0.01, 0.01)	4	0.80
csp_{13}	(0.02, 0.03, 0.02, 0.02)	5	0.81
csp_{14}	(0.30, 0.25, 0.35, 0.40)	5	0.88
csp_{15}	(0.80, 0.80, 0.80, 0.80)	5	0.99

6.2 Complexity Analysis

The cost of computing the trust rating vector depends on the number of recent interaction records saved in the system, denoted T. The cost of the direct trust value is $O(4T+20)$. The cost of computing the indirect trust value is $O(4T\times z\times m+20)$. The computing of α is $O(4z)$. Thus, the total cost of trust evaluation is $O(4T+20+4T\times z\times m+20+4z)$. Based on previous analysis, the total cost of QoS evaluation would be $O(4T+20+4T\times z\times m+20+4z+8T)=O(12T+4T\times z\times m+4z+40)$. If we assume the number of dimensions is d, then the total cost of QoS evaluation would be

$O(3d \times T + d \times T \times z \times m + d \times z + 10d)$. Generally, if we treat T and m as constants, then the cost is $O(d \times z)$. The total cost of finding the best CSP in n_{csp} CSPs is $O(d \times z \times n_{csp})$. In references [7-9], the total cost is $O(d \times h \times n_{csp}^2)$, where h is the depth of trust reasoning. Therefore, the time efficiency of our proposed method is superior.

7. Experimental Evaluation

This section discusses experiments performed to evaluate our proposed approach. All experiments are implemented in C++.

In our experiments, CSCs are divided into two types, honest CSCs (CSC1) and dishonest CSCs (CSC2). CSPs are also divided into two types, honest CSPs (CSP1) and dishonest CSPs (CSP2). CSC1s always provide accurate evaluation. CSC2s make unfairly negative evaluations for CSP1s and unfairly positive evaluations for CSP2s. CSP1s always provide high-quality service to CSCs. CSP2s claim to provide high-quality service to CSCs, but actually provide poor-quality service. In the experimental evaluation, we mainly focus on analyzing the effectiveness of our proposed method for CSP1s and CSP2s, and compare it with the trust reasoning based method (abbreviated as TR method) [7-9].

7.1 Parameter Settings

Some experimental parameters are set as follows:

(1) There are 500 CSCs and 300 CSPs in the experimental environment. And the proportion of each type is shown in **Table 4**.

(2) In each round, approximately 250 CSCs make service requests, and each of these 250 CSCs send requests to 10 CSPs.

Table 4. Proportion of entities in different scenarios

Scenarios	CSC1	CSC2	CSP1	CSP2
1	80%	20%	85%	15%
2	50%	50%	85%	15%
3	20%	80%	85%	15%

(3) We assume that all CSPs claim to provide high-quality service, and their initial j-th $(j = 1,2,3,4)$ dimensional reported QoS value is a random number between 0.7 and 0.8.

(4) For a CSP2, we assume its j-th $(j = 1,2,3,4)$ dimensional reported QoS value is between 2 and 2.5 times the real value.

(5) To avoid the real value of the j-th $(j = 1,2,3,4)$ dimensional QoS $Q^i_{csc_A, csp_B(j)}$ getting too small, we assume that $Q^i_{csc_A, csp_B(j)}$ is larger than 0.1. To avoid $Q^i_{csc_A, csp_B(j)}$

getting too large, we impose a limit of $Q^i_{csc_A,csp_B(j)} - q^i_{csp_B(j)} \le 0.4$. If csc_A is honest and csp_B is honest, $-\delta_j \le Q^i_{csc_A,csp_B(j)} - q^i_{csp_B(j)} \le 0.1$.

(6) Suppose the weights of every dimension are equal, i.e. $\omega_{(j)} = 1/4 \quad (j = 1,2,3,4)$.

(7) For the TR method, we set the depth of trust reasoning equal to one, because this typically provides the best results [8].

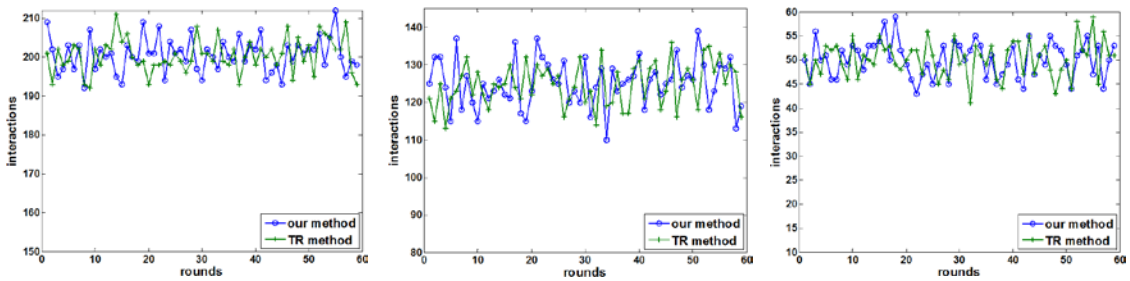
7.2 Analysis and Comparison

7.2.1 CSP1

From the experiments, we observe three properties of a CSP1 e_{csp1}: interactions, final trust value, and QoS evaluation value. These are labeled as scenario 1, scenario 2, and scenario 3 respectively. e_{csp1} is one of 10 CSPs in each round, and is always the same, the other 9 CSPs are chosen randomly.

(1) Interactions

As shown in **Fig. 2**, the interactions between CSC1s and e_{csp1} are all relatively stable for both methods in the three scenarios. For our method, because the confidence factor α is determined by both praise and credibility factors and can better adjust the weights for direct and indirect experience, the interactions remain stable and less affected even when the number of CSC2s increases. There are large differences among values of interactions in the three scenarios. This is because the number of CSC1s decreases as the number of CSC2s increases. **Table 5** shows the standard deviation of interactions for the three scenarios. It can be seen that our method performs slightly better than the TR method when the number of CSC2s increases.



(a) scenario 1 **(b)** scenario 2 **(c)** scenario 3

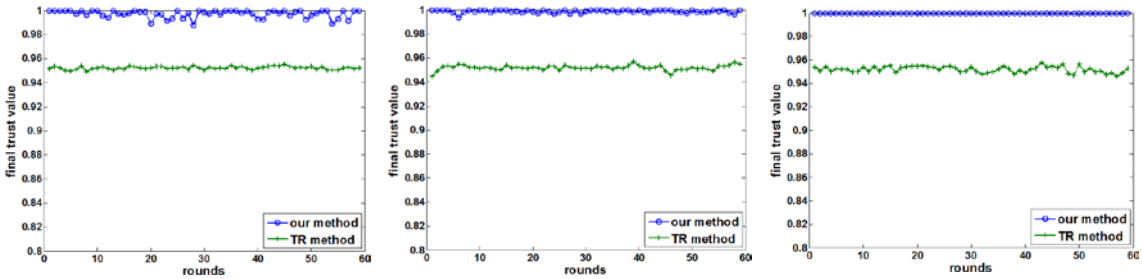
Fig. 2. Interactions(CSP1)

Table 5. Standard deviation of interactions

Scenarios	Our method	TR method
1	4.39	4.35
2	5.94	6.29
3	3.72	3.76

(2) Final trust value

Fig. 3 shows the trust values of e_{csp1} computed by both methods in the three scenarios. The final trust values obtained by both methods remain greater than 0.95. For our method, as the number of CSC2s increases, α will grow and allow the direct trust value to dominate in the final trust value little by little. From **Fig. 3** we can see that the fluctuation of the trust values decreases over time, meaning increasing numbers of CSC2s have little immediate impact on final trust value. For the TR method, however, the fluctuation range increases over time. **Table 6** shows the standard deviations in final trust value. It can be seen that our method effectively weakens the influence of CSC2s.



(a) scenario 1 **(b)** scenario 2 **(c)** scenario 3

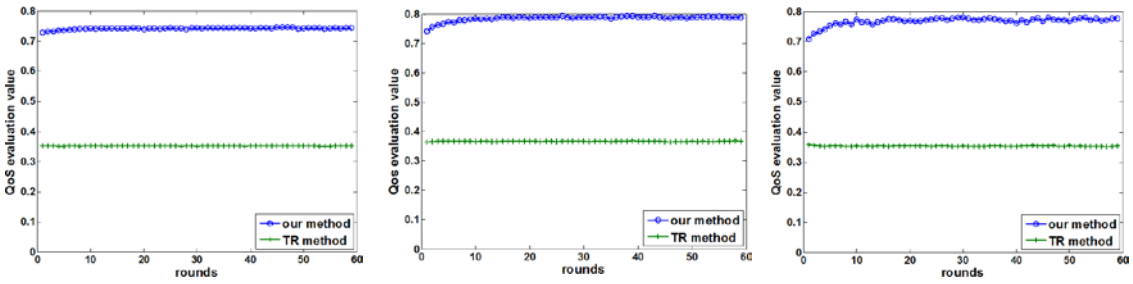
Fig. 3. Final trust value (CSP1)

Table 6. Standard deviation of trust values

Scenarios	Our method	TR method
1	0.03	0.01
2	0.001	0.02
3	0.00003	0.03

(3) QoS evaluation value

The overall QoS evaluation values of e_{csp1} from both methods in the three scenarios are shown in **Fig. 4**. With increasing interactions, the QoS evaluation value gradually increases during the first 10 rounds and then begins to level off when using our method. Initially, the direct QoS evaluation value dominates in the overall QoS evaluation value. When the CSC1s have accurate views on e_{csp1} for each interaction, the credibility factor γ tends to be larger, which results in a smaller value of α. The impact of the indirect QoS evaluation value grows, and the overall QoS evaluation value will gradually increase. Then, when α stabilizes, the overall QoS evaluation value will also stabilize. In the TR method, because the weights of the direct QoS evaluation value and indirect QoS evaluation value cannot be adjusted well, the change in the overall QoS evaluation value is very small throughout. From **Fig. 4** we can also see that the overall QoS evaluation values achieved by our method are much closer to the reported QoS values.



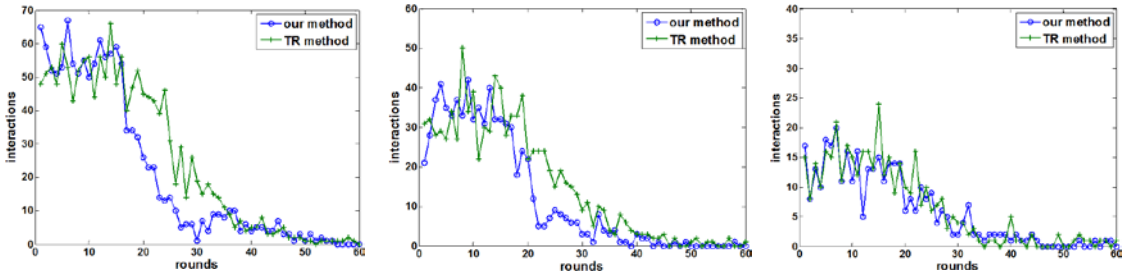
(a) scenario 1 **(b)** scenario 2 **(c)** scenario 3

Fig. 4. QoS evaluation value (CSP1)

7.2.2 CSP2

We now observe the same three properties of a CSP2 e_{csp2} in the same three scenarios. Again, we use a fixed CSP2 e_{csp2} as one of the 10 CSPs in each round, with the other nine being chosen randomly. Additionally, we assume that CSP2s provide services that match their claims during the first 15 rounds, and expose their dishonesty in subsequent rounds.

(1) Interactions



(a) scenario 1 **(b)** scenario 2 **(c)** scenario 3

Fig. 5. Interactions(CSP2)

Table 7. Total interactions

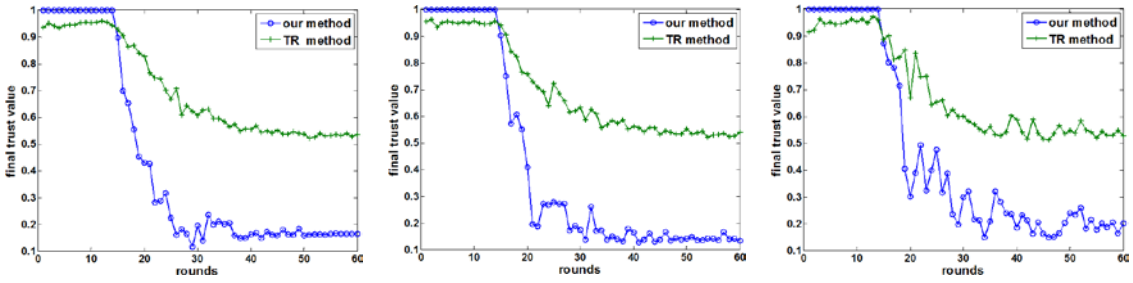
Scenarios	Our method	TR method
1	1254	1479
2	738	914
3	359	390

As shown in **Fig. 5**, the interactions between CSC1s and e_{csp2} are relatively stable for approximately 15 rounds, for both methods, in the three scenarios, because of our assumption made above. After that point, the number of interactions begins to decrease as the number of rounds increases because e_{csp2} provides lower quality services. As shown in **Fig. 5**, our method can effectively reduce the number of interactions with e_{csp2}, and it outperforms the TR method. In scenarios 1 and 2, after approximately 30 rounds, the number

of interactions when using our method is reduced to a lower value, but the TR method needs approximately 37 rounds. Thus, our method can more quickly detect the dishonest CSP e_{csp2}. **Table 7** verifies this by showing that our method achieves a lower number of totally interactions with e_{csp2}.

(2) Final trust value

Fig. 6 displays the final trust values of e_{csp2} from both methods across the three scenarios. Because it provides high-quality services during the first 15 rounds, it has a high trust value within that period. After approximately 15 rounds, however, its trust value all begins to fall. Using our method, the trust value is adjusted very quickly, and after approximately 10 rounds of dishonest interactions, it reaches the real value. Even when the proportion of CSC2s reaches 80 percent, our method still performs well. In the TR method, however, this change is not as clear as the change achieved by our method, and the calculated trust value does not quickly drop to the real value.



(a) scenario 1 **(b)** scenario 2 **(c)** scenario 3

Fig. 6. Final trust value (CSP2)

We use the ratio of the trust value's variation to the number of completed rounds to express the rate of change in trust value, as shown in Eq. (15). The rate of change, variation, and number of rounds completed are denoted by $Rate_{trust}$, V_{trust}, and $round_{completed}$ respectively. **Table 8** shows the rate of change in trust value after the first 15 rounds for both methods in the three scenarios. Our method outperforms the TR method, and can more quickly detect CSP2s.

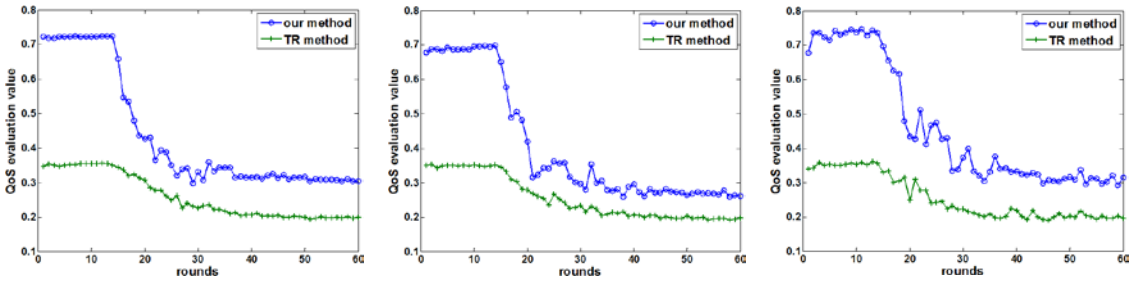
$$Rate_{trust} = V_{trust} \Big/ round_{completed} \tag{15}$$

Table 8. Rate of change in trust value

Scenarios	Our method	TR method
1	0.076	0.019
2	0.059	0.020
3	0.054	0.021

(3) QoS evaluation value

Fig. 7 shows the overall QoS evaluation values for e_{csp2}. After 15 rounds, the QoS evaluation values decrease as the rounds increase for both methods, because e_{csp2} provides lower quality services than it reports. After this decrease, the values level off. The rate of change for QoS evaluation values with our method is faster than the change using the TR method. This phenomenon indicates that our method can more quickly react to the dishonesty of e_{csp2}. Additionally, the QoS evaluation value achieved by our method is more accurate. During the first 15 rounds, the QoS evaluation value is approximately 0.7, and after 30 rounds, it meets the previous assumption that the reported QoS value is 2 to 2.5 times the real value.



(a) scenario 1 **(b)** scenario 2 **(c)** scenario 3

Fig. 7. QoS evaluation value (CSP2)

8. Conclusions and Future Works

This paper proposed a service evaluation method based on the fuzzy theory for cloud computing. We use fuzzy theory to compute direct trust values and recommendation trust values, then calculate their final trust value, and evaluate the QoS in terms of reported QoS and real QoS for the CSPs. We introduced a dynamic confidence factor to minimize the negative impact of CSC2s, and improve the accuracy of trust and service quality evaluation. Experimentation shows that our method can effectively and accurately evaluate the trust value and service quality of providers, while weakening the influence of CSC2s, and quickly detect CSP2s.

Our method considers four attribute indices to evaluate service quality, and can be easily extended to for larger multi-dimensional cases. These indices should be chosen according to type of service being evaluated. In future works, we will further optimize our method of cloud service evaluation, enhance the recommendation trust evaluation to better restrain CSC2s, and improve experimental environments to ensure that experimental data is more accurate.

References

[1] Cloud computing, 2012. Article (CrossRef Link).

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: a berkeley view of cloud computing," 2009. Article (CrossRef Link).

[3] Chunming Rong, Son T. Nguyen, Martin G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," *Computer and Electrical Engineering*, no. 39, pp. 47-54, 2013. Article (CrossRef Link).

[4] Y. Huang, "The research on evaluation model of cloud service based on QoS and application," *Master, Thesis*, Zhejiang GongShang University, CN, 2013.

[5] C. R. Choi, H. Y. Jeong, "Quality evaluation and best service choice for cloud computing based on user preference and weights of attributes using the analytic network process," *Electronic Commerce Research*, vol. 14, no. 3, pp. 245-270, 2014. Article (CrossRef Link).

[6] S. G. Wang, Z. P. Liu, Q. B. Sun, H. Zou, F. C. Yang, "Towards an accurate evaluation of quality of cloud service in service-oriented cloud computing," *Journal of Intelligent Manufacturing*, vol. 25, no. 2, pp. 283-291, 2014. Article (CrossRef Link).

[7] C. H. Hu, X. X. Luo, S. C. Wang, Y. Liu, "Approach of service evaluation based on trust reasoning for cloud computing," *Journal on Communication*s, vol. 32, no.12, pp. 72-81, 2011. Article (CrossRef Link).

[8] C. H. Hu, B. G. Chang, H. Xu, Q. L. Zhao, "Approach of service combination based on deepness trust reasoning in complex cross-organizational collaboration," *Journal of Central South University (Science and Technology)*, vol. 43, no. 2, pp. 567-575, 2012.

[9] C. H. Hu, X. H. Chen, M. Wu, J. X. Liu, "A service trust negotiation and access control strategy based on SLA in cloud computing," *Science China: Information Science*s, vol. 42, no. 3, pp. 314-332, 2012. Article (CrossRef Link).

[10] M. Blaze, J. Feigenbaum, J. Lacy, "Decentralized trust management," in *Proc. of the IEEE 17th Symposium on Security and Privacy*, Oakland, CA, pp. 164-173, 1996. Article (CrossRef Link).

[11] A. A. Rahman, S. Hailes, "A distributed trust model," in *Proc. of the new Security Paradigms Workshop*, Cambria, UK, pp. 48-60, 1998. Article (CrossRef Link).

[12] A. Jøsang and R. Ismail, "The beta reputation system," in *Proc. of the 15th Bled Electronic Commerce Conference*, Bled, pp. 41-55, 2002. Article (CrossRef Link).

[13] W. T. Teacy, J. Patel, N. R. Jennings, M. Luck, "Travos: trust and reputation in the context of inaccurate information sources," *Autonomous Agents and Multi-Agent Systems*, vol. 12, no. 2, pp.183-198, 2006. Article (CrossRef Link).

[14] R. Zhou, K. Hwang, "Powertrust: a robust and scalable reputation system for trusted peer-to-peer computing," *IEEE Transactions on Parallel and Distributed Systems*, vol.18, no. 4, pp. 1-14, 2007. Article (CrossRef Link).

[15] Shanshan Song, Kai Hwang, Runfang Zhou, Yu-Kwong Kwok, "Trusted P2P transactions with fuzzy reputation aggregation," *IEEE Internet Computing Magzine Special Issue on Security for P2P and AdHoc Networks*, vol. 9, no. 6, pp. 24-34, 2005. Article (CrossRef Link).

[16] Tang Wen, Hu Jianbin, and Chen Zhong, "Research on a fuzzy logical-based subjective trust management model," *Journal of Computer Research and Development*, vol. 42, no. 10, pp. 1654-1659, 2005.

[17] S. D. Ramchurn, C. Sierra, L. Godo, N. R. Jennings, "Devising a trust model for multi-agent interactions using confidence and reputation," *International Journal of Applied Artificial Intelligence*, vol. 18, no. 10, pp. 833-852, 2003. Article (CrossRef Link).

[18] M. Supriya, L. J. Venkataramana, K. Sangeeta, G. K. Patra, "Estimating trust value for cloud service providers using fuzzy logic," *International Journal of Computer Application*, vol. 48, no. 19, pp. 28-34, 2012. Article (CrossRef Link).

[19] A. Selvaraj, S. Sundararajan, "Evidence-based trust evaluation system for cloud services using fuzzy logic," *International Journal of Fuzzy Systems*, pp. 1-9, 2016. Article (CrossRef Link).

[20] Changsong Li, Shilong Wang, Ling Kang, Liang Guo, Yang Cao, "Trust evaluation model of cloud manufacturing service platform," *International Journal of Advanced Manufacturing Technology*, vol. 75, no. 1, pp. 489-501, 2014. Article (CrossRef Link).

[21] M. Alhamad, T. Dillon, and E. Chang, "SLA-based trust model for cloud computing," in *Proc. of the IEEE* 13*th International Conference on Network-Based Information Systems*, Takayama, Japan, pp. 321-324, 2010. Article (CrossRef Link).

[22] S. Chakraborty and K. Roy, "An sla-based framework for estimating trustworthiness of a cloud," in *Proc. of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, Liverpool, UK, pp. 321-324. 2012. Article (CrossRef Link).

[23] S. M. Habib, S. Ries, and M. Muhlhauser, "Towards a trust management system for cloud computing," in *Proc. of the IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, Changsha, China, pp. 933-939, 2011. Article (CrossRef Link).

[24] T. H. Noor and Q. Z. Sheng, "Trust as a service: a framework for trust management in cloud environments," in *Proc. of the IEEE 12th International Conference on* Web Information System Engineering, Sydney, Australia, pp. 314-321, 2011. Article (CrossRef Link).

[25] T. H. Noor, Q. Z. Sheng, A. Ngu, J. Law, "CloudArmor: A platform for credibility-based trust management of cloud services," in *Proc. of the 22nd ACM Conference on Information and Knowledge Management*, San Francisco, USA, pp. 2509-2512, 2013. Article (CrossRef Link).

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

[27] Hiroyuki Sato, Atsushi Kanai, Shigeaki Tanimoto, "A cloud trust model in a security aware cloud," in *Proc. of the 10th Annual International Symposium on Applications and the Internet*, Seoul, Korea, pp. 121-124, 2010. Article (CrossRef Link).

[28] L. F. Wang, Z. P. Wu, "A novel trustworthiness measurement model for cloud service," in *Proc. of the IEEE/ACM 7th International Conference on Utility and Cloud Computing*, London, UK, pp. 928-933, 2014. Article (CrossRef Link).

[29] W. J. Fan, S. L. Yang, H. Perros, J. Pei, "A multi-dimensional trust-aware cloud service selection mechanism based on evidential reasoning approach," *International Journal of Automation and Computing*, vol. 12, no. 2, pp. 208-219, 2015. Article (CrossRef Link).

[30] M. Chiregi, N. J. Navimipour, "A new method for trust and reputation evaluation in the cloud environments using the recommendations of opinion leaders' entities and removing the effect of troll entities," *Computers in Human Behavior*, vol. 60, pp. 280-292, 2016. Article (CrossRef Link).

[31] M. D. Tang, X. L. Dai, J. X. Liu, J. J. Chen, "Towards a trust evaluation middleware for cloud service selection," *Future Generation Computer Systems*, 2016. Article (CrossRef Link).

[32] V. Viji Rajendran, S. Swamynathan, "Hybrid model for dynamic evaluation of trust in cloud services," *Wireless Networks*, vol. 22, pp. 1807-1818, 2016. Article (CrossRef Link).

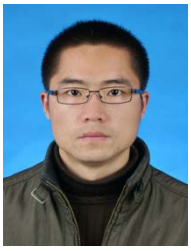
[33] C. Elizabeth, H. Farookh, D. Tharam, "Trust and reputation for service-oriented environments: technologies for building business intelligence and consumer confidence," New York: Wiley, 2006.

[34] H. Ma, Z. G. H, "User preferences-aware recommendation for trustworthy cloud services based on fuzzy clustering," *Journal of Central South University*, vol. 22, no. 9, pp. 3495-3505, 2015. Article (CrossRef Link).

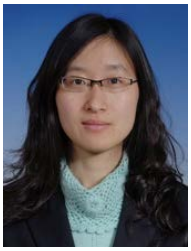
Liangmin Guo received her PhD degree from the School of Computer Science and Technology, University of Science and Technology of China in 2011. Since 2013, she has been an associate professor in School of Mathematics and Computer Science, Anhui Normal University. Currently she is the master student supervisor of Anhui Normal University. Her research interests include cloud computing, information security, and recommender system.

Yonglong Luo received his PhD degree from the School of Computer Science and Technology, University of Science and Technology of China in 2005. Since 2007, he has been a professor in School of Mathematics and Computer Science, Anhui Normal University. Currently, he is the PhD supervisor of Anhui Normal University. He is the Director of Engineering Technology Research Center of Network and Information Security. His research interests include information security and spatial data processing

Xiaokang He is currently working toward bachelor's degree in the Department of Software Engineering, Anhui Normal University, China.



Guiyin Hu received his M.S. degree from the School of Computer from Nanjing University of Posts and Telecommunications, China, in 2010. Currently, he is a lecturer in the Department of Software Engineering of Anhui Normal University. His research interests include information security and virtual tour.



Yan Dong received her M.S. degree in Economics from University of International Business and Economics, Beijing, China, in 2006. Currently, she is a Research Associate in the Experiment Center of School of Mathematics and Computer Science, Anhui Normal University. Her research interests are E-commerce and data mining.