J Inf Process Syst, Vol.16, No.6, pp.1281~1292, December 2020
https://doi.org/10.3745/JIPS.03.0153

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Service Oriented Cloud Computing Trusted Evaluation Model

Hongqiang Jiao*, Xinxin Wang**, and Wanning Ding*

Abstract

More and more cloud computing services are being applied in various fields; however, it is difficult for users and cloud computing service platforms to establish trust among each other. The trust value cannot be measured accurately or effectively. To solve this problem, we design a service-oriented cloud trust assessment model using a cloud model. We also design a subjective preference weight allocation (SPWA) algorithm. A flexible weight model is advanced by combining SPWA with the entropy method. Aiming at the fuzziness and subjectivity of trust, the cloud model is used to measure the trust value of various cloud computing services. The SPWA algorithm is used to integrate each evaluation result to obtain the trust evaluation value of the entire cloud service provider.

Keywords

Cloud Computing, Subjective Weight, Trust Evaluation

1. Introduction

Cloud computing is a type of computing model for network users that comprises computing, data storage, software, and platform services; it packages a network of storage resources, software resources, computing resources, and so on into services, forming a large virtual shared "resource pool" [1]. This computing model embodies the idea "network is the computer" to provide users with a variety of services. In the cloud computing environment, users obtain the necessary services from the cloud computing center and pay the corresponding costs to cloud computing service providers. It does not need to purchase the appropriate infrastructure and computer hardware and software resources. Cloud computing can effectively reduce management and maintenance costs, which allows users to focus more on their core business development.

With the development of cloud computing in line with the current low-carbon and green computing trends, this technology is most likely to develop into applications in cyberspace and the nervous system with great market prospects [2]. Therefore, cloud computing has received wide attention from academia, industry, and government.

However, advances in this technology have also resulted in certain adverse consequences. With the development of cloud computing, a fraud-driven "black cloud" has developed rapidly. This led to the

Manuscript received July 26, 2019; first revision May 21, 2020; accepted May 29, 2020.
Corresponding Author: Hongqiang Jiao (94099428@qq.com)
* Information Engineering College, Handan College, Handan, China (94099428@qq.com, 360305531@qq.com)
** Art College, Hebei University of Science and Technology, Shijiazhuang, China (1097183635@qq.com)

emergence of a crisis of trust among cloud computing resource owners, service providers, and service requesters. This has become one of the main limitations in the development of cloud computing as a mainstream service platform [3].

In [4] and [5], the authors pointed out that in cloud computing, IaaS user VMs are continuously exposed to risk. In the relevant cloud computing literature, there are many problems pointed out by researchers. For example, if the provider itself experiences moral corruption, then malicious vendors can be defined.

As a result, trust management (TM) has emerged as an important and effective alternative to solve the security problem in new-generation networks. Research on trust theory and design of suitable management models for cloud computing trust has a great significance for the healthy development of cloud computing.

2. Related Work

In recent years, researchers have studied the entity trust relation, trust model, and trust management strategy in the domain of distributed network computation. They obtained many valuable research results.

With the widespread use of cloud computing services, tenants of cloud computing have put forward higher and higher requirements for security. The dynamics, randomness, complexity, and openness of the cloud computing environment make the original security program difficult to apply, which hinders the further development and application of cloud computing.

Lin et al. [6] analyzed the security challenges, mechanisms, and model evaluations of three aspects of research based on a cloud computing security architecture. In the cloud trust mechanism suggested by Huang and Nicol [7], the cloud service attribute is the user's trust judgment evidence. There were certain informal studies on the analysis of trust in cloud computing, but they did not establish a model to solve the problem of trust. Manuel [8] proposed a trust model based on the quality of service. First, the model checks whether the supplier has the ability to provide good service. Second, it examines the supplier's past credentials. The selection process for a vendor is divided into two factors: past credentials (a description of the reputation) and the service record of the cloud resource. Past credentials include availability, reliability, turnover rate, and data integrity. Cloud resource capabilities include environmental security levels, computing power, and network strength. Du et al. [9] chose a reliable and satisfactory service from a large number of services with the same or similar functions but different qualities of service. They proposed a cloud computing environment service selection model based on preferences and trust. The model included a service selection algorithm to determine the closest classification to the individual preferences of the service requester.

The trust evaluation mechanism was introduced to combine direct trust and domain recommendation trust. Thus, the requester can choose the service resource securely and reliably. This can satisfy the personality preference in the determined classification. Yang et al. [10] proposed a framework for a lightweight cloud computing trust service system including two trust modules: the trust module and trust-assisted evaluation module. Trust is calculated by introducing the D-S evidence theory and the Dirichlet distribution PDF. Li et al. [11] designed a quantitative and update algorithm using the discrete method of direct trust value. The recommended trust services evaluation algorithm was based on cloud theory. Kashif et al. [12] proposed a distributed trust protocol for cloud computing. However, the implementation of this protocol requires the use of the consumer's trusted platform module, which reduces the practicality of the protocol.

The trust degree evaluation defines the quantification method, operation, trust relationship transmission method, and calculation method of the trust relation. It uses a relative method of measuring and evaluating security information, and its immediate purpose is to provide support for trust decisions to establish trust relationships. Trust evaluation can be abstractly understood as a process of using one or a set of algorithms to deal with the evidence that affects the trust of the subject and obtains the degree of trust. In the comprehensive calculation of trust evaluation and the dynamic updating of trust, scholars have conducted a significant amount of research. Chiregi and Navimipour [13] provided an evaluation scheme for trust in the cloud using the opinion of the leader and by removing the influence of the entities. However, trust data is only used to select service providers. In other words, these reputation models work before the service is provided but not while the service is being provided. Chahal and Singh [14] proposed an expert system based on a fuzzy rule to evaluate the trust of the cloud service provider. Lynn et al. [15] suggested the expansion of a cloud credibility tag via a Delphi method. However, weight allocation is very important for scientific evaluation, and there are limitations in the Delphi method itself. Selvaraj and Sundararajan [16] provided an assessment method for cloud services according to a fuzzy system. Trust is a complex and ambiguous conception; a fuzzy system cannot express the degree of trust perfectly. Singh and Sidhu [17] proposed the design of a credibility assessment framework that uses a compliance detection mechanism to determine the credibility of cloud service providers. Tang et al. [18] suggested a chosen framework for cloud services based on credibility. Singh and Sidhu [19] provided an approach to solve the problem of determining the trust of cloud service providers in a cloud environment. Wang et al. [20] proposed a cloud service assessment scheme based on trust and privacy awareness. Somu et al. [21] provided a trust-centric method called HBFFOA to distinguish between suitable and trustworthy cloud service providers. Alhanahnah et al. [22] proposed the framework of a lightweight cloud computing trust service system that includes two trust modules: a trust module and trust-assisted evaluation module. Smithamol and Rajeswari [23] proposed trust management middleware (TMM), a framework for trust service identification in the cloud. However, these frameworks cannot be applied in practice at present. Li [24] proposed a cloud model for solving trust assessment.

3. Cloud Model

Cloud models can formally describe the inherent relation between randomness and fuzziness [25]. They provide a forward cloud generator and backward cloud generator algorithm for achieving qualitative and quantitative conversion.

Algorithm 1. Cloud generator algorithm

Input: The trust attribute assessment value x_i, where i=1,…,N.

Output: The trust attribute assessment cloud C_j

1. Compute the mean of the assessment values $\overline{X} = \frac{1}{N}\sum_{i=1}^{N} x_i$
2. Calculate $\frac{1}{N}\sum_{i=1}^{N} |x_i - \overline{X}|$
3. Calculate $S^2 = \frac{1}{N-1}\sum_{i=1}^{N} (x_i - \overline{X})^2$
4. Calculate $E_x = \overline{X}$ $E_n = \sqrt{\frac{\pi}{2}} \times \frac{1}{N}\sum_{i=1}^{N} |x_i - E_x|$, $H_e = \sqrt{S^2 - E_n^2}$

The cloud generator is shown in Algorithm 1. At present, a second-order normal cloud model with the three numerical characteristics *Ex* (expected value), *En* (entropy), and *He* (hyperentropy) has been widely studied and applied [26–28]. The digital features of the cloud are shown in Fig. 1 [29]. More details about the cloud model are presented in [24].

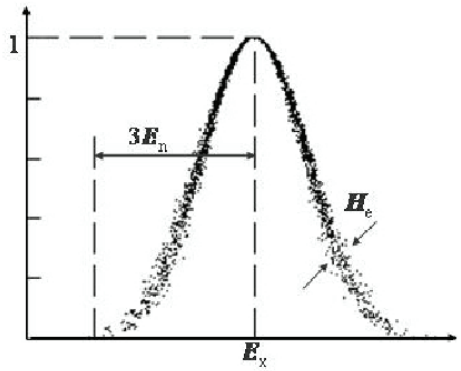


Fig. 1. Digital features of cloud. Adapted from Qiang and Bi [29].

4. Trust Evaluation Model

4.1 Trust-Evaluation-Scheme-Based Cloud Model

We define the linguistic terms for the trust evaluation as shown in Table 1. A cloud model is then used to express them (see Fig. 2).

Table 1. Assessment of qualitative attributes

Linguistic values	The cloud numbers
Very low (VL)	(0.1, 0.0394, 0.014)
Low (L)	(0.3, 0.0394, 0.014)
Medium (M)	(0.5, 0.0394, 0.014)
Relatively high (RH)	(0.7, 0.0394, 0.014)
Very high (VH)	(0.9, 0.0394, 0.014)

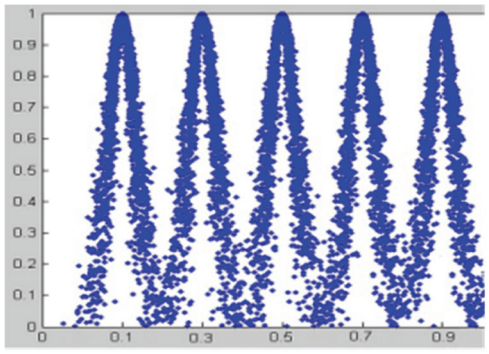


Fig. 2. Five levels of trust assessment cloud.

The trust assessment method by a cloud model is as follows:

Algorithm 2. Trust assessment method by cloud model

Input: Trust assessment cloud C_j and the attribute weight ω_j.
Output: Final trust assessment cloud C.
First, we compute service I_j's trust and calculate the assessment cloud C_j using Algorithm 1.
Second, we calculate the weight ω_j of the attributes by the method proposed in Sections 4.2 and 4.3.
Finally, we calculate the value of cloud trust C by formula $C = \sum_{j=1}^{n} \omega_j C_j$.

4.2 Subjective Preference Weight Set Method

Through a study of various objective weight allocation schemes, it was found that the evaluation results obtained by objective methods such as the entropy weight method are not ideal and cannot effectively reflect the subjective intentions of decision-makers. This paper designs a subjective weight allocation algorithm that can effectively distribute the weights of evaluation indicators according to the subjective intentions of decision-makers.

For the set of evaluation indicators $A = \{A_1, A_2, \cdots, A_M\}$, assuming that P decision-makers decide the weight of the indicator together, we use A_{ij} ($i \in [1, P], j \in [1, M]$) to denote the indicator set placed by the ith decision-maker at the jth position. The decision-makers can choose one location to place any number of indicators, and can place the already placed indicator repeatedly in other locations. Taking the weight of five indicators determined by two decision-makers as an example, the ranking of indicators is as follows:

$A_{11} = \{A_2\}, A_{12} = \{A_3\}, A_{13} = \{A_1\}, A_{14} = \{A_4\}$;

$A_{21} = \{A_2\}, A_{22} = \{A_2, A_3\}, A_{23} = \{A_1, A_3\}, A_{24} = \{A_1, A_3, A_4\}$.

If decision-maker Q_i places an indicator j at a certain location k, then we set the a_{kj} value to 1. Otherwise, we set it to 0. Then, according to the ranking of the two groups of aforementioned indicators, we obtain the quantitative decision matrix A_{kj}^i of each decision-maker.

An example is presented here. Two decision-makers' quantitative decision matrixes are as follows:

$$A_{kj}^1 = (a_{kj}^1)_{4\times4} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad A_{kj}^2 = (a_{kj}^2)_{4\times4} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

We assume that decision-makers have different decision-making powers and set the weights of P decision-makers as $P_W = (\omega_1, \omega_2, \ldots, \omega_P)$. A simple case is that they have the same decision-making power. We synthetically calculate the common decision-making matrix of P decision-makers by using each decision-maker's quantitative decision matrix.

$$T_{ki} = \sum_{i=1}^{P} A_{kj}^i \omega_i \tag{1}$$

Consider that the two decision-makers have the same decision-making powers. We obtain the common decision-making matrix as follows:

$$T_{kj} = (t_{kj})_{4\times4} = \begin{bmatrix} 0 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 2 & 0 & 1 & 0 \\ 1 & 0 & 1 & 2 \end{bmatrix}$$

To improve the computational efficiency, we design a linear descent method of position importance. This is not limited to the method we provide as long as the method satisfies the monotonic descent.

$$I_k = 1 - (k - 1)/M \tag{2}$$

I_k denotes the importance of the kth location. We obtain a vector Z by the product of the common decision-making matrix, and I_k: M denotes the number of evaluation indicators.

$$Z = [\,T_{kj}\,]^T * I_k \tag{3}$$

By (2), we obtain $I_1 = 1$, $I_2 = 0.75$, $I_3 = 0.5$, and $I_4 = 0.25$. These four numbers can express the importance of the four locations.

Using (3), we calculate the vector Z value: (1.25, 2.75, 2.25, 1).

By normalizing Z, we calculate the weight value of the index:

$$W_i = Z_i / \sum_{i=1}^{M} Z_i \tag{4}$$

According to (4), the weights of the four indexes are (0.172, 0.379, 0.311, and 0.138).

4.3 Advanced Flexible Weight Model Combining SPWA with Entropy Method

The SPWA is a type of subjective weight allocation algorithm. A combination of subjective and objective weighting methods can lead to a comprehensive evaluation. A flexible weight model is advanced by combining SPWA with the entropy method. The main idea of the entropy method is that the larger the entropy, the lower the weight. We can compute the entropy En easily using a cloud model.

The entropy values of n attributes are $E_{n1}, E_{n2}, \cdots, E_{nj}$ ($j = 1, 2, \cdots, n$). The objective weight is calculated using (5):

$$\omega^O = \frac{(1 - En_j)}{\sum_{j=1}^{n}(1 - En_j)} \tag{5}$$

$$\omega = \lambda\omega^S + (1 - \lambda)\omega^O, \lambda \in (0,1) \tag{6}$$

ω^s denotes the subjective weight calculated by the group preference weight allocation algorithm. ω^o denotes the objective weight calculated by (5). ω denotes the fusion weight calculated using (6). λ is the harmonic parameter, which is set to 0.5.

5. Simulation and Results Analysis

5.1 Data of Simulation Experiment

This experiment uses the dataset from [30] (Table 2).

Table 2. Index and assessment results

Item_id	The index corresponding to item	The trust indexes evaluation cloud
79	I_1 Database service	C_1 (0.808,0.1154,0.0386)
87	I_2 Mobile service	C_2 (0.8142,0.2658,0.1316)
104	I_3 Cloud communication	C_3 (0.7884,0.2176,0.09)
106	I_4 Elasticity calculation	C_4 (0.8926,0.1634,0.0842)
184	I_5 Video service	C_5 (0.7484,0.2372,0.1158)
188	I_6 Storage service	C_6 (0.662,0.277,0.1158)
223	I_7 Analysis service	C_7 (0.966,0.0724,0.0846)
224	I_8 Management and monitoring services	C_8 (0.8518,0.2336,0.1162)
225	I_9 Application service	C_9 (0.7036,0.3278,0.1758)

5.2 Experimental Result and Discussion

We consider nine kinds of cloud services provided by Ali cloud, all of which are associated with items in the rating data (see Fig. 3). Algorithm 1 in Section 3 is used to compute the trust assessment cloud for every service. Then, the final trust assessment cloud of the cloud service is computed by method 2. The final result of trust assessment cloud C = (0.8027, 0.202, 0.099), as shown in Fig. 4. The weight is calculated as follows:

$$\omega = \{\omega_1, \omega_2, ..., \omega_9\} = (0.127, 0.097, 0.083, 0.132, 0.095, 0.124, 0.092, 0.134, 0.116).$$

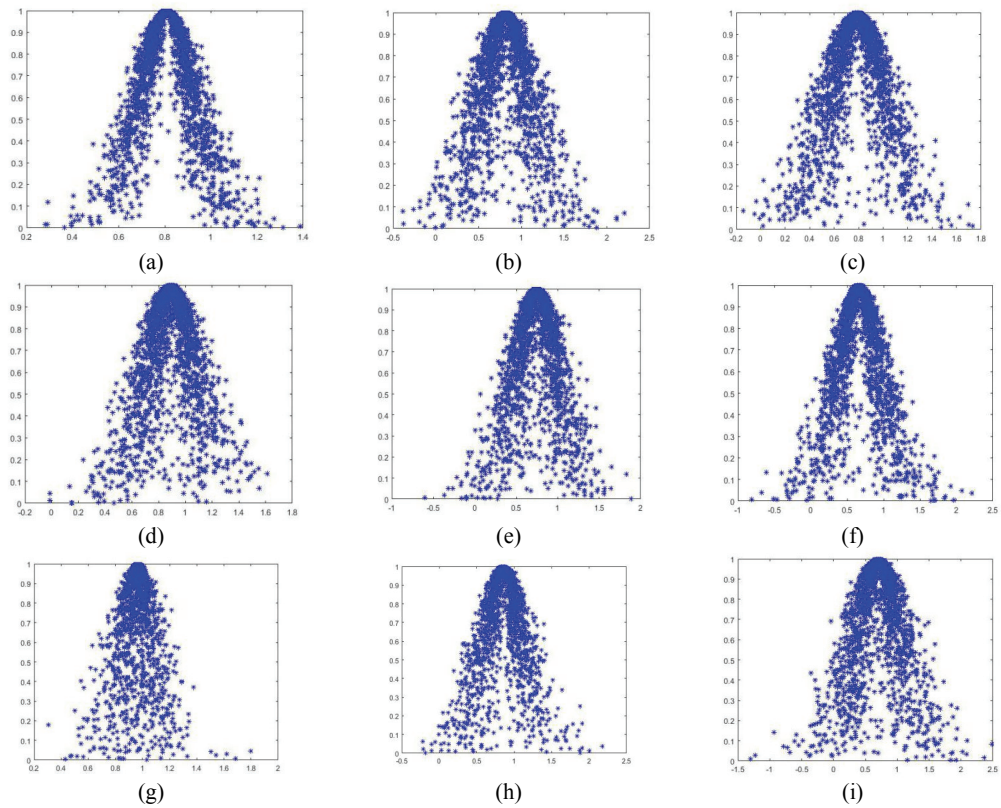


Fig. 3. Trust evaluation cloud for each service: (a) database service, (b) mobile services, (c) cloud communication service, (d) elasticity calculation, (e) video services, (f) storage services, (g) analysis service, (h) management and monitoring services, and (i) application service.

The results indicate that the trust values (0.8926 and 0.966) of cloud services S_4 and S_7 are very high and that the entropy values (0.1634 and 0.0724) are relatively small. This means that the uncertainty of these results is low. Thus, users can trust the cloud provider completely when using these cloud services. In sharp contrast to the aforementioned services, the trust value of service S_6 is 0.662, and the entropy value is 0.277. This shows that the degree of trust is general, and the uncertainty is high. When users choose this type of cloud service, their decision needs to be considered carefully.

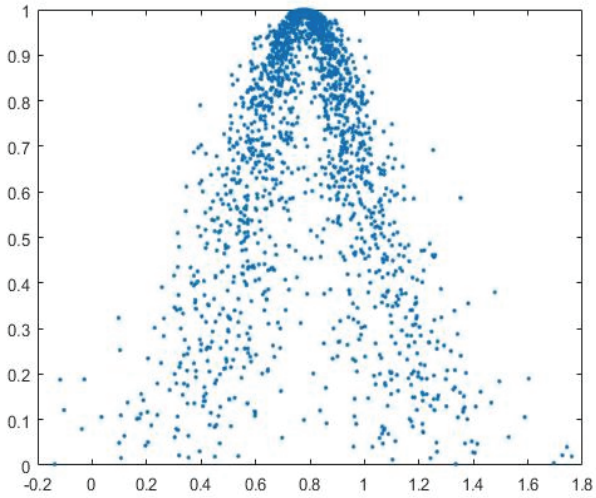


Fig. 4. Comprehensive trust evaluation cloud C = (0.8027, 0.202, 0.099).

The trust value of service S_9 is 0.7036 (relatively high), and the entropy value is 0.3278 (very high). This means that some people believe they can trust this service. Others believe should not trust this service because there is a large uncertainty with this kind of service. The trust of other services (S_1, S_2, S_3, S_5, S_7, and S_8) is relatively high, and the trust values are listed in Table 2. In general, users can choose these services more safely.

5.3 Comparison with Other Methods

In this section, we compare our model with the trust evaluation method in [17]. The sample dataset is the same as in [17] (Tables 3, 4). The weight vector value is calculated by the method described in Section 4.2:

$\omega = \{\omega_1, \omega_2, ..., \omega_{10}\}$ = (0.107, 0.097, 0.083, 0.122, 0.095, 0.094, 0.092, 0.084, 0.116, 0.110).

Table 3. Instance specifications for cloud database server

Database server	Type CPU cores	Memory (GB)	Storage
Small (S)	4	8–16	50 GB data volume
Medium (M)	8	16–32	100 GB data volume
Large (L)	16	32–64	200 GB data volume

Table 4. Compliance of 18 NCSPs

CSP	SP_{int}	SP_{fp}	MP_{sc}	MP_{td}	SRW_{dp}	RRW_{dp}	SRW_{pc}	RRW_{pc}	N_l	C_{od}
Amazon EC2 (S)	0.1027	0.1120	0.2794	0.2865	0.1354	0.0964	0.2144	0.2098	0.0831	0.036
DigitalOcean (S)	0.0826	0.1139	0.1962	0.2151	0.0806	0.0872	0.1401	0.1505	0.2494	0.0204
Google (S)	0.0875	0.0991	0.2986	0.2937	0.0128	0.0106	0.2549	0.2206	0.3603	0.0480
Microsoft Azure (S)	0.0575	0.0593	0.1195	0.1202	0.1449	0.1567	0.2133	0.2186	0.3270	0.0412
Rackspace (S)	0.1340	0.1595	0.2343	0.2271	0.4232	0.1939	0.3024	0.2897	0.2328	0.1166
SoftLayer (S)	0.0973	0.1208	0.2278	0.2129	0.2532	0.2418	0.2029	0.2864	0.0554	0.0405
Amazon EC2 (M)	0.1945	0.2066	0.2834	0.2806	0.3025	0.0914	0.1920	0.2152	0.0776	0.0720
DigitalOcean (M)	0.1728	0.1981	0.2029	0.2149	0.1021	0.1105	0.1300	0.1409	0.2162	0.0408
Google (M)	0.1687	0.1767	0.2938	0.2974	0.0255	0.0212	0.2567	0.2614	0.3658	0.0960
Microsoft Azure (M)	0.0956	0.1128	0.0482	0.0477	0.1446	0.156	0.2997	0.2231	0.3326	0.0823
Rackspace (M)	0.2307	0.2483	0.2382	0.2312	0.6158	0.8191	0.2357	0.2869	0.1607	0.2332
SoftLayer (M)	0.1876	0.2159	0.2352	0.2195	0.0634	0.0328	0.3193	0.2925	0.0665	0.0751
Amazon EC2 (L)	0.3501	0.3238	0.2814	0.2813	0.1521	0.0883	0.1906	0.2092	0.0610	0.1441
DigitalOcean (L)	0.2324	0.2741	0.2003	0.2188	0.1361	0.1473	0.1132	0.1220	0.1995	0.7666
Google (L)	0.2840	0.2586	0.2598	0.2761	0.0506	0.0426	0.2241	0.2659	0.3658	0.1209
Microsoft Azure (L)	0.4579	0.4019	0.2533	0.2430	0.1446	0.1560	0.2997	0.2231	0.3326	0.1921
Rackspace (L)	0.3976	0.3823	0.2376	0.2288	0.2732	0.1362	0.3084	0.3291	0.1275	0.4665
SoftLayer (L)	0.3543	0.3640	0.2086	0.2053	0.2536	0.2660	0.2000	0.1773	0.0721	0.1362

The evaluation results are listed in Table 5 and Fig. 5.

Table 5. Instance specifications for cloud database server

CSP	Normalized $Trust_i$ in our model	Normalized $Trust_i$ in [17]
Amazon EC2 (S)	0.4199	0.3893
DigitalOcean (S)	0.3708	0.3425
Google (S)	0.4694	0.4544
Microsoft Azure (S)	0.3995	0.3782
Rackspace (S)	0.6246	0.5769
SoftLayer (S)	0.4598	0.4443
Amazon EC2 (M)	0.5181	0.5079
DigitalOcean (M)	0.4236	0.4165
Google (M)	0.5462	0.5148
Microsoft Azure (M)	0.4212	0.4014
Rackspace (M)	0.8854	1
SoftLayer (M)	0.4569	0.4297
Amazon EC2 (L)	0.5695	0.6124
DigitalOcean (L)	0.6859	0.5563
Google (L)	0.5994	0.5936
Microsoft Azure (L)	0.7501	0.7777
Rackspace (L)	0.7915	0.7394
SoftLayer (L)	0.6080	0.7018

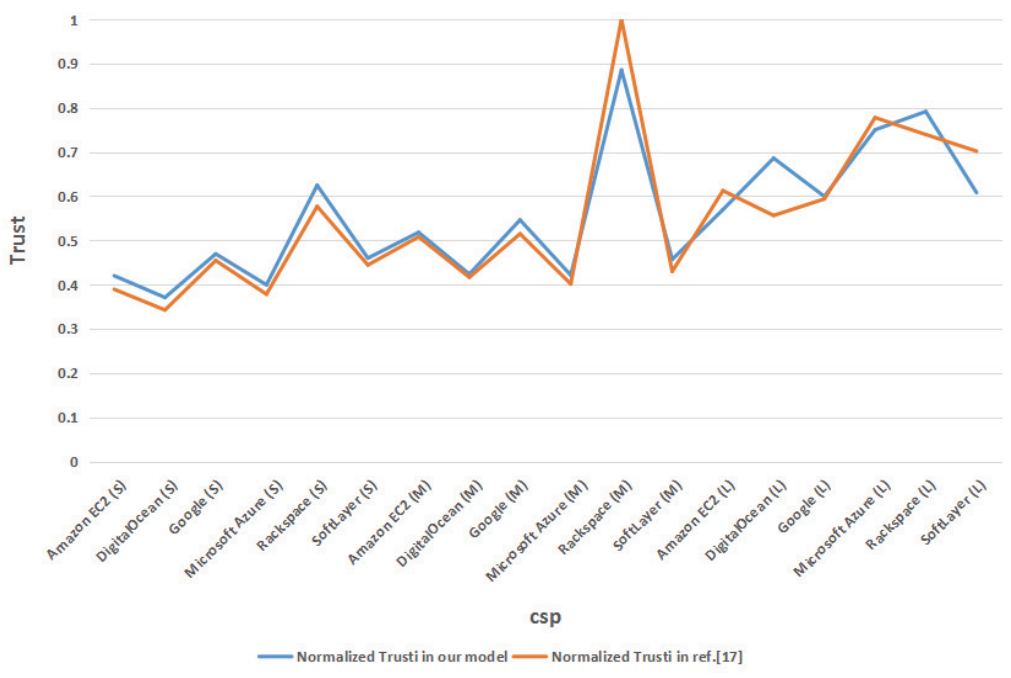


Fig. 5. Trust evaluation result comparison with a study of Sidhu and Singh [17].

6. Conclusion

Aiming at different cloud services, we researched the establishment of trust relationships between users and cloud computing service platforms. We concluded that the trust value cannot be accurately and effectively measured by analyzing existing trust evaluation models. To solve this problem, we designed a subjective preference weight allocation algorithm. The SPWA algorithm was used to integrate each evaluation result to obtain the trust evaluation value of the entire cloud service provider.

A flexible weight model was advanced by combining SPWA with the entropy method. The model can integrate subjective weight and objective weight. This overcomes the disadvantage of using only one traditional weight distribution scheme.

The use of the cloud model by the SPWA algorithm effectively makes the qualitative assessment of trust into a quantitative evaluation, and the evaluation results are more in line with the trust of fuzzy and subjective characteristics.

This paper did not identify the authenticity of the trust evaluation data, nor did it design reputation punishment for malicious users. Future work will enhance the model to make it more effective.

Acknowledgement

This work was supported by the project “Supply Chain Trust and Risk Research Based on Cloud Computing”, the Handan College School-level (No. 2017104).

References

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, et al., "A view of cloud computing," *Communications of the ACM*, vol. 53, no.4, pp. 50-58, 2010.

[2] D. G. Feng, M. Zhang, Y. Zhang, and Z. Xu, "Study on cloud computing security," *Journal of Software*, vol. 22, no. 1, pp. 71-83, 2011.

[3] Q. Xie, J. Wu, G. Wang, W. Liu, D. Chen, and X. Yu, "Provably secure authentication protocol based on convertible proxy signcryption in cloud computing," *Scientia Sinica Informationis*, vol. 42, no. 3, pp. 303-313, 2012.

[4] L. M. Vaquero, L. Rodero-Merino, and D. Moran, "Locking the sky: a survey on IaaS cloud security," *Computing*, vol. 91, no. 1, pp. 93-118, 2011.

[5] K. Hashizume, D. G. Rosado, E. Fernandez-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications*, vol. 4, article no. 5, 2013.

[6] C. Lin, W. B. Su, K. Meng, Q. Liu, and W. D. Liu, "Cloud computing security: architecture, mechanism and modeling," *Chinese Journal of Computers*, vol. 36, no. 9, pp. 1765-1784, 2013.

[7] J. Huang and D. M. Nicol, "Trust mechanisms for cloud computing," *Journal of Cloud Computing*, vol. 2, article no. 9, 2013.

[8] P. Manuel, "A trust model of cloud computing based on Quality of Service," *Annals of Operations Research*, vol. 233, no. 1, pp. 281-292, 2015.

[9] 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)*, vol. 47, no. 1, pp. 53-61, 2013.

[10] Z. Yang, X. Qin, Y. Yang, and T. Yagink, "A hybrid trust service architecture for cloud computing," in Proceedings of *2013 International Conference on Computer Sciences and Applications*, Wuhan, China, 2013, pp. 674-680.

[11] C. Li, S. Wang, L. Kang, L. Guo, and Y. Cao, "Trust evaluation model of cloud manufacturing service platform," *The International Journal of Advanced Manufacturing Technology*, vol. 75, no. 1-4, pp. 489-501, 2014.

[12] U. A. Kashif, Z. A. Memon, A. R. Balouch, and J. A. Chandio, "Distributed trust protocol for IaaS cloud computing," in *Proceedings of 2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, Islamabad, Pakistan, 2015, pp. 275-279.

[13] M. Chiregi, and 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.

[14] R. K. Chahal and S. Singh, "Fuzzy rule-based expert system for determining trustworthiness of cloud service providers," *International Journal of Fuzzy Systems*, vol. 19, no. 2, pp. 338-354, 2017.

[15] T. Lynn, L. van der Werff, G. Hunt, and P. Healy, "Development of a cloud trust label: a Delphi approach," *Journal of Computer Information Systems*, vol. 56, no. 23, pp. 185-193, 2016.

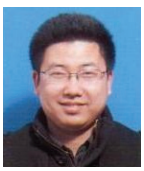
[16] A. Selvaraj and S. Sundararajan, "Evidence-based trust evaluation system for cloud services using fuzzy logic," *International Journal of Fuzzy Systems*, vol. 19, no. 2, pp. 329-337, 2017.

[17] J. Sidhu and S. Singh, "Improved topsis method based trust evaluation framework for determining trustworthiness of cloud service providers," *Journal of Grid Computing*, vol. 15, no. 1, pp. 81-105, 2017.

[18] 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.

[19] 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.

[20] Y. Wang, J. Wen, X. Wang, and W. Zhou, "Cloud service evaluation model based on trust and privacy-aware," *Optik*, vol. 134, pp. 269-279, 2017.
[21] N. Somu, G. R. MR, K. Kirthivasan, and S. S. VS, "A trust centric optimal service ranking approach for cloud service selection," *Future Generation Computer Systems*, vol. 86, pp. 234-252, 2018.
[22] M. Alhanahnah, P. Bertok, Z. Tari, and S. Alouneh, "Context-aware multifaceted trust framework for evaluating trustworthiness of cloud providers," *Future Generation Computer Systems*, vol. 79, pp. 488-499, 2018.
[23] M. B. Smithamol and S. Rajeswari, "TMM: trust management middleware for cloud service selection by prioritization," *Journal of Network and Systems Management*, vol. 27, no. 1, pp. 66-92, 2019.
[24] D. Li, H. Meng, and X. Sui, "Membership clouds and membership cloud generators," *Computer Research and Development*, vol. 32, no. 6, pp. 15-20, 1995.
[25] H. Chen and B. Li, "Approach to uncertain reasoning based on cloud model," *Journal of Chinese Computer Systems*, vol. 32, no. 12, pp. 2449-2455, 2011.
[26] Y. Du, Z. Song, and D. Li, "Mining association rules based on cloud model," *Journal of PLA University of Science and Technology*, vol. 1, no. 1, pp. 29-34, 2000.
[27] X. Y. Meng, G. W. Zhang, C. Y. Liu, J. C. Kang, and H. S. Li, "Research on subjective trust management model based on cloud model," *Journal of System Simulation*, vol. 19, no. 14, pp. 3310-3317, 2007.
[28] G. W. Zhang, D. Y. Li, P. Li, J. C. Kang, and G. S. Chen, "A collaborative filtering recommendation algorithm based on cloud model," *Journal of Software*, vol. 18, no. 10, pp. 2403-2411, 2007.
[29] G. Qiang and Y. M. Bi, "Effectiveness evaluation of command of missile information war based on cloud model," *Command Control & Simulation*, vol. 30, no. 4, pp. 61-64, 2008.
[30] J. Tian, H. Jiao, B. Wang, and C. Chen, "An e-commerce trust model based on expanded subjective logic," *International Journal of High Performance Computing and Networking*, vol. 9, no. 5-6, pp. 372-381, 2016.



Hongqiang Jiao **https://orcid.org/0000-0002-9840-6070**

He received his M.S. degree in computer application technology from Hebei University, China in June 2008. He is currently working towards his Ph.D. degree in management science and engineering at Hebei University, China. His current research interest includes network security and trust management.

Xinxin Wang **https://orcid.org/0000-0002-1353-6811**

She received her M.S. degree from Hebei University, China in June 2005. She works in Hebei University of Science and Technology as a professor. Her current research interest includes the art of management and software test.

Wanning Ding **https://orcid.org/0000-0002-3993-1916**

He received his M.S. degree in College of Information Engineering from Jiangnan University, China in June 2008. He is currently working as a professor in Handan College and his research interest include graphic processing and algorithm design and so on.