International Journal of Automation and Computing 12(2), April 2015, 208-219
DOI: 10.1007/s11633-014-0840-3

A Multi-dimensional Trust-aware Cloud Service Selection Mechanism Based on Evidential Reasoning Approach

Wen-Juan Fan[1, 2] Shan-Lin Yang[1, 3] Harry Perros[2] Jun Pei[1, 4]

[1]School of Management, Hefei University of Technology, Hefei 230009, China
[2]Department of Computer Science, North Carolina State University, Raleigh 27695-7534, USA
[3]The Ministry of Education Key Laboratory of Process Optimization and Intelligent Decision Making, Hefei 230009, China
[4]Department of Industry and System Engineering, University of Florida, Gainesville 32608, USA

Abstract: In the last few years, cloud computing as a new computing paradigm has gone through significant development, but it is also facing many problems. One of them is the cloud service selection problem. As increasingly boosting cloud services are offered through the internet and some of them may be not reliable or even malicious, how to select trustworthy cloud services for cloud users is a big challenge. In this paper, we propose a multi-dimensional trust-aware cloud service selection mechanism based on evidential reasoning (ER) approach that integrates both perception-based trust value and reputation based trust value, which are derived from direct and indirect trust evidence respectively, to identify trustworthy services. Here, multi-dimensional trust evidence, which reflects the trustworthiness of cloud services from different aspects, is elicited in the form of historical users′ feedback ratings. Then, the ER approach is applied to aggregate the multi-dimensional trust ratings to obtain the real-time trust value and select the most trustworthy cloud service of certain type for the active users. Finally, the fresh feedback from the active users will update the trust evidence for other service users in the future.

Keywords: Cloud service selection, multi-dimensional trust evidence, trust and reputation evaluation, evidential reasoning (ER), clond service trustworthiness.

1 Introduction

Cloud computing is a gradually maturing computing service paradigm where infrastructure and software resources are provided over the internet as scalable and on demand (web) services[1]. In a cloud computing environment, there is a huge amount of service providers that develop and deliver services to external users. With cloud environment becoming more complicated and unpredictable, cloud services are not always trustworthy, and the service level agreements (SLAs) may not satisfy users′ requirements. On the other hand, in a cloud environment, it is actually required that users give up their physical control to their applications and the underlying operations may be not transparent to them.

The above mentioned issues have caused the major concerns of cloud service users, which can be concluded as follows:

1) Whether the cloud service providers (especially those new comers) can be trusted or not, e.g., the cloud service providers shouldn′t spy the users′ data or sell them to their competitors. Besides, the users′ data and applications should be protected from any way of damage.

2) Whether the cloud services are always available or not, i.e., the cloud service providers should guarantee that their services supports "plug and play", just as the applications are equipped on local disks.

3) Whether other non-functional requirements, such as quality of services (QoS), are provided by cloud according to SLA, since users will not trust a cloud service just considering one factor, but for many properties they concern. In other word, the trust evidence should be multi-dimensional so as to reflect different aspects of the performance of the cloud services.

To ensure the normal operation and running of the whole cloud service system, trust management is essential for individuals to evaluate others and make satisfactory selection and thus can interact with the ones with high reputation[2, 3]. Therefore, there should be a mechanism which helps users to make right decisions on selecting trustworthy cloud services for further interactions. However, in existing web services, service descriptions via web service description language (WSDL) are not sufficient in service selection based on service trust[4].

In this paper, we propose a multi-dimensional trust-aware cloud service selection mechanism based on evidential reasoning (ER) approach, which aggregates individual users′ multi-dimensional trust feedback ratings to form the reputation values of the cloud service providers, and the reputation values serve for an important part (i.e., the reputation-based trust value) of the final trust value for the active user. Specifically, in this paper, two types of trust values are considered, which are perception-based trust value and reputation-based trust value. The perception-based trust value uses the perception of the active user based on the direct service interactions as trust evidence,

Regular paper
Manuscript received March 26, 2013; accepted March 13, 2014
This work was supported by National Natural Science Foundation of China (Nos. 71131002, 71071045, 71231004 and 71201042).
Recommended by Associate Editor Dong-Ling Xu

and reputation-based trust value uses the reputation values which have been assigned to the services based on other users′ interactions as trust evidence. Unlike other previous studies on trust-based service provider selection, which just takes local trust as the direct trust of one individual, and reputation as the aggregate trust value of all individuals, we integrate the reputation into individual′s local trust (i.e., the reputation-based trust value) using a mapping function, such that the final trust value can take two aspects of individual′s trust opinion, i.e., how much the active user trusts the cloud service provider and how much he/she trusts other users′ trust evaluation. This multi-dimensional trust-aware mechanism can address the following issues: 1) establishing a real-time trust-evidence base for all the cloud services that are enrolled in cloud system, including trust value base for each user experienced services and reputation value base for all users′ aggregate trust opinion on each service; 2) assigning dynamic trust and reputation level to cloud services before selecting them, i.e., the priori trust evaluation; 3) dynamically selecting the optimal services and building a feedback mechanism for service users, i.e., the posterior trust assignment.

The paper is structured as follows. Section 2 reviews the related work. Section 3 analyzes users′ main trust requirements for cloud services, and corresponding multi-dimensional trust evidence from multiple sources and in different formats. In Section 4, we introduce our proposed cloud service selection mechanism framework. In Section 5, the detailed mechanism is described to express the cloud service selection problem. We conduct a case study to illustrate our mechanism in Section 6. And the paper is concluded in Section 7.

2 Related works

2.1 Basic trust theory

It has been widely recognized that trust is an important issue in a lot of scenarios including social science and information technology service domain. Although the definitions of trust are borrowed from the social science literature, there is no consensus on trust notion in distributed computer networks[5], and the definitions are usually discipline-specific[6]. Broadly speaking, trust means an act of faith, confidence, and reliance in something that is expected to behave or deliver as promised[7]. The concept of trust adjusted to the case of two parties involved in a transaction can be described as "An entity A is considered to trust another entity B when entity A believes that entity B will behave exactly as expected and required." The notion of trust in an organization could be defined as the customer′s certainty that the organization is capable of providing the required services accurately and infallibly[8].

Trust involves many associated factors, such as reputation, risk, uncertainty, expectation, etc. First of all, by evaluating and storing the reputation ("what is generally said or believed about a person or the character or standing of a thing") of other members, it is possible to calculate how much those members can be trusted ("the firm belief in the reliability or truth or strength of an entity") to perform a particular task[9]. Secondly, just as the content mentioned above, the trust relation between the service providers and users involves the problems of taking risks under uncertainties, and behavior expectation and prediction. Trust is essential in reducing risk and uncertainty when an individual has to work in an environment over which he has no control[10]. Cloud computing is such an environment and participating parties have to rely on intermediaries′ security services to realize a specific task or make a deal with each other.

Traditional research on software and information systems mostly concentrates on functionality features of specific system units. Nevertheless, it is the service capacity that users purchase and really concern in cloud computing service system, instead of a fixed hardware resource. In addition, the physical resources are logically virtualized, thus do not bind to specific system units. Therefore, in a cloud computing environment, the criterion of service trustworthiness and influential factors is more complex than before. As a result, we should establish trust relation that is distinct for the virtual environment and separate from the hosting platform[11].

2.2 Trust and reputation models

The study of trust and reputation has many applications in information and communication technologies. A trust model is an assessment system which quantifies trust values, and is used to measure the trustworthiness of the entities in the system. The trust model proposed in [12] is one of the earliest. The model only takes into account direct interactions. It differentiates three types of trust: basic trust, general trust, and situation trust[13]. Modern approaches model trust as two values: probability and certainty. The probability theory can be utilized to design trust models. For instance, the Bayes′ theorem has been used as a tool for designing Bayesian trust models that promote a probabilistic view of trust, so that a priori probability based on the observation towards trust can be used to make predictions on the outcomes in the future. Based on Bayesian trust network model, Commerce et al.[14, 15] introduced a binary assessment method, which used satisfaction and dissatisfaction as input and recorded the results of the assessment by Beta probability function.

The reason for using trust is that in many distributed systems, especially those of an open and dynamic nature, it is not feasible to use traditional techniques that involve a central source guaranteeing the reliability of users and resources. Designing a trust model to enhance trust in distributed computing has been an important step toward the security and privacy in such a decentralized and mobile space. Most trust mechanisms in distributed systems consist of either using certificates as a guarantee or reputation derived from the experiences of other entities in the system[16].

To increase the flexibility of network computing systems, many researchers have proposed trust-based approaches, i.e., the trust information sharing mechanisms, algorithms for selecting entities to trust, evaluation mechanisms and so on in distributed systems, such as peer-to-peer networks[2, 3, 17], ad hoc sensor network[18], ubiquitous computing, and electronic commerce communities. However, due to the uncertainty of the trust cognition and the inherent human subjective nature in the trust evaluation, there are still big challenges needed to be addressed.

A multi-dimensional trust model is based on a multi-dimensional evaluation model towards the trust value. In most network communities, trustworthiness has multi-dimensional properties. There are extended and multi-dimensional trust factors that have influences on the trust evaluation. Li et al.[3] proposed a trust model for large-scale P2P computing, in which multiple factors are incorporated to reflect the complexity of trust, and the weights are dynamically assigned to the factors by weighted moving average and ordered weighted averaging (WMA-OWA) combination algorithms. Wang and Wu[19] proposed a multi-dimensional evidence-based trust management system with multi-paths to conduct trust computation on any arbitrarily complex trusted graph. This approach has some innovations on the three-tier trust computation respectively on node tier, path tier, and graph tier.

Nowadays, the study of trust models for cloud computing is still in the early stage, and many of them borrow the methods and ideas from grid computing, P2P computing and other distributed computing environments. The common feature of all the studies is that there are no reliable centralized trusted nodes. Persasice trust management model based on D-S theory (PTM) which is the sub-project of ubiquitous security (UBISEC) is supported by European IST FR6. It defines the trans-domain dynamic trust model based on the pervasive environment, and uses improved evidential theory to model the trust[20−23]. The trust values are updated according to the history records and other factors. In Sun′s model[24, 25], which is a trust model based on entropy theory and applies a modified evidential reasoning approach, the trust values are calculated using the probability of the weighted average method. The George′s model[26] is a trust model based on semi-ring algebra theory, in which the trust problem is described as a directed graph routing problem, and trust values are calculated using semi-ring algebra and finally conduct trust evaluation. Song and Hwang[27] proposed a dynamic fuzzy logic trust model based on grid, which includes the definition and description of trust, the fuzzy reasoning and evaluation of trust relationship, and the updating and evolution of trust values.

Recent research on trust model provides us with a promising starting point for a solution to service selection[28]. Quite number of trust research argues that trust management emerges as an essential complementary to security mechanisms[19, 29], while using trust evaluation model to address service selection involving complex relation and contradiction between the nodes is rare. Our previous work introduced a two-stage process to evaluate the trustworthiness of cloud services[30]. This paper focuses on the service selection in cloud computing environment considering the trust value of the service providers and users′ preference, based on the overview of the trust models in the main service environment.

2.3 Evidential reasoning algorithm

Evidential reasoning means reasoning with evidence, which can be used to handle different types of uncertainty in multi-attribute decision making (MADM) processes, including incompleteness (or ignorance) and vagueness (or fuzziness). The core idea of ER is that it is based on the belief structure which is considered as evidence for decision making under a variety of uncertainties. A belief structure is represented by an expectation that was originally designed to model a subjective assessment with uncertainty[31−33]. A modeling framework for representing subjective assessments is constructed, in which a set of evaluation grades for a qualitative attribute is defined. An attribute is evaluated to one or more grades with certain degrees of belief.

The ER algorithm has been widely applied in many related areas such as software selection[34, 35], software safety synthesis[19], E-Commerce security assessment[36] and E-Commerce risk assessment[37]. Besides, there are already some ER-based software tools developed which are used to help with the MADM process for applications, such as the intelligent decision system (IDS)[38]. In this paper, we will use this tool in the process of cloud service selection.

3 Cloud trust issues

3.1 Multiple trustworthiness factors in cloud

Basically, uncertainties can result in untrustworthiness in cloud services. In cloud service system, a range of uncertainties, such as bugs, faults, breakdowns, or misbehaviors from the underlying system infrastructure to the service interface level can have impact on trust. Obviously that the larger uncertain the cloud service system is, the less trustworthiness it can achieve. Based on the main concerns to cloud services, we conclude the following three aspects of key requirements for trust:

1) The key requirements for the system operational performance: Under this level, the attributes are usually quantitative and can be acquired from the system records or simulation experiments.

2) The key requirements for the QoS: In the context of web services, it requires a precise description of the non-functional properties of the services offered. Some of the service properties such as throughput, scalability, latency and so on are commonly referred to as quality of service.

3) The key security and privacy requirements for cloud services: The concerns on this aspect are cloud-specific,

as the characteristics of cloud computing environment are more uncertain and dynamic than the traditional computing environments. So the privacy concern is considered as an important facet of cloud service trustworthiness[39].

Table 1 shows the details of the requirements for cloud service trustworthiness respectively in three aspects. In Table 1, the key requirements are tightly related to the trust from users to services. Here, the definition of trust is inherited from the idea that "trust is a level of belief representing the relationship established between two entities for a specific action", i.e., the trust that entity A (usually a users) places in entity B (usually a service provider (SP)) is the degree of entity A's certainty (or belief) that entity B will behave for a specific action with required standard which will satisfy entity A's request. In this sense, trust can be considered as the trustworthiness indicator of the service that a SP can provide, which is also a subjective evaluation measurement from the perspective of users. We propose a multi-indicator evaluation system to evaluate different aspects of the SP′s interactions with the users, based on which the multi-dimensional trust evidences can be generated.

3.2 Trust evidence in cloud

In general, the trust evidence of a service for a user can be divided into two categories, one is the historical records of his/her direct interactions with the service, the other is the direct interaction records of other users with the service.

Therefore, as for service users, there are mainly two types of evidence that can be used for service trustworthiness evaluation, which are respectively: 1) Direct evidence: It is derived from the direct service interactions between the service provider and the user, i.e., if the user has used the service before, then his/her perception is the direct evidence whether the service is trustable or not. 2) Indirect evidence: If the service users have not experienced the service before, then the service trustworthiness evaluation can be only made based on the reputation value which is trustable according to the other users′ feedback, so the indirect evidence is the active user′s trust opinion based on the other recommendation from the users who have direct interactions with the service.

Trust evidence also has the characteristic of multi-dimension. Just as mentioned above, there are multi-indicators reflecting users′ different aspects of requirements and measuring trustworthiness of cloud services. We associate the multiple trustworthiness indicators/attributes with the trust value evaluation process, i.e., the service trustworthiness evaluation is actually an MADM problem. In this paper, we apply ER model to integrate the multi-dimensional trust evidence, which is in the form of multi-attribute feedback from users.

If cloud system makes best use of the multi-dimensional trust evidence, then it will provide reliable enough service selection suggestion. A trust evidence based cloud service selection mechanism is needed to search, elicit, and process multi-dimensional evidence.

4 Cloud service selection mechanism framework

Our proposed cloud trust service selection mechanism is used for eliciting, integrating, processing, and aggregating all the trust evidence in the system, and giving them optimal choice of service selection according to users′ specific requirements for the trustworthiness of the service.

The cloud service selection mechanism is composed of five modules:

Request specification module is used to receive users′ specifications on both the functional and non-functional requirements for the services. There are many services meeting the functional requirements but some of them may not satisfy the non-functional requirements. Through this module, users can describe their requirements from different dimensions of attribute, such as service type, reliability, response time, etc. The specification would be in certain forms, including numerical data, linguistic data, which will be introduced in detail in the following section.

Evidence collection module is used for extracting and collecting trust evidence, especially those reflecting users′ most concerned factors for trust in cloud services. And the evidence either comes from the direct historical transactions of the active user, or from the indirect trust relation with other users which give their feedback ratings on the cloud service. All the evidence is elicited into the evidence base for temporal use.

Trust/Reputation value evaluation module performs the core function of the cloud trust management system. The trust/reputation value evaluation module is to compute the service trust value and reputation value based on the collected trust evidence. Here, the trust value is the local trust value of the active user, so different users may attain different trust values on the same cloud service. The reputation value is actually the global trust value, which reflects the global trust opinion about the cloud service. Then the real-time trust and reputation value of the services will dynamically update the trust value base and reputation base respectively.

Table 1 Concerned requirements on cloud service

Key operational performance requirements	Key QoS requirements	Key security and privacy requirements
Adaptability	Availability	Openness and transparency
Resilience	Reliability	Controllability
Scalability	Usability	Access and accuracy
flexibility	Consistency	Accountability
Continuity	Quick response	Auditability

Service selection module is responsible for matching users′ requirements for cloud service trustworthiness and the trust values of all the optional services. If there is any matched pair, this module will select and invoke the service that best satisfies the active user and send him/her a report of the service trust value evaluation.

For assessment feedback module, after choosing to use the service that is selected by service selection module for the active user, he/she can give the multi-dimensional feedback ratings back to the assessment feedback module. This module is used for storing the real-time updating assessment from users.

Trust/reputation value management module performs the function of real-time updating of the reputation/trust value of cloud services, which is based on the trust value evaluation module that gives the priori trust value of services, and the assessment feedback module that gives the posterior trust value evaluation of the specific services.

Fig. 1 shows our cloud service selection mechanism framework. In Fig. 1, there are two important types of databases, i.e., the trust value database and the reputation value database. Once a user has used a specific cloud service, he/she will start his/her own trust value base, which stores the local trust value assigned by the individual user on the services that he/she has used, and the trust value is assigned by the user according to his/her satisfaction to the direct interactions with the services, and also can be updated with new interactions. So the trust value bases are separated by the user domains and distributed over the cloud service user domain. In view of this, the trust value base stores each user′s direct trust evidence on the cloud services that he/she has experienced before, and this type of trust evidence is the subjective and personalized view to the services.

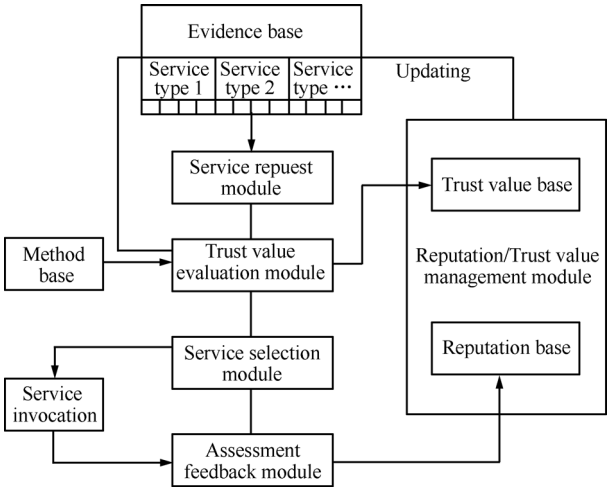


Fig. 1 Cloud service selection mechanism framework

On the other hand, the reputation base stores the reputation value of each service, and it is calculated based on the aggregation of all the feedback assessment given by the experienced users. In this paper, the assessment results are users′ posterior evaluation of all the services after using them, and the reputation value of each service is the global opinion aggregation of all the users. We will introduce the two types of bases in the next section.

5 Mechanism design

In this section, we first investigate the main concerned issues on cloud service trust and reputation evaluation process. The main problems can be concluded as follows: First of all, there are various attributes which reflect cloud service users′ various requirements for the cloud service trustworthiness. Secondly, since all these attributes are evaluated by users either qualitatively or quantitatively, the trust value evaluation is needed to be made in a unified framework. Last but not the least, as the trust evidence is collected in different forms, the evidence must be changed into a unified manner.

5.1 Problem definition

Suppose the following problem: A group of consumers $c^j(j = 1, 2, \cdots, n)$ need to rank a set of cloud services $s_i(i = 1, \cdots, m)$ according to the degree of satisfaction for each service, so as to select an optimal service that can best meet an active user′s needs. Here the service selection problem is to determine the optimized trust level associated with the service′s implementations, i.e., picking the most trustworthy service. This is reasonable only if the trust assignment depends on the service implementation′s qualities[40]. Next we will give some mathematical description and definitions of the related notions.

Definition 1 (Cloud provider). A cloud provider $cp \in CP$ is a double-tuple $\langle N_m, R_s \rangle$, where N_m is the name of the cloud provider, and R_s denotes the service resource (or functions) that the cloud provider can offer to service providers or directly to the end users.

Definition 2 (Service provider). A service provider $sp \in SP$ is a triple-tuple $\langle i, s, c \rangle$, where $i \in In$ is the interface that the service provider offers, $s = \langle s1, \cdots, s_n \rangle$ is a set of cloud services that it provides, and c denotes the cloud provider(s) that the service provider is depending on.

Definition 3 (Cloud service). A cloud service $cs \in CS$ is a five-tuple $\langle id, T, p, f, cp \rangle$, in which $id \in ID$ is the ID number of the service, and $T \in Tc$ is the type of cloud service, $p \in Pr$ is the service provider that offers this service, $f \in Func$ is a set of key function(s) that the service can perform, and cp is the cloud provider that hosts this service.

Definition 4 (Service trust evidence). For each service user, the service trust evidence is a triple-tuple $\langle id, \Phi_1, \Phi_2 \rangle$, in which id is the ID number of the services that have existed in the cloud service system, Φ_1 denotes the direct trust evidence related to the service, i.e., the evidence comes from the trust value base of all the users who have used the specific service before, and Φ_2 denotes the indirect trust evidence, which comes from the reputation base storing the aggregated assessment reputation value of the specific service. Here, service trust evidence is associated with the multi-attribute trustworthiness.

Definition 5 (Service trust value). The service trust value may not be unique, since it is actually a user-service trust value, i.e., the service trust value is the subjective evaluation that reflects an active user′s trust opinion on the service. Service trust value is a four-tuple $\langle su, id, t, tv\rangle$, where su is the user who assigns trust value to the specific service, id is the specific service′s ID number, t is corresponding time scale of the service′s trust value, and tv is the real-time service′s trust value.

Definition 6 (Service reputation value). The reputation value of a service is a global evaluation result of the specific service, which is a triple-tuple $\langle id, t, Rp\rangle$, where id is the specific service′s ID number, t is the time scale of the assigned reputation value to the service, and Rp is the corresponding reputation value of the service on the t-th instant.

5.2 Cloud service selection process

1) User $c_j(j = 1, \cdots, n)$ sends his/her service request R_j to the cloud service system, then the system selects the services of which both the type T and the function f meet the demands of the service user. And the remaining services are included into a service set $FS_j = \{FS_j^1, FS_j^2, \cdots, FS_j^m\}$ which indicates that there are m services which can satisfy the user′s functional requirements, and the number from 1 to m represents the index of the service.

2) Elicit the active user′s nonfunctional requirements for service, i.e., the key attributes concerned by the user. These requirements can form an attribute choice space (ACS). Here we assume that there are q dimensions of requirements specified by active user c_j:

$$req_j = \{Q_j^1, Q_j^2, \cdots, Q_j^q\}. \tag{1}$$

Besides, user c_j assigns weights to all the required attributes, according to the importance that user c_j considers to cloud service trustworthiness. The assigned weights are

$$w^j = \{w_j^1, w_j^2, \cdots, w_j^q\}. \tag{2}$$

3) Elicit trust evidence of all the service $FS_j^k \in FS_j(1, \cdots, m)$ from evidence base. There are two sources of trust evidence, i.e., direct evidence Φ_1 and indirect evidence Φ_2. The direct interaction evidence is elicited from the history records that he/she has direct interaction with the service. If he/she has not interacted with the service before, then the direct evidence will be null. The indirect evidence is elicited from the history records of other users who have direct interactions with the cloud service.

4) Calculate the services′ reputation value: Based on the total feedback assessment of the service, the real-time global reputation values of services $FS_j^k(k = 1, \cdots, m)$ are calculated, which are based on the global user′s history records. The results then update the latest reputation values of the services $FS_j^k(k = 1, \cdots, m)$ in the reputation value base.

5) Evaluate the services′ trust values by the active user c_j: Based on the direct and indirect trust evidence, calculate the real-time trust values of services $FS_j^k(k = 1, \cdots, m)$. In this paper, we introduce two types of trust values, which are perception-based trust value and reputation-based trust value, respectively. The former one is calculated according to the direct evidence elicited from the user′s history records under the circumstance that he/she has interacted with the service before. The latter one is applied when the active user has no interaction with the service before, and it is calculated based on the reputation value of the service, associated with the user′s personalized mapping function from reputation value to trust value, i.e., how much user c_j trusts the reputation value of the service. If the user c_j has interacted with the service, his/her trust value for this service is calculated considering the two types of trust values. The results then update the latest trust values of services $FS_j^k(k = 1, \cdots, m)$ in the individual trust value base of the user c_j.

6) Calculate the aggregated trustworthiness of services $FS_j^k(k = 1, \cdots, m)$. In this paper, the cloud service trustworthiness depends on the trust value and reputation value of the services. The two values should be assigned relative weights when they are aggregated. The weight assignments to trust value and reputation value by different users will be varied too. In other word, if the user c_j is inclined to trust himself/herself more, then the weight of trust value will be larger, otherwise larger weight should be assigned to reputation value of the service.

7) Select the optimal service. Based on the calculated results of the trustworthiness of all the services in FS_j, the service selection module then helps the active user c_j to select the most trustworthy service.

8) Collect the feedback assessment from the user c_j. After using the selected service, the user c_j is asked to give his/her assessment to the attributes in the specified ACS $req_j = \{Q_j^1, Q_j^2, \cdots, Q_j^q\}$ which is rated to five grades: best, good, average, poor, and worst. The feedback ratings will form new evidence for the selected service.

5.2.1 Reputation value calculation

Here, the services′ reputation values are evaluated through multiple attributes in the ACS $req_j = \{Q_j^1, Q_j^2, \cdots, Q_j^q\}$, then how to calculate the reputation value is an MADM problem. For each attribute $Q_j^r(r = 1, \cdots, q)$, let Θ be a frame of discernment, and let the basic probability assignment (BPA) be specified as the function m: $2^\Theta \to \{0, 1\}, m(\phi) = 0$, and $\sum_{H_n \in \Theta} m(\{H_n\}) = 1$, where ϕ is the null set and 2^Θ is the power set of Θ. Here H_n is referred to the evidence where n denotes the degree of user satisfaction with the attribute of the service. Let those users give their assessments to five grades as best, good, average, poor, and worst, which are denoted as $H = \{H_1, H_2, H_3, H_4, H_5\}$. A belief structure is used to describe subjective assessment information of the attributes in the ACS, and the MADM problem can be modeled using the following expectations for service $FS_j^k(k = 1, \cdots, m)$ to attributes $Q_j^r(r = 1, \cdots, q)$ in the t-th time window:

$$S^t(Q_j^r(FS_j^k)) = \{(H_i, \beta_{i,j,k}^t(FS_j^k)), i = 1, \cdots, 5\}$$
$$r = 1, \cdots, q, \quad k = 1, \cdots, m \tag{3}$$

where $\beta^t_{i,k,r}(FS^k_j) \geq 0$, $\sum_{i=1}^{5} \beta^t_{i,k,r}(FS^k_j) \leq 1$, $\beta^t_{i,k,r}(FS^k_j)$ denotes a degree of belief that an attribute Q^r_j at an alternative FS^k_j is assessed to a grade H_i with a degree of belief of $\beta^t_{i,k,r}(FS^k_j)(i = 1, \cdots, 5)$ in the t-th time window. And a generalized decision matrix D_g with $S(Q^r_j(F^k_j))$ as its elements is constructed as

$$D_g = (S^t(Q^r_j(FS^k_j)))_{r\times n}. \tag{4}$$

Then the evaluation results can be aggregated using the following evidential reasoning algorithm:

$$m^t_{i,k,r} = w^r_j \beta^t_{i,k,r}(FS^i_j),\ i = 1, \cdots, 5,\ k = 1, \cdots, m \tag{5}$$

$$m^t_{H,k,r} = 1 - \sum_{i=1}^{5} m^t_{i,k,r} = 1 - w^k_j \sum i = 1^5 \beta^t_{i,k,r}(FS^k_j),$$
$$k = 1, \cdots, m, \quad r = 1, \cdots, q \tag{6}$$

$$\{H_i\} : m_{i,I(k+1),r} = K^t_{I(k+1)} m^t_{i,I(k)} m^t_{H,k+1} +$$
$$m^t_{H,I(k)} m^t_{i,k+1}, \quad i = 1, \cdots, 5 \tag{7}$$

$$\{H\} : m^t_{H,I(k+1)} = K^t_{I(k+1)} m^t_{H,I(k)} m^t_{H,k+1} \tag{8}$$

$$K^t_{I(k+1)} = \left[1 - \sum_{u=1}^{5} \sum_{v=1,v\neq u}^{5} m^t_{u,I(k)} m^t_{v,k+1}\right]^{-1},$$
$$k = 1, \cdots, N-1 \tag{9}$$

$$\beta^t_h(FS^k_j) = C_2 = \sum_{r=1}^{q} w_r (1 - \sum_{n=1}^{5} \beta^t_{n,k}(FS^k_j)) \tag{10}$$

$$\beta^t_i(FS^k_j) = \frac{1 - C_2}{1 - m^t_{H,I(q)}} m^t_{i,I(q)},\ i = 1, \cdots, 5 \tag{11}$$

where $m^t_{i,I(1)} = m^t_{i,1} (n = 1, \cdots, 5)$ and $m^t_{H,I(1)} = m^t_{H,1}$. The aggregated assessment for FS^k_j can be described by

$$S(y(FS^k_j)) = \{(H_i, \beta^t_i(FS^k_j)), i = 1, \cdots, 5\}. \tag{12}$$

Suppose the utility of an evaluation grade H_i is denoted by $u(H_i)$, then the expected utility of $S(y(FS^k_j))$ is defined as

$$u(S(y(FS^k_j))) = \sum_{i=1}^{5} u(H_i) \beta^t_i(FS^k_j). \tag{13}$$

The maximum, minimum and average utilities of FS^k_j are given by

$$u^t_{\max}(FS^k_j) = \sum_{i=1}^{4} \beta^t_i(FS^k_j) u^t(H_i) +$$
$$(\beta^t_N(FS^k_j) + \beta^t_H(FS^k_j) u^t(H_N)) \tag{14}$$

$$u^t_{\min}(FS^k_j) = (\beta_1(FS^k_j) + \beta^{\mathrm{T}}_H(FS^k_j)) u^t(H_1) +$$
$$\sum_{i=2}^{5} \beta^t_i(FS^k_j) u^t(H_i) \tag{15}$$

$$u^t_{\mathrm{aver}}(FS^k_j) = \frac{u^t_{\max}(FS^k_j) + U^t_{\min}(FS^k_j)}{2}. \tag{16}$$

Here we use the average utility of FS^k_j as the reputation value of service FS^k_j in the t-th time window.

5.2.2 Trust value calculation

In this part, we introduce two types of trust values: perception-based and reputation-based trust values, which are respectively inferred based on the subjective interactions and objective reputation. The final trust value of the service is aggregated by the two types of trust values.

1) Perception-based trust value: p_Trust

If an active user c_j has used the service before, p_Trust value of the service is based on the direct perception of the interaction(s). For a specific service $(FS^k_j)(i = 1, \cdots, 5)$, we assume that the active user c_j has interacted with the service for $\tau^k_j (\tau^k_j \geq 1)$ times. Let $p\_Trust^{\tau^k_j}_j(r)$ denote the perception-based trust value by user c_j for service k on attribute $Q^r_j (r = 1, \cdots, q)$ after τ^k_j-th interaction, $V^{\tau^k_j}_j(r) \in [0, 1]$ denotes the real-number assessment to the attribute r's performance when the user c_j finishes the τ^k_j-th interaction with the service, and $Rp^t(k)$ denotes the reputation value of service k in the t-th time window, respectively. The formulas are

$$p\_Trust^{\tau^k_j}_j(k_r) = \alpha_1 \times p\_Trust^{\tau^k_j - 1}_j(k_r) + \alpha_2 \times V^{\tau^k_j}_j(k_r) \tag{17}$$

where $\alpha_1 + \alpha_2 = 1, \alpha_1, \alpha_2 > 0$, and if $\tau^k_j = 1$, then $p\_Trust^1_j(k) = V^1_j(k)$.

Here the service's trust value vector by the user c_j is formed as

$$\{p\_Trust^{\tau^k_j}_j(k_1), \cdots, p\_Trust^{\tau^k_j}_j(k_r), \cdots, p\_Trust^{\tau^k_j}_j(k_q)\},$$
$$r = 1, \cdots, q \tag{18}$$

where each component in the vector denotes respective perception trust value on each attribute r's $(r = 1, \cdots, q)$ performance of the service.

Then, these multi-attribute based perception trust values are aggregated to form a general trust value of the service, by combining each attribute's weight of the service, which is calculated as

$$p\_Trust^{\tau^k_j}_j(k) = \sum_{r=1}^{q} w_r \times p\_Trust^{\tau^k_j}_j(K_r). \tag{19}$$

However, this is not the final trust value of the service, since trust decays with time. In other word, if the user used the service once long time ago, obviously the level he/she trusts the service now should be less than the trust level when he/she just finished the interaction. In view of this, here we introduce a decay factor σ of time. Then the real-time perception-based trust value is calculated using

$$p\_Trust^t_j(k) = p\_Trust^{\tau^k_j}_j(K) \times (1 - \sigma)^{\tau^k_j}. \tag{20}$$

2) Reputation-based trust value: r_Trust

Besides direct trust relationship, there is indirect trust which is based on the service's reputation value, i.e., the trust level of the user on the service's reputation value. It needs to be noted here that reputation value and reputation-based trust value may be confused with each

other. However, there is a significant difference between them, i.e., the reputation-based trust value is still a subjective and personalized opinion of users. The service′s reputation-based trust value by the user needs to add a mapping function of the service′s reputation value, which reflects the user′s preference, bias, belief, etc.

Therefore, in order to fit an approximate mapping function curve for the active user, we have to do some preliminary survey to get some representative points. First of all, the users can be roughly divided into three types, which are respectively positive users, neutral users, and negative users. No matter which type the user belongs to, the mapping function is a non-decreasing function. If the user belongs to the neutral user group, then the curve will be a straight line with 45 degrees, which is based on the survey result that he/she totally believes the reputation trust value.

Fig. 2 is an example for the three classes of user, where the convex curve, the straight line, and the concave curve represent the mapping function of positive, neutral, and negative users, respectively.

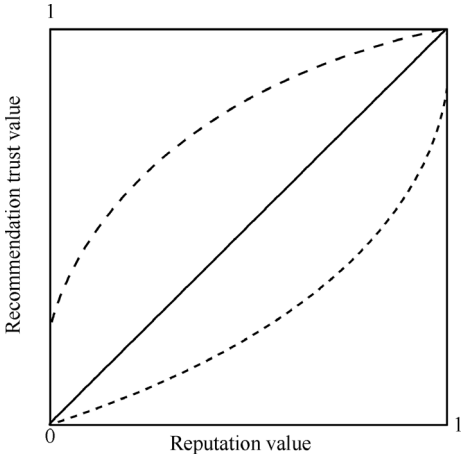


Fig. 2 Mapping function curves

The three lines are the simplest curves, and the real curves that describe the mapping function from reputation value to reputation-based trust value are not straight and may be nonlinear.

There are some questions should be answered by the active user, which are

1) If the reputation value of the service is 0, then how much will you trust it?

2) If the reputation value of the service is 1, then how much will you trust it?

3) If the reputation value of the service is 0.5, then how much will you trust it?

4) If the reputation value of the service is 0.25, then how much will you trust it?

5) If the reputation value of the service is 0.75, then how much will you trust it?

The answers to these questions should also be in [0, 1]. From the above five questions, we can get five representative points of the active user′s mapping function from the reputation value to the reputation-based trust value. If the curve is not smooth enough and more precision is needed, then we can get more points by asking the active user more questions like these. It needs to be noted that the function is not fixed, since users′ preference, bias, and other factors are changing along with time. Therefore, it has to approximate the curve once the users change their altitude to reputation value of the service.

Assume the reputation of service FS_j^k at $(t-1)$-th time window is $Rp_j^{t-1}(k)$, and we can use $f^t(FS_j^k)$ as the user′s approximated mapping function, denoted as

$$f(FS_j^k) = f(RP_j^{t-1}(k)). \tag{21}$$

For the users who have not experienced the service before, the final trust value of service FS_j^k will be equal to reputation-based trust value r_Trust. However, for the users who have experienced the service, the final trust value of service FS_j^k is aggregated by perception-based trust value and reputation-based trust value. Due to the subjective feature of trust, the weights assigned to the two types of trust values depend on the active user′s relative belief level on himself/herself and other cloud service users. Assuming the weight assigned to the perception-based trust value by user c_j is ω_j^P, and that assigned to the reputation-based trust value is ω_j^R, then the final trust value of service FS_j^k is calculated by

$$TV_j^t(k) = \omega_j^P \times (p\_Trust_j^t(k)) + \omega_j^R \times (r\_Trust_j^t(k)). \tag{22}$$

5.2.3 Service selection and feedback assessment

Based on the final trust values of the candidate services, the service that has the largest trust value in the chosen service set FS_j will be selected automatically by the cloud service selection system and then be invoked.

After using the service, the user can give his/her latest perceived performance feedback ratings on the service, of which the attributes in his/her ACS are to be rated into five grades as best, good, average, poor, and worst. All these assessments will then be stored into the reputation base to update it. In addition, the user will be asked to assign the latest trust value on the service, and the value will be stored into the user′s trust value base to update his/her local trust evaluation on the service.

From the above analysis to our proposed cloud service selection mechanism, we can see that the process actually forms a circulation, i.e., prior trust and reputation values of cloud services can be served as the trust evidence to calculate the real-time trust and reputation values, which will be reused again as trust evidence in the future by the user or others. By applying this service selection mechanism, the cloud service system will provide more trustworthy services to users.

6 Case study

In this section, we will illustrate our proposed multi-dimensional trust-aware cloud service selection mechanism

based on ER approach by a case study.

Suppose there is an active user c_j, who wants to select an online office service in a cloud service system, where there are a mass of service providers that can offer this type of service. We assume that after the preliminary screening, there are five services $\{FS_j^1, FS_j^2, \cdots, FS_j^5\}$ which can meet user c_j's functional needs, and the cloud service selection mechanism has to select the most trustworthy one according to his nonfunctional requirements for service. Assume that the nonfunctional attributes chosen by c_j is ACS_j. These attributes are adaptability, scalability, availability, reliability, quick response, controllability, and security, which can be denoted by $\{Q_j^1, Q_j^2, \cdots, Q_j^7\}$. The weights of these concerned attributes according to relative importance deemed by the user are respectively $\{w_j^1, w_j^2, \cdots, w_j^7\} = \{0.1, 0.14, 0.19, 0.18, 0.11, 0.13, 0.15\}$.

Then the evidence is to be elicited from the evidence base, including the direct and indirect evidence. Assume that until the t-th time window, there are two services that user A has used before, denoted as $\{FS_j^1, FS_j^2\}$ and the rest three services are not used, which are denoted as $\{FS_j^3, FS_j^4, FS_j^5\}$.

1) For services $\{FS_j^3, FS_j^4, FS_j^5\}$, the active user′s reputation-based trust value are respectively denoted as $r\_Trust_j^4$ and $r\_Trust_j^5$, respectively. Before calculating the reputation-based trust value, the reputation value of the service on t-th time window is to be calculated first. The belief structures of the performance of the 7 nonfunctional attributes are denoted in Tables 2–4 (here we use the probability mass as the belief degree):

Then we aggregate the belief structures on each attributes. In order to facilitate the calculation process of evidential reasoning, here we use the intelligent decision system (IDS) to get the final assessments of the services, which are served as their reputation values. The results are shown in Fig. 3.

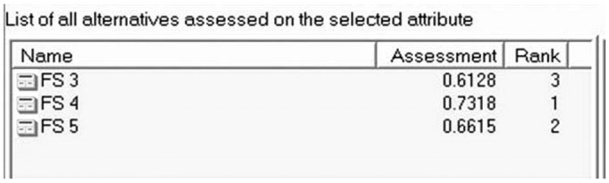


Fig 3 The assessment results of reputation-based trust value of FS_j^3, FS_j^4, and FS_j^5

Therefore, the reputation value of services FS_j^3, FS_j^4 and FS_j^5 are respectively 0.6128, 0.7318 and 0.6615. Then user c_j is asked to complete a survey to get his mapping function from the reputation value to reputation-based trust value. Assume that the answers to these questions can approximate a mapping function curve as shown in Fig. 4.

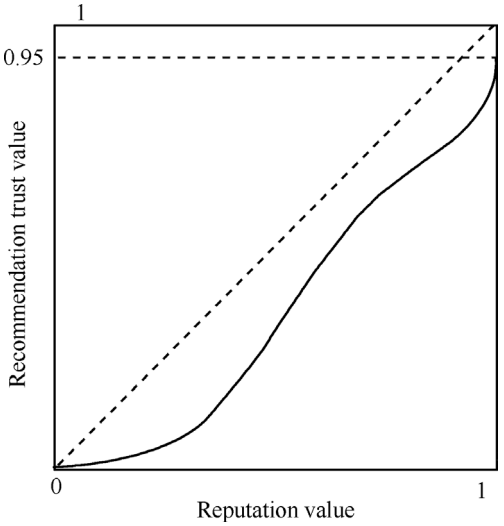


Fig. 4 Mapping function curves of the user

Table 2 The belief structures for services FS_j^3, FS_j^4 and FS_j^5-(1)

Services	Q_j^1	Q_j^2
FS_j^3	$\{H_1, 0; H_2, 0.1; H_3, 0.4; H_4, 0.3; H_5, 0.2\}$	$\{H_1, 0; H_2, 0.2; H_3, 0.5; H_4, 0.2; H_5, 0.1\}$
FS_j^4	$\{H_1, 0; H_2, 0; H_3, 0.1; H_4, 0.3; H_5, 0.6\}$	$\{H_1, 0; H_2, 0; H_3, 0.4; H_4, 0.4; H_5, 0.3\}$
FS_j^5	$\{H_1, 0; H_2, 0; H_3, 0.3; H_4, 0.4; H_5, 0.3\}$	$\{H_1, 0; H_2, 0.1; H_3, 0.3; H_4, 0.4; H_5, 0.2\}$

Table 3 The belief structures for services FS_j^3, FS_j^4 and FS_j^5-(2)

Services	Q_j^3	Q_j^4
FS_j^3	$\{H_1, 0; H_2, 0.1; H_3, 0.3; H_4, 0.4; H_5, 0.2\}$	$\{H_1, 0; H_2, 0.1; H_3, 0.5; H_4, 0.2; H_5, 0.2\}$
FS_j^4	$\{H_1, 0; H_2, 0; H_3, 0.1; H_4, 0.6; H_5, 0.3\}$	$\{H_1, 0; H_2, 0; H_3, 0; H_4, 0.8; H_5, 0.2\}$
FS_j^5	$\{H_1, 0; H_2, 0; H_3, 0.3; H_4, 0.5; H_5, 0.2\}$	$\{H_1, 0; H_2, 0.1; H_3, 0.2; H_4, 0.4; H_5, 0.3\}$

Table 4 The belief structures for services FS_j^3, FS_j^4 and FS_j^5-(3)

Q_j^5	Q_j^6	Q_j^7
$\{H_1, 0; H_2, 0.1; H_3, 0.5; H_4, 0.2; H_5, 0.2\}$	$\{H_1, 0; H_2, 0.1; H_3, 0.5; H_4, 0.4; H_5, 0.2\}$	$\{H_1, 0.1; H_2, 0.2; H_3, 0.5; H_4, 0.1; H_5, 0.1\}$
$\{H_1, 0; H_2, 0; H_3, 0.4; H_4, 0.4; H_5, 0.2\}$	$\{H_1, 0; H_2, 0; H_3, 0.4; H_4, 0.4; H_5, 0.2\}$	$\{H_1, 0; H_2, 0.1; H_3, 0.3; H_4, 0.4; H_5, 0.2\}$
$\{H_1, 0; H_2, 0.1; H_3, 0.6; H_4, 0.2; H_5, 0.1\}$	$\{H_1, 0; H_2, 0; H_3, 0.6; H_4, 0.3; H_5, 0.1\}$	$\{H_1, 0; H_2, 0.1; H_3, 0.6; H_4, 0.2; H_5, 0.1\}$

From Fig. 4 we can see that the user c_j is a negative user, i.e., his reputation-based trust value is smaller than the corresponding reputation value. Then the corresponding reputation-based trust value can be attained as

$$TV_j^t(FS_j^3) = r\_Trust_j^3 = 0.5786$$
$$TV_j^t(FS_j^4) = r\_Trust_j^4 = 0.6843$$
$$TV_j^t(FS_j^5) = r\_Trust_j^5 = 0.6729.$$

2) As for services $\{FS_j^1, FS_j^2\}$, they have been used by the user c_j before. First of all, the reputation value of these services also needs to be calculated. The other users′ aggregate belief structures on each attribute are listed in Tables 5–7.

We use IDS to get the assessment results to the services $\{FS_j^1$ and $FS_j^2\}$, as shown in Fig. 5.

List of all alternatives assessed on the selected attribute

Name	Assessment	Rank
FS 1	0.8000	1
FS 2	0.7250	2

Fig. 5 The assessment results of reputation value of FS_j^1 and FS_j^2

So, the real-time reputation values of services FS_j^1 and FS_j^2 are 0.8 and 0.725, respectively.

Next, the user′s perception trust values on the services are to be calculated.

Assume that the user c_j has used FS_j^1 and FS_j^2 for once and twice respectively, with $d_j^{FS_j^1} = 2$, $d_j^{FS_j^2} = 1$, $\alpha_1 = 0.4$, and $\alpha_2 = 0.6$. And there is $V_j^1(FS_j^1) = \{0.35, 0.75, 0.5, 0.75, 0.6, 0.45, 0.3\}$ and $p\_Trust_j^{t-2}(FS_j^2) = \{0.6, 0.45, 0.5, 0.75, 0.8, 0.4, 0.6\}$. So we have $p\_Trust_j^{t-2}(FS_j^1) = \{V_j^1(FS_j^1(k))\} \times \{w_k\} = 0.544$ and $p\_Trust_j^{t-1}(FS_j^2) = \{\alpha_1 \times p\_Trust_j^{t-2}(FS_j^2(k)) + \alpha_2 \times V_j^2(FS_j^1(k))\} \times \{w_k\} = 0.5788$.

Then $p\_Trust_j^t(FS_j^1) = p\_Trust_j^{t-2}(FS_j^1) \times (1-0.05)^2 = 0.491$ and $p\_Trust_j^t(FS_j^2) = p\_Trust_j^{t-1}(FS_j^1)(1-0.05)^2 = 0.55$.

Combining the reputation value of the services, for which the weight is 0.4, we have $TV_j^t(FS_j^1) = 0.6 \times 0.491 + 0.4 \times 0.8 = 0.6146$ and $TV_j^t(FS_j^2) = 0.6 \times 0.55 + 0.4 \times 0.75 = 0.63$.

Now we have the ranking of the five services based on the final trust value as $FS_j^4 \succ FS_j^2 \succ FS_j^5 \succ FS_j^1 \succ FS_j^3$.

Therefore, the cloud service selection mechanism will recommend the user c_j to select service FS_j^4 in the end.

7 Conclusions

The service selection problems in cloud computing environment are significant for users to get the satisfactory services according to their requirements. This paper proposes a novel and effective mechanism for cloud service selection based on multi-attribute trust value evaluation. The trust value evaluation is based on two aspects of trust: perception-based trust and reputation-based trust, of which the trust evidence is stored in the trust value base and reputation base. Users can get the trust evidence from the two bases, and then use the evidential reasoning approach to form the final trust results. For the service users, after using the service, they will give their feedback evaluation for the cloud system, which is stored in the trust value base and reputation value base for other users to get the indirect trust evidence. This approach is effective in cloud systems, since the trust value is generated from both the direct trust evidence (perception-based trust value) and personalized indirect trust evidence (reputation-based trust value), which is consistent with the service users′ requirements.

Table 5 The belief structures for services FS_j^1 and FS_j^2-(1)

Services	Q_j^1	Q_j^2
FS_j^1	$\{H_1, 0; H_2, 0; H_3, 0.2; H_4, 0.4; H_5, 0.4\}$	$\{H_1, 0; H_2, 0; H_3, 0; H_4, 0.4; H_5, 0.6\}$
FS_j^2	$\{H_1, 0; H_2, 0.1; H_3, 0.2; H_4, 0.4; H_5, 0.3\}$	$\{H_1, 0; H_2, 0; H_3, 0.2; H_4, 0.3; H_5, 0.5\}$

Table 6 The belief structures for services FS_j^1 and FS_j^2-(2)

Services	Q_j^3	Q_j^4
FS_j^1	$\{H_1, 0; H_2, 0; H_3, 0.1; H_4, 0.5; H_5, 0.4\}$	$\{H_1, 0; H_2, 0; H_3, 0.1; H_4, 0.4; H_5, 0.5\}$
FS_j^2	$\{H_1, 0; H_2, 0; H_3, 0.3; H_4, 0.4; H_5, 0.3\}$	$\{H_1, 0; H_2, 0.1; H_3, 0.2; H_4, 0.4; H_5, 0.3\}$

Table 7 The belief structures for services FS_j^1 and FS_j^2-(3)

Q_j^5	Q_j^6	Q_j^7
$\{H_1, 0; H_2, 0; H_3, 0.2; H_4, 0.4; H_5, 0.4\}$	$\{H_1, 0; H_2, 0.1; H_3, 0.1; H_4, 0.4; H_5, 0.5\}$	$\{H_1, 0; H_2, 0; H_3, 0.5; H_4, 0.4; H_5, 0.1\}$
$\{H_1, 0; H_2, 0; H_3, 0.3; H_4, 0.5; H_5, 0.2\}$	$\{H_1, 0; H_2, 0; H_3, 0.4; H_4, 0.2; H_5, 0.2\}$	$\{H_1, 0; H_2, 0; H_3, 0.5; H_4, 0.1; H_5, 0.2\}$

References

[1] G. Andrzej, M. Brock. Toward dynamic and attribute based publication, discovery and selection for cloud computing. *Future Generation Computer Systems*, vol. 26, no. 7, pp. 947–970, 2010.

[2] L. Xiong, L. Liu. Peer-trust: Supporting reputation-based trust in peer-to-peer communities. *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 6, pp. 843–857, 2010.

[3] X. Y. Li, F. Zhou, X. D. Yang. A multi-dimensional trust

evaluation model for large-scale P2P computing. *Journal of Parallel Distributed Computing*, vol. 17, no. 6, pp. 837–847, 2011.

[4] W. Tao, G. Q. Zhang. Trusted interaction approach for dynamic service selection using multi-criteria decision making technique. *Knowledge Based Systems*, vol. 32, pp. 116–122, 2012.

[5] Y. Sun, W. Yu, Z. Han, J. R. Liu. Information theoretic framework of trust modeling and evaluation for ad hoc networks. *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 305–317, 2006.

[6] N. V. Ozaa, T. Halla, A. Rainera. Trust in software outsourcing relationships: An empirical investigation of Indian software companies. *Information and Software Technology*, vol. 48, no. 5, pp. 345–354, 2006.

[7] M. K. Khaled, M. Qutaibah. Establishing trust in cloud computing. *IT Professional*, vol. 12, no. 5, pp. 20–27, 2010.

[8] Z. Dimitrios, L. Dimitrios. Addressing cloud computing security issues. *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, 2012.

[9] J. Lopez, R. Roman, A. Isaac, F. Carmen. Trust management systems for wireless sensor networks: Best practices. *Computer Communications*, vol. 33, no. 9, pp. 1086–1093, 2010.

[10] S. Yang. Security and Trust Management in Collaborative Computing, Ph. D. dissertation, University of Florida, USA, 2003.

[11] F. J. Krautheim, D. S. Phatak, T. Alan Sherman. Introducing the trusted virtual environment module: A new mechanism for rooting trust in cloud computing. In *Proceedings of the 3rd International Conference on Trust and Trustworthy Computing*, *Lecture Notes in Computer Science*, Springer, Berlin, Germany, vol. 6101, pp. 211–227, 2010.

[12] S. Marsh. Formalizing Trust as a Computational Concept, Ph. D. dissertation, University of Stirling, UK, 1994.

[13] J. Sabbater, C. Sierra. A. Isaac, F. Carmen. Review on computational trust and reputation models. *Artificial Intelligence Review*, vol. 24, no. 1, pp. 33–60, 2005.

[14] B. E. Commerce, A. Josang, R. Ismail. The beta reputation system. In *Proceedings of the 15th Bled Electronic Commerce Conference*, Bled, Slovenia, pp. 41–55, 2002.

[15] Q. Xue, K. Cao. Research on evaluation of transaction trust model for P2P network. *Energy Procedia*, vol. 13, pp. 66–72, 2011.

[16] T. Jiang. Autonomic Trust Management in Dynamic Systems, Ph. D. dissertation, University of Maryland, USA, 2007.

[17] F. Almenarez, A. Marin, D. Diaz, A. Cortes, C. Campo, C. Garcia-Rubio. Trust management for multimedia P2P applications in autonomic networking. *Ad Hoc Networks*, vol. 9, no. 4, pp. 687–697, 2011.

[18] P. B. Velloso, R. P. Laufer, D. de O Cunha, O. C. M. B. Duarte, G. Pujolle. Trust management in mobile ad hoc networks using a scalable maturity-based model. *IEEE Transactions on Network and Service Management*, vol. 7, no. 3, pp. 172–185, 2010.

[19] G. J. Wang, J. Wu. Multi-dimensional evidence-based trust management with multi-trusted paths. *Future Generation Computer Systems*, vol. 27, no. 5, pp. 529–538, 2011.

[20] F. Almenárez, A. Martín, C. Campo, R. C. García. PTM: A Pervasive Trust management model for dynamic open environments. In *Proceedings of the 1st Workshop on Pervasive Security, Privacy and Trust*, IEEE, Boston, USA, pp. 1–8, 2004.

[21] F. Almenárez, A. Martín, C. Campo, R. C. García. Trust AC: Trust-based access control for pervasive devices. In *Proceedings of the 2nd International Conference on Security in Pervasive Computing*, Springer, Boppard, Germany, pp. 225–238, 2005.

[22] F. Almenárez, A. Martín, D. Diaz, J. Sanchez. Developing a model for trust management in pervasive devices. In *Proceedings of the 4th Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, IEEE, Pisa, Italy, pp. 267–272, 2006.

[23] H. Jameel, L. X. Hung, U. Kalim, A. Asjjad, S. Y. Lee, Y. K. Lee. A trust model for ubiquitous systems based on vectors of trust values. In *Proceedings of the 7th IEEE International Symposium on Multimedia*, IEEE, Irvine, CA, USA, vol. 4, pp. 674–679, 2005.

[24] Y. Sun, W. Yu, Z. Han, J. R. Liu. Trust modeling and evaluation in ad hoc networks. In *Proceedings of the Global Telecommunications Conference*, IEEE, St. Louis, Missouri, USA, vol. 3, pp. 1862–10867, 2005.

[25] R. He, J. W. Niu, G. W. Zhang. CBTM: A trust model with uncertainty quantification and reasoning for pervasive computing. In *Proceedings of the 3rd International Symposium on Parallel and Distributed Processing and Application*, *Lecture Notes in Computer Science*, Springer, Nanjing, China, vol. 3758, pp. 541–552, 2005.

[26] G. Theodorakopoulos, J. S. Baras. On trust models and trust evaluation metrics for ad-hoc networks. *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 318–328, 2006.

[27] S. Song, K. Hwang. Fuzzy trust integration for security enforcement in grid computing. In *Proceedings of IFIP International Conference on Network and Parallel Computing, Lecture Notes in Computer Science*, Springer, Wuhan, China, vol. 3222, pp. 9–21, 2005.

[28] C. Hang, M. P. Singh. Trustworthy service selection and composition. *ACM Transactions on Autonomous and Adaptive Systems*, vol. 6, no. 1, Article 5, 2006.

[29] I. Abbadi, A. Martim. Trust in the Cloud. *Information Security Technical Report*, vol. 16, no. 3, pp. 108–114, 2011.

[30] W. J. Fan, S. L. Yang, J. Pei. A novel two-stage model for cloud service trustworthiness evaluation. *Expert Systems*, vol. 32, no. 2, pp. 136–153, 2014.

[31] J. B. Yang, M. G. Singh. An evidential reasoning approach for multiple attribute decision making with uncertainty. *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 24, no. 1, pp. 1–18, 1994.

[32] J. B. Yang, P. Sen. Preference modelling by estimating local utility functions for multi-objective optimization. *European Journal of Operational Research*, vol. 95, no. 1, pp. 115–138, 1996.

[33] J. B. Yang. Rule and utility based evidential reasoning approach for multi-attribute decision analysis under uncertainties. *European Journal of Operational Research*, vol. 131, no. 1, pp. 31–61, 2001.

[34] C. Fu, S. Yang. The group consensus based evidential reasoning approach for multiple attribute group decision analysis. *Expert Systems with Applications*, vol. 206, no. 3, pp. 601–608, 2012.

[35] S. L. Yang, C. Fu. Constructing confidence belief functions from one expert. *Expert Systems with Applications*, vol. 36, no. 4, pp. 8537–8548, 2009.

[36] Y. J. Zhang, X. Y. Deng, D. J. Wei, Y. Deng. Assessment of E-Commerce security using AHP and evidential reasoning. *Expert Systems with Applications*, vol. 39, no. 3, pp. 3611–3612, 2009.

[37] R. H. Khokhar, D. A. Bell, J. W. Guan, Q. W. Wu. Risk assessment of E-commerce projects using evidential reasoning. In *Proceedings of the 3rd International Conference on Fuzzy Systems and Knowledge Discovery*, *Lecture Notes in Computer Science*, Xi′an, China, vol. 4223, pp. 621–630, 2006.

[38] D. L. Xu, McCarthy, J. B. Yang. Intelligent decision system and its application in business innovation self assessment. *Decision Support Systems*, vol. 42, no. 2, pp. 664–673, 2006.

[39] S. Pearson. Taking account of privacy when designing cloud computing services. In *Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing*, IEEE, Vancouver, BC, Canada, pp. 44–52, 2009.

[40] D. Li, C. H. Yang. A trust evaluation model for web service selection. In *Proceedings of the 3rd International Symposium on Intelligent Information Technology and Security Informatics*, IEEE, Jinggangshan, China, pp. 306–310, 2010.

Wen-Juan Fan received the B. Sc. degree at Nanjing University of Aeronautics and Astronautics, China in 2009. She received the Ph. D. degree and is currently a lecturer at School of Management, Hefei University of Technology, China. She was working as a visiting scholar in the Department of Computer Science, North Carolina State University, Raleigh, USA, when working on this paper.

Her research interest include intelligent decision making theory under cloud computing environment.

E-mail: wfan3@ncsu.edu (Corresponding author)
ORCID iD: 0000-0002-6633-0358

Shan-Lin Yang was graduated from Hefei University of Technology, China in 1985. He has been affiliated with Hefei University of Technology as a full professor since 1985. He is now is a professor and Ph. D. adviser at the School of Management, Hefei University of Technology, China. He is currently a member of the Chinese Academy of Engineering.

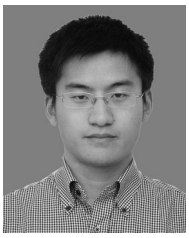
His research interests include decision theory, artificial intelligence, information management and information systems.

E-mail: hgdysl@gmail.com

Harry Perros is a professor of computer science, an alumni distinguished graduate professor, and the co-founder and program coordinator of the master of science degree in computer networks at North Carolina State University, USA. He is an IEEE fellow.

His research interests including the areas of next generation networks, multi-domain routing, resource allocation under QoS, and queueing theory.

E-mail: hp@ncsu.edu



Jun Pei received the B. Sc. degree at Hefei University of Technology, China. He received the Ph. D. degree and is currently a lecturer at School of Management Hefei University of Technology, China in 2009. He was working as a visiting scholar in the Department of Industrial and Systems Engineering, University of Florida, USA, when working on this paper.

His research interests include intelligent decision making theory, production scheduling, and algorithms.

E-mail: feiyijun.ufl@gmail.com