A QoS&SLA-Driven Multifaceted Trust Model for Cloud Computing

Runlian Zhang[1,4(✉)], Qingzhi Wang[2], Jinhua Cui[3], and Xiaonian Wu[1]

[1] Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin 541004, China
zhangrl@guet.edu.cn
[2] Qingdao Technological University, Qindao College, Qindao 266106, China
[3] College of Computer, National University of Defense Technology, Changsha 410073, China
[4] Guangxi Colleges and Universities Key Laboratory of Cloud Computing and Complex Systems, Guilin 541004, China

Abstract. Quality of Service (QoS) plays a vital role in cloud computing while Service Level Agreements (SLA) to a service contract is indispensable as well. Selecting a trusted cloud service based on service performance, thus, is raising fundamental concern. This work presents a QoS&SLA-driven multifaceted trust model for efficiently evaluating the trustworthiness of a cloud service in the light of its multiple differential service attributes. Owing to the uncertainty of QoS, the interval number theory is naturally introduced into our trust model. In the trust evaluation, moreover, an adaptive weight adjustment method that depends on connection number is exploited to dynamically accommodate their respective factors. The proposed trust model is the composition of two types of trust metrics, which are QoS trust and user satisfaction trust. QoS trust, specifically, that indicates the level of actual performance of the cloud service. User satisfaction trust virtually reflects to what extent actual service performance is in accord with SLA. Finally, we assess the proposed trust model based on real datasets derived from CloudHarmony, which makes the approach more objective and effective for cloud computing.

Keywords: Trust model · Quality of Service · Service Level Agreements · Interval number theory

1 Introduction

The cloud paradigm gains increasing acceptance because of its cost-efficient computing manner. Cloud services have been enclosed into standard computer programs in the form of services for cloud users. Still, there exist several challenges such as the related issues of security, privacy and trust [1]. One major difficulty is to determine which cloud service provider is trustworthy and reliable as per the requirement and application for cloud users. Meanwhile, cloud service providers should monitor the status of cloud services whenever and wherever possible so as to provide the better cloud services and resist various attacks.

W. Han et al. (Eds.): CTCIS 2019, CCIS 1149, pp. 281–295, 2020.
https://doi.org/10.1007/978-981-15-3418-8_18

Trust is an integral component in the cloud paradigm as a result of the indispensable interactions between the cloud user and the service provider. Bridging the trust among them, however, is a sophisticated procedure. Nowadays, many researchers have developed several trust frameworks from different perspectives to achieve it. Policy-based trust model [2–4] can establish and authenticate trust relationship through the certificate policies which mainly realize the privilege management to protect sensitive resources and services. Behavior-based trust framework [5–8] intends to make trust decision with the assistance of past experiences wherein the positive experience generally increases the estimate of the trustworthiness while the negative reduces it. Reputation-based trust framework [9–11] can aggregate a large number of user's ratings. Consequently, it covers more situations and has a broader view on the service provider than a single user does.

However, most existing trust models utilize subjective assessment of the cloud users, which enables them depend heavily on recommendation mechanisms to quantify trustworthiness of cloud services. Trustworthiness evaluation is a complex process closely related to many factors which usually are determined via the subjective weight assignment model. With the complicated and various service attributes, prior works basically lack adaptability when assigning weights to trust attributes. To address the above problem, this paper proposed a Multifaceted Trust Framework based on Quality of Services (QoS) and Service Level Agreements (SLA) for cloud computing environments. The main contributions of this work are illustrated as follows:

- We propose an objective QoS-based scheme instead of involving user's subjective ratings. In virtue of advantages of the interval number theory, trust evaluation with considerations of multi-dimensional trust factors is implemented. This can exhibit a better view of objectivity and uncertainty of trust evidence unlike that in the traditional trust model.
- We present how to regulate the trust factor weights adaptively according to changes of trust factors. Exploiting multivariate connection number theory, we eliminate limitations of traditional weighting methods for multiple trust factors, in which the weights are assigned subjectively.
- We resolve the issue of user satisfaction on the basis of the nearness degree of trust factors between monitored values and that in SLA. That genuinely indicates the objective achievement scale on SLA index system.
- We conduct comprehensive experiments to compare the effectiveness of the proposed model and existing trust models. The results show the proposed is more objective and effective.

The remainder of the paper is organized as follows. Some existing works are first reviewed in Sect. 2. In Sect. 3, we then describe our proposed trust model followed by presenting our simulation results in Sect. 4. Finally, we conclude our work in Sect. 5.

2 Related Works

Trust in our daily life often serves as a foundation for making decisions in various complex situations [12]. Naturally, the cloud paradigm involves in it as well, in which trust is as a subjective mutual measurable relationship between the service and the user in certain specific context. Especially, It not only has the guarantee of service quality on the cloud computing, but also help users select the most trustworthy cloud services [13]. For instance, QoS-based and SLA-based trust mechanisms are an effective measurement solution to the trustworthiness of cloud services.

Manuel [14] introduced a trust model based on previous credentials and present capabilities of a cloud resource provider wherein trust was measured in terms of four attributes such as availability, reliability, turnaround efficiency and data integrity. In addition, it presented how a service level agreement is prepared while combining users' QoS requirements and capabilities of cloud resource provider.

Li et al. [15] proposed an adaptive and attribute-based trust model in which rough set theory is employed to trust analysis with considerations of multi-dimensional trust attributes, and utilizing the IOWA operator aggregates the global trust degree according to time series.

Fan et al. [16] developed a trust management framework for the calculation of both the objective and the subjective trust of a CSP. This framework with two-layer trust evaluation model depends on a set of TSPs distributed over the clouds.

Tan et al. [17] proposed a SLA trust model based on behavior evaluation. Time and successful transaction are integrated to calculate the trust value, especially in an iterative way. Providers are chosen according to the fulfillment of SLA parameters monitored in the serving process and the users' demands.

Chakraborty et al. [18] identified and formalized several parameters that can be extracted from SLA or retrieved during the sessions. It designed a trust evaluation engine to estimate trustworthiness of a CSP. The framework can cater to different requirements of different consumers as it calculates trust based on individual consumer's policies.

Ding et al. [19] designed a CSTrust framework for conducting cloud service trust worthiness evaluation by combining QoS prediction and customer satisfaction estimation. It defined the usage structure factor to reduce the influence of negative neighbors in similarity computation. Moreover, it presented the similarity parameter to determine how many neighbors' records have been adopted to predict missing QoS value.

Sidhu and Singh [20] presented the design of a trust evaluation framework that uses the compliance monitoring mechanism to determine the trustworthiness of service providers. The framework generates trust on CSPs by evaluating the compliance of QoS parameters and then by utilizing the improved TOPSIS method.

Alhanahnah et al. [21] proposed a context-aware multifaceted trust framework (CAMFT) to help evaluate trust in cloud service providers. It considers two kinds of trust factors: SLA trust factors and non-SLA trust factors, both of which are measured in virtue of AHP method and fuzzy simple additive weighting, respectively.

Tang et al. [22] proposed a trustworthy selection framework for cloud service, named TRUSS. The integrated trust evaluation method is comprised of both objective and subjective trust assessment. The objective one is based on QoS monitoring while the subjective is with the dependence of user feedback ratings.

3 QoS&SLA-Driven Trust Model

This section first discusses the trust preliminaries to the model. In the following, we present the architecture of QoS&SLA-driven multifaceted trust model in the cloud computing environment.

3.1 Trust Preliminaries

Trustor. A trustor is an agent that trusts another entity. In our model, the trustor is the cloud user (CU). Let CU be a collection of the cloud user, $CU = \{cu_1, cu_2, \cdots\cdots, cu_n\}$.

Trustee. A trustee is an entity that the trustor trusts. In our model, the trustee is the cloud service (CS). Let CS be a collection of the cloud service, $CS = \{cs_1, cs_2, \cdots\cdots, cs_m\}$.

Trust. Trust is a trait having congruence between the desired and perceived participation and it is characterized by hope, faith, confidence, assurance and initiative [12]. Here, trust is defined as a belief level that a cloud user puts on a cloud service for a specific action according to previous observation of QoS performance and user satisfaction. In this paper, the trustworthiness of the cloud service ranges from 0 to 1. A value of 1 means completely trustworthy and 0 means the opposite.

QoS Trust. QoS parameters represent the first hand information or evidence after the CU interacts with the CS. QoS trust is a kind of trust calculated by QoS parameters, which reflects how much extent the cloud user trusts the cloud provider from the point of view of QoS.

User Satisfaction Trust. SLA is an important document that gives a clear definition of the formal agreements about service terms like performance, availability and billing. User satisfaction trust is a kind of trust calculated by user satisfaction degree, which reflects how much extent the cloud service can actualize the SLA.

Global Trust. Global trust, which reflects the trust degree of the cloud service from the cloud user's point of view, is an integration of QoS trust and user satisfaction trust.

Reputation. Reputation is the sum of impressions held by all cloud users. Here the cloud service's reputation is assumed as the aggregate generated through the global trust from different cloud users.

3.2 Trust Model

Figure 1 shows the system architecture of our proposed trust model, which is mainly composed of five components: cloud service provider, cloud user, performance monitor, SLA agent and trust management module. A cloud service provider deploys its services and provides services to cloud users. A cloud user is the consumer of cloud services. The performance monitor is used to monitor the actual service performance at runtime. The SLA agent is responsible for the negotiation between the cloud service provider and the cloud user about the SLA details, which will finally publish a SLA document to the cloud service provider and the cloud user. With the SLAs, a cloud user can identify whether a service satisfies his/her service requirements. The trust management module is charge of evaluating the trustworthiness of cloud services through the monitored evidence.

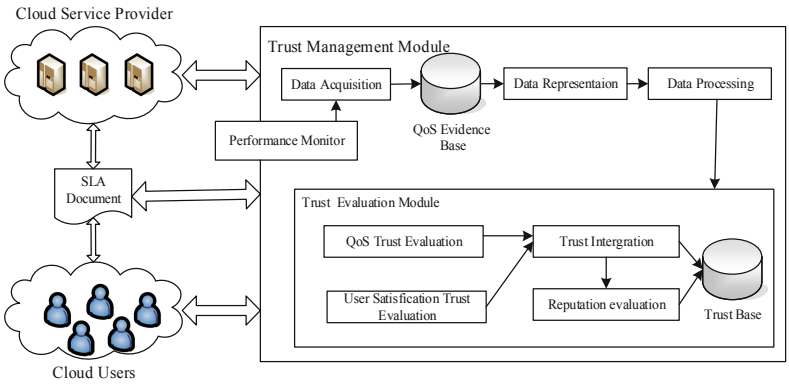

Fig. 1. QoS&SLA-driven trust model

4 Trusts and Reputation Evaluation for the Cloud Services

In this section, we describe trusts and reputation evaluation for the cloud services. First of all, we discuss QoS trust evaluation and the calculation of trust factor weights. The second part presents user satisfaction trust evaluation. The next part discusses how to integrate QoS trust and user satisfaction trust, which is followed by discussion of reputation evaluation.

4.1 QoS Trust

QoS is a measure of service quality that the service provider offers to the service user. In cloud paradigm, QoS data involves many parameters such as up-time, down-time, delay, bandwidth etc. Performance monitor component is responsible for obtaining QoS data continuously. Suppose we can obtain QoS parameters of the interaction between the CS and the CU by the performance monitor component, these parameters are denoted as follows.

$$QoS_{s,j} = \{Q_{s,j,1}, Q_{s,j,2}, \cdots\cdots, Q_{s,j,k}\} \qquad (1 \le s \le m, 1 \le j \le n) \tag{1}$$

$Q_{s,j,u}$ represents u-kind QoS parameter value of the interaction between CSs and CUj. $QoS_{s,j}$ represents QoS parameter set of the interaction which indicates abilities of the CS to provide appropriate service according to the requirements of the CU. We hence evaluate the trustworthiness of the CS based on QoS parameters which refers to QoS trust.

The QoS data is dynamically obtained several times during a pre-defined time, and randomly varies with the time of transmission. Such an operation will form a sequence of QoS data. Comparing to the fixed value, the uncertain one is more appropriate for the QoS data representation while the interval number is indeterminate. So the QoS data is expressed in the interval number, denoted by $QoS^t_{s,j}$. Based on the sliding window, we pull the QoS data between CSs and CUj at $[t', t]$. It is denoted as follows.

$$QoS^t_{s,j} = \{\tilde{q}_{s,j,1}, \tilde{q}_{s,j,2}, \cdots\cdots, \tilde{q}_{s,j,k}\} \qquad (1 \le s \le m, 1 \le j \le n) \tag{2}$$

$\tilde{q}_{s,j,u} = [q^-_{s,j,u}, q^+_{s,j,u}]$ represents the interval number of the u-kind QoS parameter. $q^-_{s,j,u}, q^+_{s,j,u}$ are the lower and the upper bound of the interval number, respectively, which indicates the variation range of QoS parameter values in $[t', t]$.

Accordingly, the below is the QoS parameter matrix between CU_j and CS, denoted by $Q_j(t)$.

$$Q_j(t) = \begin{bmatrix} \tilde{q}_{1,j,1} & \tilde{q}_{1,j,2} & \cdots\cdots & \tilde{q}_{1,j,k} \\ \tilde{q}_{2,j,1} & \tilde{q}_{2,j,2} & \cdots\cdots & \tilde{q}_{2,j,k} \\ \vdots & \vdots & \vdots & \vdots \\ \tilde{q}_{m,j,1} & \tilde{q}_{m,j,2} & \cdots\cdots & \tilde{q}_{m,j,k} \end{bmatrix} \qquad (1 \le j \le n) \tag{3}$$

Each QoS parameter has different ranges, and the according values are significant distinct. Furthermore, some are beneficial parameters and others are cost parameters. For the beneficial parameter, the bigger value is the better. For the cost parameter, the smaller value is the better. Accordingly, we normalize these values to the no-dimensional form. So, each QoS parameter is transformed into the beneficial parameter within the range of [0, 1]. The concrete computational methods are as follow.

For the beneficial parameter:

$$[r^-_{s,j,u}, r^+_{s,j,u}] = \left[\frac{q^-_{s,j,u}}{\max\limits_{1 \le s \le m} q^-_{s,j,u}}, \frac{q^+_{s,j,u}}{\max\limits_{1 \le s \le m} q^+_{s,j,u}} \right] \qquad (s = 1, 2, \cdots\cdots, m) \tag{4}$$

For the cost parameter:

$$[r^-_{s,j,u}, r^+_{s,j,u}] = \left[\frac{\min\limits_{1 \le s \le m} q^-_{s,j,u}}{q^-_{s,j,u}}, \frac{\min\limits_{1 \le s \le m} q^+_{s,j,u}}{q^+_{s,j,u}} \right] \qquad (s = 1, 2, \cdots\cdots, m) \tag{5}$$

So the normalization value of each QoS parameter is written $\tilde{r}_{s,j,u}$, $\tilde{r}_{s,j,u} = [r^{-}_{s,j,u}, r^{+}_{s,j,u}]$. The standardized matrix of values of the QoS parameter is shown below.

$$RQ_j(t) = \begin{bmatrix} \tilde{r}_{1,j,1} & \tilde{r}_{1,j,2} & \cdots\cdots & \tilde{r}_{1,j,k} \\ \tilde{r}_{2,j,1} & \tilde{r}_{2,j,2} & \cdots\cdots & \tilde{r}_{2,j,k} \\ \vdots & \vdots & \vdots & \vdots \\ \tilde{r}_{m,j,1} & \tilde{r}_{m,j,2} & \cdots\cdots & \tilde{r}_{m,j,k} \end{bmatrix} \qquad (1 \le j \le n) \tag{6}$$

Connection number is a structural function used to describe the certainty and uncertainty of objects and the relationships among them. To better express the certainty and uncertainty of QoS parameters, these values are denoted with "mean value + max deviation" binary connection number (a kind of connection number) instead of the interval number. Let $r_{s,j,u}$ be the binary connection number of $\tilde{r}_{s,j,u}$.

$$\begin{cases} r_{s,j,u} = A_{sju} + B_{sju} i \\ A_{sju} = \dfrac{r^{+}_{s,j,u} + r^{-}_{s,j,u}}{2} \\ B_{sju} = \dfrac{r^{+}_{s,j,u} - r^{-}_{s,j,u}}{2} \end{cases} \qquad (1 \le s \le m, 1 \le j \le n, 1 \le u \le k, -1 \le i \le 1) \tag{7}$$

Then $q_{s,j,u}$ is transformed into trigonometric function as follows.

$$\begin{cases} q_{s,j,u} = r_{sju}(\cos\theta_{sju} + i\ \sin\theta_{sju}) \\ r_{sju} = \sqrt{A^2 + B^2} \\ \theta_{sju} = \arctan\frac{A}{B} \end{cases} \qquad (-1 \le i \le 1, A \ne 0) \tag{8}$$

Each QoS parameter affects the trust evaluation to varying degrees. Note that we cannot determine the parameter weights in advance. At most time, while the CSP can maintain stable QoS performance, the trust degree of the CSP will change with fluctuations in QoS parameter values. In current settings, we don't take the CU's preferences into account, and instead suppose each QoS parameter has the same importance in interactions. The CSPs always provide the stable and reliable services at most cases, so there exists the basic principle that the smaller the fluctuation of certain QoS attribute is, the less the effect of this QoS parameter on trust evaluation is, conversely, and that the bigger fluctuation will incur the severely effect. Therefore, the bigger the QoS parameter value fluctuates, the greater the weight should be given. Let w_u be the weight of the u-kind QoS attribute.

$$\begin{cases} w_u = \dfrac{D_u}{\sum D_u} \\ D_u = \dfrac{\sum (r_{sju} - \bar{r}_{sju})^2}{m-1} \end{cases} \qquad (1 \le u \le k) \tag{9}$$

Here, $\bar{r}_{sju}$ is the average value of the norm of each QoS attribute. The QoS trust degree of the service provider is computed by principle model, denoted by $QT^t_{s,j}$.

$$QT^t_{s,j} = \sum r_{sju} w_u \qquad (1 \le s \le m, 1 \le u \le k) \tag{10}$$

4.2 User Satisfaction Trust

A service level agreement is legal contract between a cloud user and a cloud service provider, which is usually promised by the service provider to the user. That contains many QoS parameters like main memory, response time, bandwidth, and so on. However, actual monitored QoS parameter is normally different from the one promised by the service provider in the SLA. As a general rule, if monitored QoS parameter value is greatly close to it in the SLA, the user satisfactory is much higher accordingly. We hence compute user satisfactory trust by using interval number nearness degree.

Suppose the QoS parameter value in SLA is denoted as $SQoS_{s,j}$.

$$SQoS_{s,j} = \{\tilde{a}_{s,j,1}, \tilde{a}_{s,j,2}, \cdots\cdots, \tilde{a}_{s,j,k}\} \qquad (1 \le s \le m, 1 \le j \le n) \tag{11}$$

Here $\tilde{a}_{s,j,u} = [a^-_{s,j,u}, a^+_{s,j,u}]$ is the interval number representation of the u-th$(1 \le u \le k)$ QoS parameter value. The deviation degree $L(\tilde{a}_{s,j,u}, \tilde{q}_{s,j,u})$ between the u-th QoS parameter value $SQoS_{s,j}$ and $QoS^t_{s,j}$ is as follows.

$$L(\tilde{a}_{s,j,u}, \tilde{q}_{s,j,u}) = \frac{\left|a^+_{s,j,u} - q^+_{s,j,u}\right| + \left|a^-_{s,j,u} - q^-_{s,j,u}\right|}{a^+_{s,j,u} - a^-_{s,j,u} + q^+_{s,j,u} - q^-_{s,j,u}} \tag{12}$$

The nearness degree $T(\tilde{a}_{s,j,u}, \tilde{q}_{s,j,u})$ between the u-th QoS parameter value $SQoS_{s,j}$ and $QoS^t_{s,j}$ is described below.

$$T(\tilde{a}_{s,j,u}, \tilde{b}_{s,j,u}) = \begin{cases} \frac{1-L(\tilde{a}_{s,j,u}, \tilde{b}_{s,j,u})}{1+L(\tilde{a}_{s,j,u}, \tilde{b}_{s,j,u})} & 0 \le L(\tilde{a}_{s,j,u}, \tilde{b}_{s,j,u}) < 1 \\ 0, & L(\tilde{a}_{s,j,u}, \tilde{b}_{s,j,u}) \ge 1 \end{cases} \tag{13}$$

So the user satisfactory trust $ST^t_{s,j}$ is shown as the following. The lower the deviation degree is, the higher the nearness degree is. Consequently, the user satisfactory trust gets higher.

$$ST^t_{s,j} = \frac{1}{k} \sum_{u=1}^{k} T(\tilde{a}_{s,j,u}, \tilde{b}_{s,j,u}) \tag{14}$$

4.3 Trust Integration

To obtain the global trust, we enable the integration of the QoS trust and the user satisfaction trust. Importantly, we think the historical trust value is one of influence factors, so the global trust degree of the service provider is computed by principle model, denoted by $GT^t_{s,j}$.

$$GT^t_{s,j} = \alpha GT^{t-1}_{s,j} + \beta QT^t_{s,j} + \gamma ST^t_{s,j} \qquad (\alpha + \beta + \gamma = 1) \tag{15}$$

Here, α, β, and γ are positive weights of the trust parameters.

4.4 Reputation

Trust and reputation are related, but different. Basically, trust is between two entities, but the reputation of an entity is the aggregated opinions of a community towards that entity. Usually, an entity that has high reputation is trusted by many other entities in that community. In this model, the global trust is the trustworthiness of a cloud service from the perspective of a cloud user. Reputation is the trustworthiness of a cloud service from the perspective of all cloud users. We collect the global trust of the cloud service provider from different cloud users to generate their reputation. Let RT^t_s be the reputation of the cloud service provider s.

$$RT^t_s = \frac{1}{n}\sum_{j=1}^{n} GT^t_{s,j} \tag{16}$$

5 Evaluation

In this section, we mainly conducts trusts evaluation on sample dataset extracted from Cloud Harmony Project in the fashion of emulation on Matlab [23]. The values for security parameters are α, β, and γ, which are empirical values obtained from multiple experiments. As the weight factors in Eq. (15), which is used to determine how much the final integrated global trustworthiness is affected by the last global, QoS's and user satisfaction's trustworthiness, respectively. Weights of QoS parameters are evaluated by Eq. (9).

Cloud service models covered in our experiments include IaaS, SaaS and PaaS. The sample dataset consists of 3 kinds of cloud service instances as shown in Table 1. The sample dataset involves 6 QoS parameters, specifically, which are Network Latency, downlink data speed (256 KB–10 MB/2 threads), downlink data speed (1–128 KB/4 threads), uplink data speed (256 KB–10 MB/2 threads), uplink data speed (1–128 KB/4 threads) and service success rate. These QoS values were fetched from Cloud Harmony website.

Table 1. Cloud service instance specifications

Cloud service model	Cloud service type	Cloud service
IaaS (I)	Compute	Google Compute Engine-europe-west4 (I1)
		Microsoft Azure Virtual Machines - australia-east (I2)
		Alibaba Elastic Compute Service - ap-southeast-1 (I3)
		Amazon EC2-ap-southeast-2 (I4)
PaaS (P)	Storage	IBM Bluemix-us-south (P1)
		Alibaba Cloud Object Storage-cn-shenzhen (P2)
		Google Cloud Storage-asia (P3)
		Microsoft Azure Cloud Storage-us-west (P4)
SaaS (S)	CDN	Azure CDN from Verizon (S1)
		Tata Communications CDN (S2)
		MaxCDN (S3)
		Rackspace Cloud CDN (S4)

5.1 Trusts Evaluation of Cloud Services

In virtue of Cloud Harmony, QoS data of 12 cloud services is first collected. QoS parameters involved are Network Latency (ms), downlink data speed (256 KB–10 MB/2 threads) (Mb/s), downlink data speed (1–128 KB/4 threads) (Mb/s), uplink data speed (256 KB–10 MB/2 threads) (Mb/s), uplink data speed (1–128 KB/4 threads) (Mb/s), service success rate. This is 12×6 matrix representing 12 cloud services and 6 attributes. The initial trust degree is set to 0.5. Positive weights of the trust parameters are $\alpha = 0.2$, $\beta = 0.4$, and $\gamma = 0.4$.

Figure 2 illustrates the trustworthiness of cloud services. It is clear that the trustworthiness changes with interactions. There are three kinds of trustworthiness that focus on different aspects. One is QoS, another is user satisfaction. Particularly, we put the two together into the global trust assessment. The values are different but the trend of the change is similar intuitively, which shows the relationship that QoS trustworthiness goes higher as user satisfaction gets higher. Thus, it is conformed to the general regularity, and indicates that our framework is more quantitative and objective.

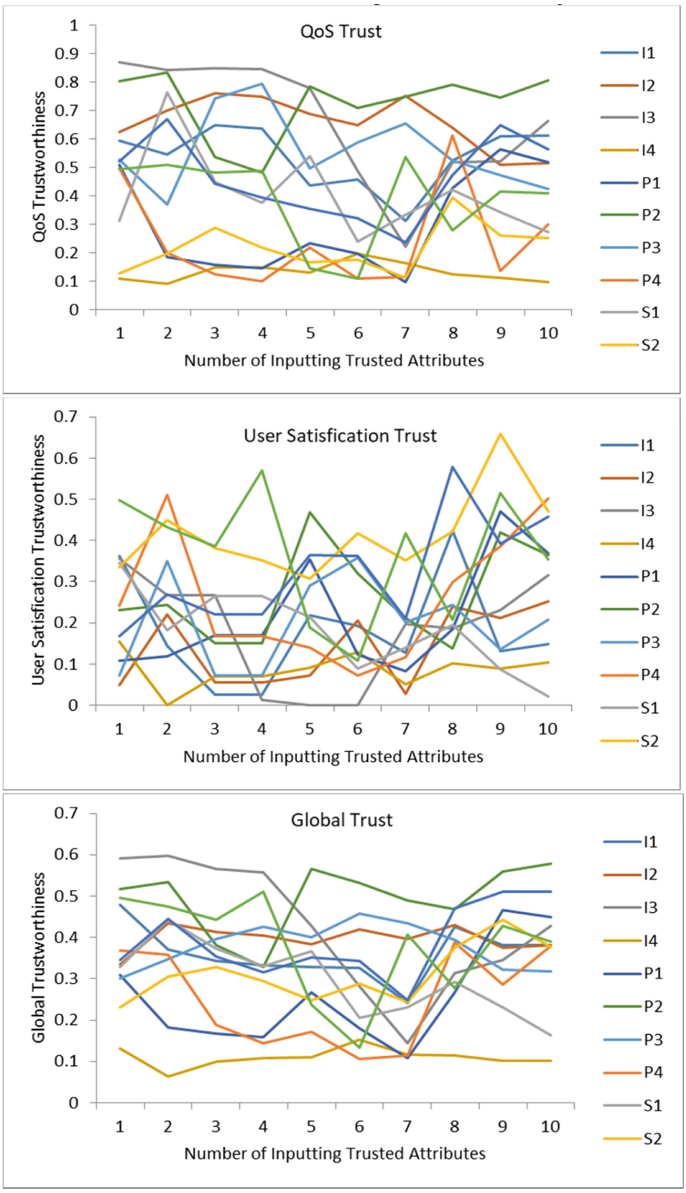

Fig. 2. Trustworthiness of cloud service

5.2 Reputation Evaluation of Cloud Services

We acquire QoS values of 12 cloud services from 10 cloud users. The reputations of 12 cloud services are evaluated based on the methods above. The results are shown in Table 2.

Table 2. Reputation of cloud Service

Cloud service	I1	I2	I3	I4
Reputation	0.3608	0.3975	0.4255	0.1099
Cloud service	P1	P2	P3	P4
Reputation	0.2558	0.4958	0.3796	0.2509
Cloud service	S1	S2	S3	S4
Reputation	0.2965	0.3134	0.389	0.3799

As shown in Table 2, in IaaS, I3 is with the highest reputation. In contrast, I4 is with the lowest reputation. In PaaS, P2 is a storage service with highest reputation while P4 is with the lowest reputation. In SaaS, S3 has highest reputation among CDN services while S1 is the lowest. The trust and reputation evaluation provides the cloud user with a reliable support that can be used in the process of service selection.

5.3 Adaptive Weight Adjustment of QoS Parameters

The changes of weights of QoS parameters are shown in Fig. 3. Service success rate is always equal to 1 in our collected data, which turns out to be lost any effect on trust evaluation. As a result, the weight of service success rate is set to 0. As we can see from the results, the weight of each QoS parameter fluctuates over time. Our algorithm can automatically detect the performance changes of the CSP and adjust the weight of each QoS parameter without any manual work. It is definite that the greater the QoS parameter fluctuates, the greater the weight of the QoS parameter changes. That can incur much more impact on trustworthiness. Therefore, it is an intelligent choice to self-adjust the weight of QoS parameters without user interaction.

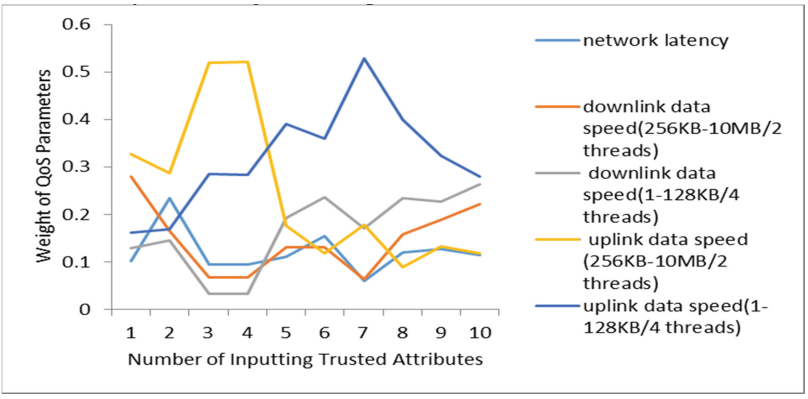

Fig. 3. The change of weight of QoS parameters

5.4 Comparisons with Other Methods

Figure 4 shows the comparing result of our model with TOPSIS, AHP and Liner Weighted methods. Due to limited space, we only give the comparing result of 3 cloud services.

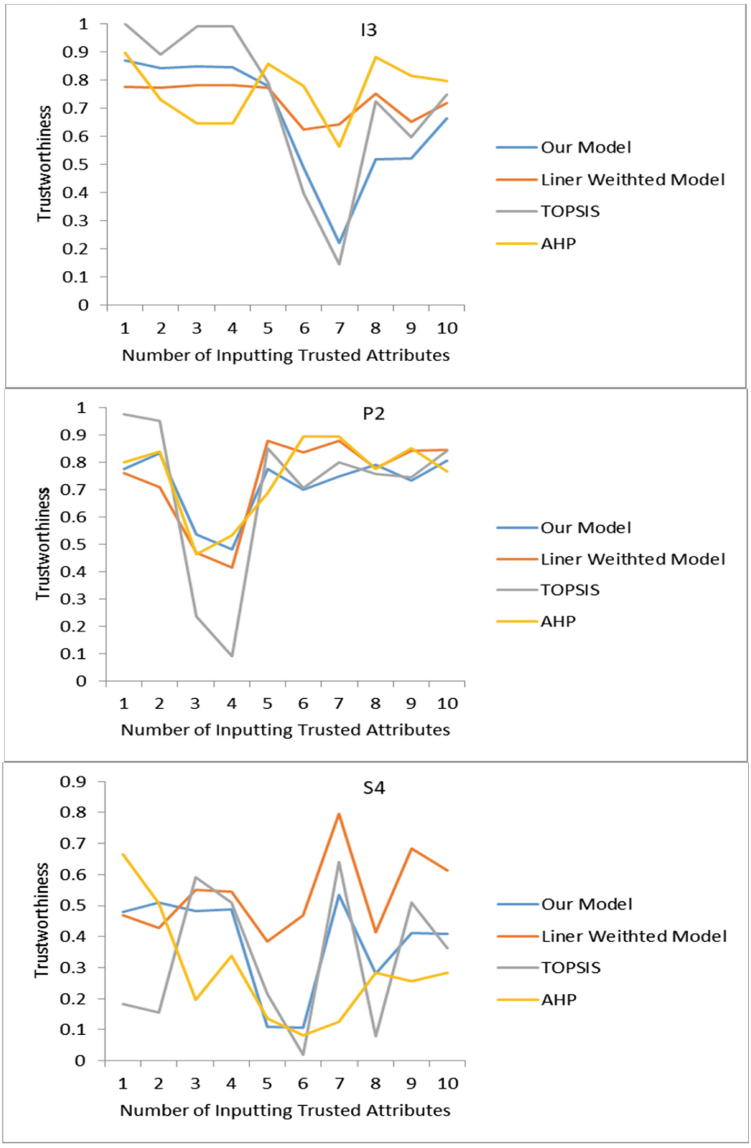

Fig. 4. Trustworthiness of cloud service in different models

It is evident that all the trust models are effective in evaluating the trustworthiness of the CS. Under the different trust model, the trend of the change of the trustworthiness is also similar. Our model has shown advantage over other models in the sense that it is objective. QoS data in interval number representation can better indicate the uncertainty of QoS data. Adaptive weight adjustment of QoS parameters can avoid the impact of subjective factor on the trust evaluation. Our model can reflect the contribution of every QoS parameter into the trustworthiness of the cloud service more objectively and dynamically.

6 Conclusion

In this paper, we proposed QoS&SLA-driven trust model for the cloud computing, which is used to evaluate the trustworthiness of the cloud services through the history service QoS information. With the assistance of interval number theory, our trust model can better represent the uncertainty of cloud service performance. Adaptive weight adjustment makes trust evaluation more objective, which can help cloud users to select a more trustworthy cloud service. Experiments have been conducted exploiting real cloud data derived from Cloud Harmony Website. The results demonstrate that our trust model is effective and objective. As part of our future work, we plan to explore the solution of trust timeliness, trust prediction and trust evaluation with user preferences.

Acknowledgement. This article is supported in part by Guangxi Natural Science Foundation (No. 2018GXNSFAA294036, 2018GXNSFAA138116), Guangxi Key Laboratory of Cryptography and Information Security of China (No. GCIS201705), Guangxi Colleges and Universities Key Laboratory of cloud computing and complex systems of China (No. YF16205), and Innovation Project of Guangxi Graduate Education (No. YCSW2018138).

References

1. Alhanahnah, M., Bertok, P., Tari, Z.: Trusting cloud service providers: trust phases and a taxonomy of trust factors. IEEE Cloud Comput. **4**(1), 44–54 (2017)
2. Blaze, M., Feigenbaum, J., Lacey, J.: Decentralized trust management system. In: Proceedings of the IEEE Symposium on Security and Privacy, vol. 30, no. 1, pp.164–173 (1996)
3. Chu, Y.-H., et al.: REFEREE: trust management for Web applications. Comput. Netw. ISDN Syst. **29**(8), 953–964 (1997)
4. Li, N., Mitchell, J.C., Winsborough, W.H.: Design of a Role-based trust-management framework. In: IEEE Symposium on Security and Privacy. IEEE Computer Society (2002)
5. Beth, T., Borcherding, M., Klein, B.: Valuation of trust in open networks. In: Gollmann, D. (ed.) ESORICS 1994. LNCS, vol. 875, pp. 1–18. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-58618-0_53
6. Liqin, T., Chuang, L., Yang, N.: Behavior value analysis and application in evaluating network entity behavior trust. In: International Conference on Computer Engineering and Technology. IEEE Computer Society (2010)
7. Pandey, S., Daniel, A.K.: Fuzzy logic based cloud service trustworthiness model. In: IEEE International Conference on Engineering and Technology (2016)

8. Yang, Z., Luo, J.: A behavior trust model based on fuzzy logic in cloud environment. Int. J. Perform. Eng. **14**, 665–672 (2018)
9. Comi, A., et al.: A reputation-based approach to improve QoS in cloud service composition. In: 24th IEEE International Conference on Enabling Technologies: Infrastructures for Collaborative Enterprises. Institute of Electrical and Electronics Engineers Inc., Larnaca (2015)
10. Singh, A., Chatterjee, K.: A multi-dimensional trust and reputation calculation model for cloud computing environments. In: 2017 ISEA Asia Security and Privacy Conference. Institute of Electrical and Electronics Engineers Inc., Surat (2017)
11. Bilecki, L.F., Fiorese, A.: A trust reputation architecture for cloud computing environment. In: IEEE/ACS International Conference on Computer Systems and Applications (2017)
12. Rathore, H., Badarla, V., George, K.J.: Sociopsychological trust model for wireless sensor networks. J. Netw. Comput. Appl. **62**, 75–87 (2016)
13. Chiregi, M., Navimipour, N.J.: A comprehensive study of the trust evaluation mechanisms in the cloud computing. J. Serv. Sci. Res. **9**(1), 1–30 (2017)
14. Manuel, P.: A trust model of cloud computing based on quality of service. Ann. Oper. Res. **233**(1), 281–292 (2015)
15. Li, X., Du, J.: Adaptive and attribute-based trust model for service-level agreement guarantee in cloud computing. IET Inf. Secur. **7**(1), 39–50 (2013)
16. Fan, W., Perros, H.: A novel trust management framework for multi-cloud environments based on trust service providers. Knowl.-Based Syst. **70**, 392–406 (2014)
17. Tan, Z., et al.: A novel trust model based on SLA and behavior evaluation for clouds. In: 14th Annual Conference on Privacy, Security and Trust, pp. 581–587(2017)
18. Chakraborty, S., Roy, K.: An SLA-based framework for estimating trustworthiness of a cloud. In: IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 937–942 (2012)
19. Ding, S., et al.: Combining QoS prediction and customer satisfaction estimation to solve cloud service trustworthiness evaluation problems. Knowl.-Based Syst. **56**, 216–225 (2014)
20. Sidhu, J., Singh, S.: Improved TOPSIS method based trust evaluation framework for determining trustworthiness of cloud service providers. J. Grid Comput. **15**(1), 81–105 (2017)
21. Alhanahnah, M., et al.: Context-aware multifaceted trust framework for evaluating trustworthiness of cloud providers. Future Gener. Comput. Syst. **79**, 488–499 (2018)
22. Tang, M., et al.: Towards a trust evaluation middleware for cloud service selection. Future Gener. Comput. Syst. **74**, 302–312 (2017)
23. CloudHarmony Homepage. http://www.cloudharmony.com/