Wang SX, Zhang L, Wang S *et al.* A cloud-based trust model for evaluating quality of Web services. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 25(6): 1130–1142 Nov. 2010. DOI 10.1007/s11390-010-1090-7

A Cloud-Based Trust Model for Evaluating Quality of Web Services

Shou-Xin Wang (王守信), *Member CCF*, Li Zhang (张　莉), *Member CCF*, Shuai Wang (王　帅) and Xiang Qiu (邱　翔)

Institute of Software Engineering, School of Computer Science & Engineering, Beihang University, Beijing 100191, China

E-mail: shouxin_wang@126.com; lily@buaa.edu.cn; wangshuai_911@sina.com; qiuxiang008@126.com

Received July 8, 2009; revised September 20, 2010.

Abstract Because trust is regarded as an essential secured relationship within a distributed network environment, selecting services over the Internet from the viewpoint of trust has been a major trend. Current research about trust model and evaluation in the context of Web services does not rationally and accurately reflect some essential characteristics of trust such as subjective uncertainty and dynamism. In this paper, we analyze some important characteristics of trust, and some key factors that affect the trust relation in the Web service environment. Accordingly, we propose a trust model based on Cloud Model theory to describe the subjective uncertainty of trust factors. A time-related backward cloud generation algorithm is given to express the dynamism of trust. Furthermore, according to the trust model and algorithm, a formalized calculation approach is provided to evaluate the trust degree of services requestors in providers. Our experiment shows that the evaluation of trust degree can effectively support trust-decisions and provide a helpful exploitation for selecting services based on the viewpoint of trust.

Keywords Web service, trust, trust evaluation, Cloud Model

1 Introduction

Web services are emerging to provide a systematic and extensible framework for application-to-application interaction, built on top of existing Web protocols and based on open XML (extended mark-up language)[1-2]. Quality of service (QoS) may serve as a key benchmark to discern differences among alternatives. Traditional QoS covers a whole range of definitions such as response time, accessibility, availability, reliability. However, in an open Internet environment, it is necessary to objectively relate service quality to the users' subjective perceptions[2-3]. Therefore, from the service consumer perspective, some researchers have recognized that the trust relation between service consumers and providers may be an important and necessary quality[4-7]. According to the trust relation, service consumers can identify trustworthy providers with whom they should interact and untrustworthy ones with whom they should avoid interaction.

Trust has been regarded as an essential securited relationship within a distributed network environment[8]. In general, trust can be viewed as the outcome of observations leading to the subjective belief that the actions of another may be relied upon to achieve a goal in a risky situation[9]. Trust is updated over time through direct interactions or information provided by others about experiences they have had[10].

In the context of Web services, trust also has a vital influence on services requestor activities and on interaction success. According to the trust relation, a services consumer can identify trustworthy service providers with whom they should interact and avoid risk caused by interaction with untrustworthy ones. Many researchers have investigated the issue of trust in the area of Web services. But most of them do not represent and reflect some essential characteristic of trust such as subjective uncertainty, time decay.

In this paper, we will firstly introduce some previous related research in Section 2. Then we will analyze the characteristics of trust in Section 3. Furthermore, a trust model is introduced according to some key factors that affect the trust relation in the context of Web Services. In Section 4, we make use of Cloud Model to represent the subjective uncertainty of computable factors including a new time-related backward cloud generation algorithm which generates the numerical characteristics of the Cloud Model to reflect the dynamism of subjective belief. Section 5 provides a quantitative approach to evaluate the trust degree of service consumers

Regular Paper

This work was supported by the National Basic Research 973 Program of China under Grant No. 2007CB310803, and the National Natural Science Foundation of China under Grant No. 90818017.

to providers. Section 6 provides the experiment applying this approach. Finally we summarize this paper and point out possible research directions for our future work.

2 Related Work

Maximillen *et al.* designed a conceptual model of Web service reputation in order to improve automatic selection for Web services[11-12]. Liangzhou Zeng *et al.*[7] also used reputation as one of the attributes of QoS for Web services composition. In these approaches, service reputation can be evaluated by the average rating given by end-users. Sravanthi Kalepu *et al.*[13] think that the reputation measurement using the average rating cannot capture the degree of variance in the service providers' compliance levels. They introduced a novel metric named Verity to quantify the consistency in compliance levels of a service contract. Verity refers to the degree of variance in the compliance levels of a service provider and provides a mechanism for assessing the service provider's reputation[13]. Unfortunately, verity is also computed by means of averaging compliance of quality attributes of Web services.

The evaluation methods for trust mentioned above are in terms of probabilistic models. In these approaches, trust degree depends on an average of sample data. However, trust is not an objective property of trustees but a subjective degree of belief of trusters about trustees[14]. Producing belief is a cognitive process during which the objective property of trustees would be mapped into a person's brain and some knowledge or concepts about trust would be formed such as *great trust* or *high trust*. This process has obvious subjective uncertainties including fuzziness and randomness[15-16]. The uncertainty of trust comes from both the objective property of trustees such as reputation and subjective cognition of trusters. For example, given a certain Web service, the reputation of it would change randomly over time, for instance 0.65, 0.66, 0.69. According to these reputations, trust degree of truster also would randomly change. This reflects one aspect of the randomness of trust. Fuzziness indicates that trust is not an absolute thought model. In other words, trust is not "either this or that" but "both this and that". For example, given a Web service, the value of its reputation is 0.65. A trustee usually does not claim simply that he trusts the service greatly. Rather, the trustee tends to place *great trust* in the service to some degree. Sometimes a trustee may both greatly and highly trust the service whose reputation is 0.65. Even though the trustee trusts the service greatly, he still may trust it a little more this time than that time. This situation embodies the randomness of subjective cognition of the truster.

Probabilistic models regard uncertainty of trust as randomness, and ignore the fuzziness of subjective belief. Additionally, the average of sample data cannot reflect the characteristic of subjective cognition about trust. Therefore, mathematical probability is unsuitable as a trust metric in dealing with uncertainty[17].

Moreover, the above approaches did not take into account the dynamic nature of trust. The dynamic nature of trust refers to the changes of trust levels. Historical trust values usually decay with time and have a relatively lesser affect on current trust-decision making. Therefore time-decay of trust may be an important factor which must be considered for trust representation and evaluation approaches.

Similar with human society, multi-agent environment is full of uncertainty. Therefore, trust research is of great significance for the solution to the interaction problem of agent entities. In multi-agent environment, trust is derived from direct trust and reputation. Reputation system is a mechanism to support trust evaluation.

Direct trust is the subjective cognition which comes from the agent's own knowledge and its direct interaction experience; the reputation system collects opinions of other agents about target agent and gets trust evaluation by reasoning process. However, the information of the target agent is incomplete or inaccurate, which results in negative effect for trust rating. So two trust factors, trustworthiness and risk, are proposed based on the objective features of Web service in this research.

In multi-agent environment, the subjectivity of trust comes from the target agent's subjective measurement, relying on the subjective cognitive of evaluating agent. The typical measure theories such as Jurca model[38], altruism of Schillo[39] and FIRE model[40], share the common feature that stiff associate evaluation concept with the discrete score, for example general trust corresponds to 3. But how to discriminate 2.5 or 3.5? This research will construct the map between qualitative concept and quantitative description using Cloud Model and analyze the fuzziness in trust by dynamic degree of membership.

In multi-agent environment, the evaluation is ahead of the interaction so the benefit risk is unavoidable. But few effective methods of recent researches are applying for the assessment and quantification of risk. This research will define the risk formally and measure it by the change tendency of reputation and trustworthiness.

Furthermore, Lea[41] proposed a comprehensive, dynamic trust ontology for trust description. Our research also proposed some characteristics for trust in Web service area. These characteristics come from the

objective features of Web service such as reputation score, SLA protocol, quality attributes. They are less complete than trust ontology but more concrete.

3 Definitions and Characteristics of Trust

Trust is a multidimensional concept that can be studied from the viewpoint of many disciplines, including social psychology, sociology, economics, and marketing[18]. Some researchers tend to examine trust as subjective cognizance. As Josang[19] states, trust is the belief that an entity has about others from their past experiences and knowledge about the entity's nature. This belief expresses an expectation on the entity's behavior, which implies risk. Elosfson defines trust as the outcome of observations leading to the belief that the actions of another may be relied upon to achieve a goal in a risky situation[20]. Additionally, Montaner *et al.* argue that trust will be updated over time through direct interaction or information provided by others about experiences they have had[21].

It is easy to see that definitions in [19-20] attempt to express trust based on its real social nature. From society's viewpoint, people use trust in a subjective manner for almost everything. Trust is not an objective property of trustees but a subjective degree of belief of trusters about trustees. Therefore, most researchers recognize that it is apparent that the belief has subjective uncertainty factors such as fuzziness and randomness. Another element that the definitions have in common is a goal perspective of trust. While trusters decide to trust others, it means that some of their goals depend on the actions of the trustees. Furthermore, trusters may be in a risky situation while a trust relation is built, and they will obtain potential benefit as well as potential loss.

Dynamism is another important characteristic of trust. Dynamism means that a trust relation is not stable and is changing over time. The trust degree of trusters to trustees will increase and decrease with the positive and negative experience of trusters during interaction with trustees.

According to the above definitions of trust, it may be concluded that the four important characteristics of trust are subjectivity, goal-driven, risk, and dynamism. We consider these four important characteristics of trust to form the basic principles for modeling and evaluating the trust relation.

4 Modeling Trust in Web Services

In this section, we analyze what factors influence the degree of trust between consumers and providers of Web services, and make use of the Cloud Model to represent computable factors in order to express the subjective uncertainty and dynamism of trust.

4.1 Trust Model in Web Service

Modeling trust attempts to evaluate trust relations among parties over the Internet from subjective trust relations in real society[22]. However its complexity relates to multiple measurement methods and various views on trust[11]. Considering all factors in one trust model is a difficult and impossible task. The trust model of this paper is not intended to define a perfect view of trust. Rather, we intend to provide some important and useful notations which can help to understand the trust relation in Web services and provide a basis for trust representation and evaluation in this context.

4.1.1 Context of Trust

Different trust models have different perceptions for context. Most trust models have an action component to trust, and note that there must be some purpose of trusters. The context of trust may be expressed as $CM = \langle R, G, P, A \rangle$.

In the context of trust denoted as CM, R and P express two sets of service requestors and providers respectively. We represent any particular requestor and provider by lower-case letters r and p, which belong to sets R and P. G is the goal set of requestors. If one requestor has to trust some service providers, he must have some goals to achieve which depend on some actions implemented by services. For example, someone may want to get today's weather report, or validate a credit card number before a transaction. In these cases, both weather report and validating credit card number are all regarded as goals of requestors and can be notated as g_1 and g_2 which belong to set G. At the same time, satisfaction of these goals requires suitable actions from a Web service. We represent required actions as lower-case letter a, where a is one element of set A in CM.

Given context of trust with CM, assume requestor r_1 whose goals are $G_{r1} = \{g_1, g_2, \ldots, g_n\}$. For each $g_i \in G_{r1}$, g_i can be achieved by certain action a_i of Web service provided by provider p_i. Notice that it is possible that there are different services provided by the same provider. That means the notation $p_i = p_j$ $(i \neq j)$ is allowed. According to these notations, we introduce trust-decision making point (hereafter TDMP) notated as $TDMP_i(r_i(g_i), p_i(a_i))$. TDMP is a situation in which g_i of r_i depends on the a_i of p_i, and the trust value of r_i in p_i should be computed.

TDMP provides one means to understand the trust relation in the context of Web services. The trust value of the relation needs some computable factors. In the

following subsections, we explain some terms which are essential components of our trust model for computing the trust degree.

4.1.2 Reputation

Chang[23] defines reputation as recommendation opinions of a third party in response to the reputation query for the trustworthiness of the trusted entity. In other literature, reputation is regarded as belief based on indirect experience, while trust is belief derived from direct experiences[24]. In accordance with real situations of service-oriented computing, we think that reputation can come from both direct and indirect experiences. For example, in the Web site of Web Service List (www.webservicelist.com), all requestors can rate the reputation of services from one star to ten stars based on their subjective experience. Therefore the definition of reputation used in this paper is as follows.

Definition 1 (Reputation). *Reputation reflects the opinions given by users about Web services, comes from the direct experience of people, but can serve as a recommendation for others.*

It is important to note that it is unreasonable to regard reputation as one kind of belief. For example, because requestors will face less future risk in interaction, they will likely trust providers despite their bad reputation. Therefore, reputation is one influencing factor to affect the belief of requestors, and used to evaluate the trust degree of requestors in providers. For a certain $TDMP_i(r_i(g_i), p_i(a_i))$, the reputation of action of service can be notated as $Rep(a_i)$.

4.1.3 Trustworthiness

In this paper, trustworthiness is defined as follows.

Definition 2 (Trustworthiness). *Given a trust context, trustworthiness can be used to measure the ability of Web services to abide by the agreement of service quality.*

One criterion to estimate trustworthiness is the mutual agreement between requestors and providers, such as Service Level Agreement (SLA). SLA is a contract agreed upon before real invocation of services and expresses the expectation of requestors and promises of providers. SLA consists of a set of parameters, such as response time, accessibility, availability. We call each SLA parameter as one kind of capability of a Web service to satisfy the agreement, where all capabilities can express the trustworthiness. The difference in the actual and projected values of SLA parameters can serve as an indicator for measuring one kind of capability. Some SLA parameters could be negative, i.e., the higher the value, the lower the quality. This includes some parameters such as response time. Others are positive, i.e., the higher the value, the higher the quality. This includes accessibility, availability and so on. In order to handle the two cases uniformly, we design negative and positive parameters respectively:

$$Cap^n_{kj} = v^e_j - v^a_j \tag{1}$$

$$Cap^p_{kj} = v^a_j - v^e_j. \tag{2}$$

Cap^n_{kj} and Cap^p_{kj} denote the k-th negative and positive capability of action a_i in given $TDMP_i(r_i(g_i), p_i(a_i))$ during the j-th invocation of service. v^e_j and v^a_j are the expected and actual values of the j-th invocation of an SLA parameter. Through (1) and (2), different classes of SLA parameters hold the same monotony that is the higher value and the higher capability of services. The values of capability could be scaled according to (3) into the range [0, 1]. Cap_{kj} in (3) is the result of scaling. c_{kj} is the value of Cap^n_{kj} or Cap^p_{kj}, $c_{\min}$ and $c_{\max}$ are their maximum and minimal values.

$$Cap_{kj} = \frac{c_{kj} - c_{\min}}{c_{\max} - c_{\min}}. \tag{3}$$

The overall trustworthiness of action a_i, notated as $TW(a_i)$, can be calculated relying on Multiple Criteria Decision Making theory. That means the $TW(a_i)$ can be expressed as the weighted arithmetic average of all capabilities.

4.1.4 Risk

Risk is one important nature of trust and taken into account in many trust models. Daniel[25] regards risk as a function of trust variables, and does not explicitly distinguish risk from trust. In our opinion, trust and risk are different concepts. The former tends to help build confidence for service requestors based on previous interactions and behavior of services. The latter is usually used to represent potential loss during future interactions, and can be viewed as one factor of trust-decision making. But surprisingly, some research for trust in the environment of Web services does not consider risk as an independent factor.

Risk in the work of Marsh[26] involves a weighing of the costs and benefits to determine whether it is worth risking the costs in order to obtain the benefits. However, it is difficult to measure the costs and benefits of service requestors. For example, costs of interactions are not only related to the price of service. Sometimes immaterial elements such as psychological and emotional sense will affect people's perception about risk. Therefore, we borrow an explanation of risk from the field of economics. A. H. Mowbray[27] regarded risk as uncertainty, and C. A. Williams[28] defined it as change of future results under given conditions.

We define risk in trust-decision making as follows:

Definition 3 (Risk). *Risk represents the potential and possible change of reputation and trustworthiness in future interactions between consumers and Web services.*

Because many fuzzy and random factors will affect future risk, we cannot give explicit metrics of risk. Rather, we give an estimate or approximate value through the historical change of reputation and trustworthiness in order to predict future risk. Therefore, we notate risk with two components: $Risk(Rep_{a_i})$ and $Risk(TW_{a_i})$.

4.2 Trust Representation

Trust can be represented as qualitative labels (discrete numbers), or as a quantitative continuous variable over a certain numerical range. In some work[4,7,15], both discrete and continuous numbers are regarded as statistical samples, and trust level is represented by probability metrics. However, trust is not an objective property of certain trustees, but a subjective perceptive behavior of trusters to judge the reputation, trustworthiness, and risk. This perception has obvious subjective uncertainty including randomness and fuzziness. Probability does not take the observers into account, merely their observations[17]. Thus, probability metrics may capture the randomness of trust factor, but not be suitable to express fuzziness of subjective cognition.

Human thought is usually not expressed in terms of mathematics. Rather, natural languages are the carrier of human thought for concepts and linguistic values. People are often able to rate trust better in the form of discrete verbal statements, rather than continuous measures[29]. Verbal statements must introduce subjective fuzziness. For example, when we say a service requestor *trusts* or *greatly trusts* a provider, we cannot ascertain whether 0.85, 0.9, or 0.95 accurately represents these trust degrees. Fuzzy set theory[30-31], which bridges numerical values to concepts, may be one method to express the fuzziness. But fuzzy sets use one fixed number to represent the fuzzy phenomenon of subjective perception. The membership function is a precise description approach of fuzziness, and does not take randomness into account[32].

Generally, to represent trust, it is always difficult to objectively distinguish randomness and fuzziness during the subjective perception process. Because of that, rationality of trust representation is essential to the modeling and measurement of trust. In fact, randomness and fuzziness are the two important features of cognitive uncertainty. The main difficulty of trust representation is how to model randomness and fuzziness of perception. In this paper, we attempt to adapt Cloud Model in the field of artificial intelligence with uncertainty to represent computable factors of trust relation in order to rationally express the subjective uncertainty of trust. The Cloud Model proposed by De-Yi Li[32] can uniformly express randomness and fuzziness in the trust relation based on random mathematic and fuzzy set theory, and already has been applied in related areas of trust such as subjective trust modeling and evaluation[33-34].

4.2.1 Basic Knowledge About Cloud Model

The Cloud Model can show the uncertain mechanism during the transformation between qualitative concepts and quantitative values. This characteristic of the Cloud Model makes it suitable to express the subjective uncertainty during the perception of trust degree. Formally, a cloud can be defined as follows.

Definition 4 (Cloud and Cloud Drops[32]). *Let U be a universal set described by precise numbers, and C be the qualitative concept related to U. If there is a number $x \in U$, which randomly realizes the concept C, and the certainty degree of x for C, i.e., $\mu(x) \in [0,1]$, is a random value with stabilization tendency*

$$\mu : U \to [0,1] \quad \forall x \in U \ x \to \mu(x).$$

Then the distribution of x on U is defined as a cloud, and every x is defined as a cloud drop.

According to Definition 4, the random realization is the realization in terms of probability. The certainty degree of x is the membership degree in the fuzzy set theory with the probability distribution. So we can see that certainty degree is also a random variable, unlike membership functions of fuzzy set whose membership degree is a fixed number.

The Cloud Model uses the expected value *Ex*, the entropy *En*, and the hyper-entropy *He* to represent the overall property of a subjective concept. *Ex*, *En*, and *He* are called the numerical characteristics of a cloud. *Ex* is the mathematical expectation of cloud drops distributed in the universal set and is most representative of the qualitative concept. *En* is the uncertainty measurement of the qualitative concept which is determined by both the randomness and fuzziness of the concept. *He* is the uncertainty measurement of the *En*, which is determined by both the randomness and fuzziness of *En*. These numerical characteristics can be generated through backward generators and arithmetic[32].

Definition 5 (One-Dimensional Normal Form Cloud[32]). *Let U be a universal set described by precise numbers, and C be the qualitative concept related to U. If there is a number $x \in U$, which randomly realizes the concept C, and x satisfies $x \sim N(Ex, En'^2)$, where $En' \sim N(En, He^2)$, and the certainty degree of x on C*

is:

$$\mu = e^{\frac{(x-Ex)^2}{2(En')^2}}. \quad (4)$$

Then the distribution of x on U is a one-dimensional normal cloud.

The normal distribution is one of the most commonly distributions in probability theory. The one-dimensional normal cloud is a model developed based on both the normal distribution and the bell-shaped membership function[32]. [35] analyzes and discusses the universe of a normal form cloud in applying uncertainty representation of knowledge. Fig.1 shows a graphical representation of reputation based on the Cloud Model whose numerical characteristics are $Ex = 0.5$, $En = 0.1$, and $He = 0.01$.

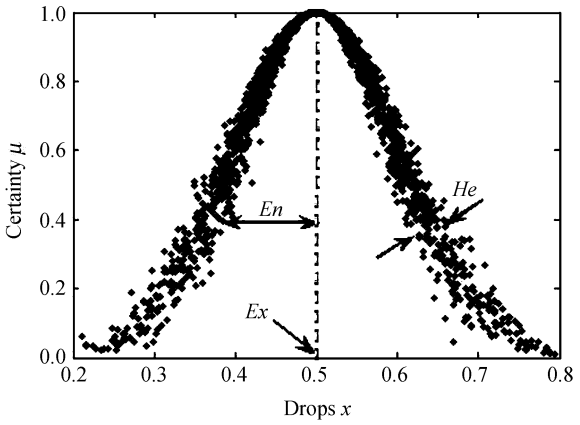


Fig.1. Representation of reputation based on Cloud Model.

The X-axis is the numerical universal set U of reputation ranged in [0, 1]. The Y-axis represents the certainty degree μ of reputation drops belonging to some concept of reputation such as *highly trust*, *greatly trust*. μ expresses the perception fuzziness of reputation. This means that values in U have different certainty degrees to belong to given concepts. Besides, *He* affects the shape of the cloud providing breadth. Unlike a membership degree of a fuzzy set, μ is a random variable following a normal distribution rather than a fixed number. The probability property of μ can express the subjective perception randomness of reputation. Therefore, we may say that the subjective uncertainty can be expressed through numerical characteristics of the Cloud Model. We use one-dimensional normal cloud to represent computable factors of the trust relation, such as reputation, trustworthiness, and risk.

4.2.2 Cloud-Based Trust Representation

From the discussion above, we can obtain the features and key factors of trust from the Trust Model, and then we try to make use of Cloud Model to describe the important factors of trust. We think Cloud Model is a tool used to represent the factors of trust. Our idea is that first we get trust factors from the trust model we have made and then we express these factors taking the advantage of Cloud Model. Using the key features of Cloud Model like *Ex*, *En*, *He*, we can express uncertainty of trust more rationally.

Subjective trust may be regarded as a kind of knowledge based on reality that mostly depends on the perception of observers. Therefore, the trust model and evaluation approach should be as people-oriented as possible and capture the property of subjective perception. We hereby define the reputation cloud, trustworthiness cloud and risk cloud, to express the computable factors of trust.

Definition 6. *Let $RCD = [0, 1]$ be a universal set of discourse, and C be a qualitative concept which represents the reputation of Web Services. The certainty degree of x in RCD to the concept C, i.e., $\mu(x) \in [0, 1]$ is a random variable with stable tendency.*

$$\mu : RCD \to [0, 1] \quad \forall x \in RCD : x \to \mu(x).$$

Then the distribution of x in RCD is called reputation cloud $RepC(x)$ and every x is called reputation cloud drops. The RepC shows the reputation of services, and mainly depends on end-user's experiences, and reflects the satisfaction degree of the end-user. Here we assume rating represents the reputation and can be scaled within the interval $[0, 1]$. If the rating is close to 0, this means lower reputation. Similarly, a rating close to 1 expresses higher reputation.

Definition 7. *Let $TWCD = [0, 1]$ be the universal set of discourse, and C be a qualitative concept which represents a capability of a Web service. Any x in $TWCD$ can be calculated by (1), (2), and (3) in Subsection 3.2.3. The certainty degree of x in $TWCD$ to the concept C, i.e., $\mu(x) \in [0, 1]$ is a random variable with stable tendency.*

$$\mu : TWCD \to [0, 1] \; \forall x \in TWCD : x \to \mu(x).$$

Then the distribution of x on $TWCD$ is defined as $TWC(x)$, and every x is called trustworthiness cloud drops. The value of trustworthiness cloud drops could be positive or negative, which expresses whether the value of an SLA parameter greater or less than the expected value. The ideal situation is the value of drops equal zero. When x is positive or negative, it indicates positive or negative compliance with the SLA.

Definition 8. *Let $RiskCD = [0, 1]$ be the universal set of discourse, and C be a qualitative concept which represents risk requestors face in future interaction. Each x in $RiskCD$ expresses the change state of reputation or capability of services in adjacent time*

slots. For any x in RiskCD, the certainty degree of x to the concept C, i.e., $\mu(x) \in [0,1]$ is a random value with stable tendency.

$$\mu : RiskCD \to [0,1]\ \forall x \in RiskCD : x \to \mu(x).$$

Then the distribution of x on RiskCD is defined as $RiskC(x)$, and every x is called risk cloud drops. The change rate of $RiskC(x)$ can be computed by (5). *R_{rate} is the change rate of reputation or capability, where x_{i+1} and x_i are two adjacent drops.*

$$R_{\text{rate}} = x_{i+1} - x_i. \tag{5}$$

In Definition 8, risk of trust-decision in the Web services environment is represented as the potential and possible change of reputation and trustworthiness in future interactions. Let R_l and R_u be lower and upper bounds on change rate of drop values of $RiskC(x)$. Because the range of both reputation and trustworthiness are [0, 1], R_l and R_u are -1 and 1 respectively. So we can use (6) to scale drops of risk into [0, 1].

$$Drop_{\text{risk}} = \frac{R_{\text{rate}} - R_l}{R_u - R_l}. \tag{6}$$

Note that the aim of this paper is to evaluate the trust degree by means of the numerical characteristics of the Cloud Model. Therefore, it is not necessary to define some trust concept for $RepC(x)$, $TWC(x)$, and $RiskC(x)$ to express the trust levels explicitly. As mentioned above, the numerical characteristics of the Cloud Model are the overall quantitative property of the qualitative concept. The subjective uncertainty of the trust relation can be expressed by means of numerical characteristics of a cloud. *Ex*, *En*, and *He* of a cloud allow us to quantify randomness and fuzziness of reputation, trustworthiness, and risk. Because *He* is a measure of the uncertainty of *En*, we can only use *Ex* and *He* to quantify the uncertainty, and call $\langle Ex, He\rangle$ the character vectors of trust factors. In addition, it is necessary to assign numerical characteristics with rational and significant meanings. In this paper, we take *Ex* as a typical value and average level of computable factors. In addition, we use *He* as a metric of measuring subjective uncertainty which reflects decentralization degrees from the average level, namely, stability of reputation, trustworthiness, and risk. For example, higher *Ex* of reputation means a higher reputation and vice versa. If *He* is small, then satisfiability of reputation is good and vice versa. In Section 4, we will explain how to compute the trust degree of requestors in providers on the basis of cloud-based trust representation.

Based the above discussion, we can get the superiority and feature of our method using the Cloud Model. According to our research, traditional method of modeling trust only consider randomness or fuzziness unilaterally, but randomness and fuzziness are the most two important features of cognitive uncertainty of trust. So if we consider only one simply, we will not represent uncertainty of trust completely. The Cloud Model is widely used to express randomness, fuzziness and relationship between them on the basis of random mathematics and fuzzy mathematics, so we make use of the Cloud Model to represent the important factors of trust. We will express cognitive uncertainty of trust well.

4.2.3 Time-Related Backward Cloud Generator

Trust relation varies with time, and is closely related to historical interaction and time. Therefore, evaluation data of the trust relation is only valid for a limited time period. This means the further away the current evaluation time from the trust decision, the lower the validity of the data. In order to correctly reflect the dynamism of trust, we extend the backward cloud generation algorithm without certainty degree in [32], and design a weighted backward cloud generation algorithm. Based on the distance from historical time to the current trust decision time, this algorithm assigns different weights to drop values of *RepC*, *TWC*, and *RiskC*. The basic weighting rule of this algorithm is, the newer the drop value is, the bigger its weight and vice versa. We first explain the time model and basic rules for weighting.

Using the time model $M = \langle X, t_c, t_b, T\rangle$, where

1) $X = \{x_1, x_2, \ldots, x_n\}$ is the full set of cloud drops of service. For any x_i, $Time(x_i)$ denotes the time slot, and is newer than t_b.

2) t_c denotes the current time of trust decision and serves as time origin. t_b denotes certain time of forward direction of time axis, and serves as time threshold for judging effectiveness.

3) $T = \{t_1, t_2, \ldots, t_{m-1}\}$ is an ordered set composed of $m-1$ time values between t_c and t_b. For any t_i, $d_i = |t_i - t_c|$ is called time distance from t_i to t_c, and satisfies the following constraint.

a) $\forall d_i\ (1 \leqslant i \leqslant m-1) \to d_i \leqslant |t_c - t_b|$;

b) $\forall d_i, d_j\ (1 \leqslant i < j \leqslant m-1) \to d_i < d_j$.

The set T separates time interval between t_c and t_b into m sub-periods called temporal windows and marked as W_t. T further separates X into m subsets, and there is strict time sequence in $X_{t_1}, X_{t_2}, \ldots, X_{t_m}$. There is an equivalent weight of effectiveness for cloud drops whose time value is in the same temporal window. For any subset X_{t_i} $(1 \leqslant i \leqslant m)$ of X, we can assign a weight w_{t_i}, which denotes the degree of influence from data in X_{t_i} to that of overall results of the trust relation. Weights should satisfy the constraints of

(7) and (8).

$$\forall x_i \in X_{t_K}, \quad x_j \in X_{t_l} \quad (1 \leqslant k < l \leqslant m) \rightarrow (w_{t_k} < w_{t_l}) \tag{7}$$

$$\sum_{i=1}^{m} w_{t_i} = 1. \tag{8}$$

Because the effectiveness of time relates to the time preference of people, we adopt some analysis methods of the inconsistent time preference theory from behavioral economics and Economics Psychology science[36] to design a weight assignment function expressed by (9).

$$w_{t_i} = \frac{w_{t_m}}{(1 + \alpha \times (m - i))^{\gamma/\alpha}} \quad (1 \leqslant i \leqslant m - 1). \tag{9}$$

W_{t_m} is the temporal window closest to the current time of a trust-decision. The value of m indicates the number of temporal windows. The weights of a temporal window older than W_{tm} will decrease at a different ratio. The decrement speed of weights can be adjusted through parameters α and γ both greater than zero. Larger γ and smaller α cause the decrement ratio of weights to become bigger, and the weights of older temporal window become smaller.

After calculating the weights, we can apply the weighted backward generation cloud algorithm proposed in [34] in calculating *Ex*, *En*, and *He*.

5 Trust Evaluation Approach

According to the definitions of *Ex* and *He* with respect to trust clouds, Web services with higher *Ex* and lower *He* can be regarded as the most suitable candidates. To assist requestors with trust-decision making, it is necessary to provide an approach to combine *Ex* with *He* to obtain quantitative results indicating the most suitable Web services that can be selected. To do so, we first compute the scores of *RepC*, *TWC*, and *RiskC* by the means of the vector $\langle Ex, He \rangle$. Then the final trust degree can be calculated based on these scores.

5.1 Scoring Computable Factors of Trust Relation

To calculate quantitatively, we consider *Ex* as the master value and *He* the slave value. The score of computable factors is a function of *Ex* and *He*, and increases with *Ex* and decreases with *He*. The function of *Ex* and *He* is shown by (10).

$$S = \frac{Ex \times e^{-He} + bEx}{b + 1}, \tag{10}$$

where parameter b is an impact factor to adjust the computing result of S, and is used to adjust the precision of the score. The smaller the inverse of parameter b, the finer the difference among scores that can be distinguished. We can prove the validity of (10) as follows.

Suppose S_a and S_b are scores of A and B. $S_a = \frac{Ex_a \times e^{-He_a} + bEx_a}{b+1}$, $S_b = \frac{Ex_b \times e^{-He_b} + bEx_b}{b+1}$, and $Ex_a > Ex_b$. If $S_a = S_b$ then:

$$Ex_a \times e^{-He_a} + bEx_a = Ex_b \times e^{-He_b} + bEx_b$$

and

$$\frac{Ex_b}{Ex_a} = \frac{e^{-He_a} + b}{e^{-He_b} + b}.$$

Because $e > 1$ and $He > 0$, so $0 < e^{-He_a} < 1$ and $0 < e^{-He_b} < 1$, this leads to $1 < \frac{Ex_b}{Ex_a} < \frac{b+1}{b}$. From the initial assumptions and step by step sequence of deduction, we can conclude that if $S_a = S_b$ then Ex_a approximately equals Ex_b.

Similarly, let the ratio of Ex_b and Ex_a be equal to α, then $\alpha e^{-He_b} + \alpha b = e^{-He_a} + b$.

Applying natural logarithmic and equation transformation to (8), we can get a new equation $He_a - He_b = Ln(\frac{1}{\alpha^2})$. Since α is close to 1, He_a is approximately equivalent to He_b.

5.2 Scoring Trust Degree

Given a trust-decision making point $TDMP_i(r_i(g_i), p_i(a_i))$, we use $Rep(a_i)$, $TW(a_i)$, $Risk(Rep_{a_i})$ and $Risk(TW_{a_i})$ to express the scores of reputation, trustworthiness, and risk, computed by (10), in the interaction between service requestors and providers. Among these scores, $TW(a_i)$ and $Risk(TW_{a_i})$ are the weighted arithmetic average of all capabilities expressed by the Cloud Model.

Through reputation, trustworthiness and risk, the trust degree of requestors in providers can be estimated. In general, the trust degree increases with reputation and trustworthiness. Risk has a negative effect on the trust-decision of requestors. But requestors have different risk aversion levels. Some of them are willing to face risk in order to make a profit, but others try to avoid taking risk. Accordingly, we design an appropriate approach to compute the trust score to represent the trust degree of requestors in providers. There may be multiple options for computing the trust score on the basis of $Rep(a_i)$, $TW(a_i)$, $Risk(Rep_{a_i})$ and $Risk(TW_{a_i})$, but we think each available function should at least satisfy the following constraints.

1) It increases or decreases with $Rep(a_i)$ and $TW(a_i)$ when the other variable is fixed.

2) It is a decreasing function of $Risk(Rep_{a_i})$ and $Risk(TW_{a_i})$.

3) When $Rep(a_i)$ and $TW(a_i)$ are equal to 1, and $Risk(Rep_{a_i})$ and $Risk(TW_{a_i})$ are equal to zero, the

trust degree reaches its maximal value, and is equal to 1.

4) In contrast to 3), when $Rep(a_i)$ and $TW(a_i)$ are equal to zero, and $Risk(Rep_{a_i})$ and $Risk(TW_{a_i})$ are equal to 1, the trust degree meets its minimal value, and is equal to zero.

5) Some parameters could be used so that the trust score function can be adjusted to control the effect of risk on trust-decision making.

We propose (11) to calculate the trust score which satisfies the constraints above.

$$TS = \frac{Rep + Com - e^{k \times Risk(Rep)} - e^{k \times Risk(Com)}}{2 \times e^k} + 1, \tag{11}$$

where TS is the trust score. Parameter k is greater than zero and used to control the effect of risk on trust-decision making. The effect of risk can be analyzed through derivatives of *Rep*, *TW*, and *Risk* of (11). The effects of different ranges on the value of k are concluded as follows.

1) If $k \geqslant 1$, then the effect of risk on the trust-decision making must be greater than that of reputation and trustworthiness.

2) If $0 \leqslant k \leqslant k_t$, and k_t satisfy $k_t \times e^{k_t} = 1 (k_t < 1)$, then the effect of risk on the trust-decision making must be less than that of reputation and trustworthiness.

3) If $k_t \leqslant k < 1$, then the effect of risk on the trust-decision making is determined by the actual numerical value of $Risk(Rep)$ and $Risk(TW)$.

6 Experiment and Discussion

The primary goal of our experiment is to show how to apply our approach in evaluating the scores of computable factors of the trust relation, and the scores of trust degree of requestors in providers. At the same time, the characteristic and validity of the approach will be discussed.

Firstly, we analyze the effect of parameter b in (10) on the scores of computable factors. Three groups of values of reputation of virtual Web services, represented by numerical characteristics of cloud *Ex* and *He*, are listed in Table 1.

Table 1. *Ex* and *He* of Reputations

Web Services	*Ex*	*He*
A	0.4	0.01
B	0.4	0.03
C	0.4	0.09

According to the values of *Ex* and *He* in Table 1, three curves of reputation scores can be shown in Fig.2. From Fig.2, the reputation score tends to be constant

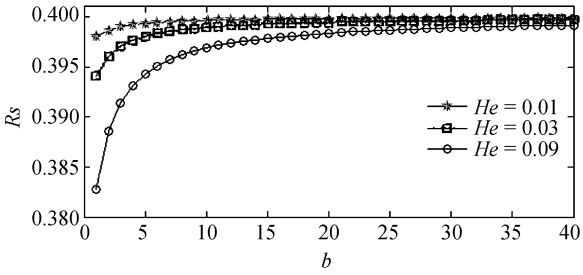


Fig.2. Reputation score of Web services *A*, *B*, and *C*.

with increment of parameter b. The trend can be analyzed quantitatively through calculating the derivative of (10). Given the values of *Ex* and *He*, the derivative of parameter b is shown as (12).

$$\frac{\mathrm{d}S}{\mathrm{d}b} = \frac{Ex \times (1 - e^{-He})}{(b+1)^2}. \tag{12}$$

Because the value of numerator is a constant, the $\frac{\mathrm{d}S}{\mathrm{d}b}$ is monotone decreasing function of variable b. If b is big enough (8 for example), $\frac{\mathrm{d}S}{\mathrm{d}b}$ gradually tends to be zero. That means the reputation scores became a constant when b is greater than a certain threshold. Therefore, the value of b will be assigned with 8 in the next experiments.

The second experiment measures trust degree on the basis of actual interaction data of Web services. The experiment includes a series of simulations based on real data from some selected Web services. We selected eight Web services from www.webservicelist.com shown in Table 2.

Table 2. The List of Selected Web Services

Name	Rating	Summary
Break Even Point	9	A break-even point defines when an investment generates a positive return.
Send Fax	9	Send fax free to any country.
Codebar	10	Code39 bar code BARCODE generator for CODE39.
Text to Braille	6	Convert text to Braille.
Global Weather	9	Retrieve current weather and upcoming weather conditions.
Stock Quote 092501	6	Stock quote Web Service, by company symbol.
Stock Quote 092502	7	Get stock quote for a company symbol.
Vaildate Email Address	10	Validate any email address against the e-mail mail server.

The value of rating in Table 2 gained from www.webservicelist.com represents the average reputation of Web services. Because we cannot get the original data, we generate 2000 simulative samples

of reputation using the average reputations. After that, we design five time windows and create *Ex*, *En*, *He* of different services using time-related backward cloud algorithm.

For explaining the advantages of cloud model to represent trust, we choose Service 4 and Service 6 for comparison as below.

In Fig.3, we can see the representation of trust using cloud model with more semantics than average reputation. For example, all sample data of reputation form a concept whose typical value is represented by *Ex* of cloud. Different data of reputation belong to the concept with different certainty degrees, and these certainty degrees are not fixed values but random ones. These semantics can preferably reflect fuzziness and randomness of trust. Besides, the average of Service 4 and Service 6 is equal shown in Table 2, but their *Ex*s and *He*s are different in Fig.3. From Fig.3, we can distinguish them easily, and make a fine-grained distinction of Web Services using the cloud model.

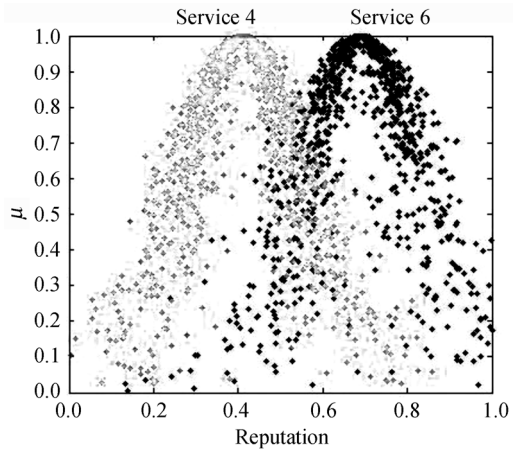


Fig.3. Clouds of Services 4 and 6.

Fig.4 compares evaluation results of reputation which are computed by averaging reputation and scoring method based on (10). We use two different groups of values of α and γ in (9), and create two weights vectors $\boldsymbol{w}_1$ = [0.1218, 0.1382, 0.1635, 0.2110, 0.3655], $\boldsymbol{w}_2$ = [0.0273, 0.0427, 0.0759, 0.1708, 0.6832]. From Fig.4, using our measurement method of reputation, we can distinguish services' reputations whose average of reputation are the same. Because the time window close to current time of trust decision gets a bigger weight, the difference of reputation's result using $\boldsymbol{w}_2$ is more obvious than that using $\boldsymbol{w}_1$.

We choose response time, availability and success rate as SLA parameters and compute their values through invoking every service 2000 times. The computing equations of these parameters are borrowed from [37], and are shown in Table 3.

We divide the 2000 data points of each computable factor into five temporal windows, and use $\boldsymbol{w}_2$ as the weights vector of each temporal window. Here we choose response time as a comparative example to compare our method with the method based on Verity, Fig.5 shows the comparison.

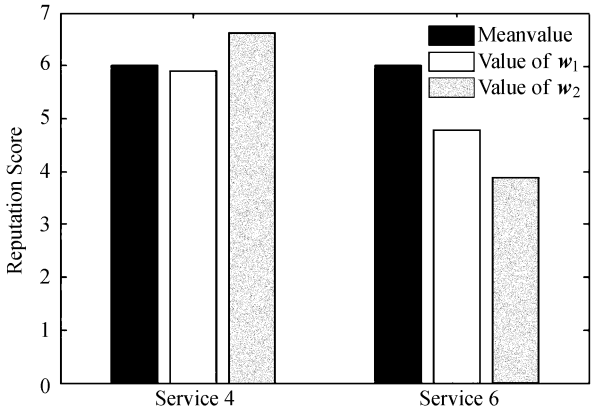


Fig.4. Comparison of Web services' reputation.

Table 3. Equations of Computing SLA Parameters

Name	Formula
Response Time	$T = t_{\text{Response}} - t_{\text{Request}}$
Availability	$A = 1 - \frac{downtime}{uptime}$
Success Execute Rate	$S = 1 - \frac{Failed\ \ Request}{Total\ \ Request}$

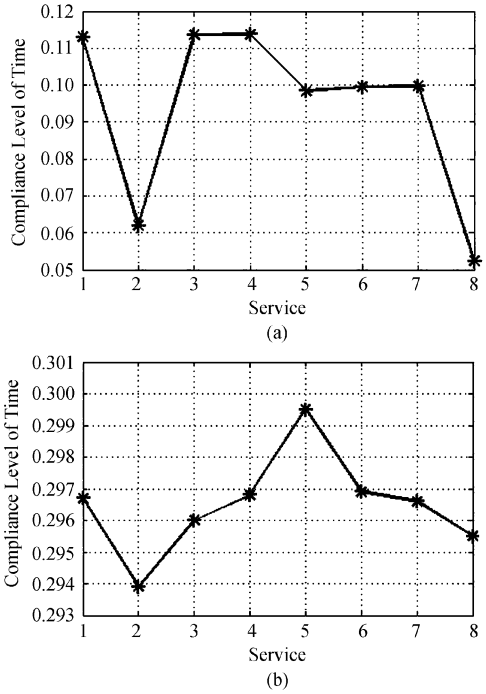


Fig.5. Comparison of response time.

Fig.5(a) shows the evaluation result using Verity, and Fig.5(b) shows the evaluation result using the trustworthiness cloud and (10). In Fig.5, the two curves have different trends. For example, the value of the fifth service is less than that of the fourth in Fig.5(a), but opposite in Fig.5(b). If reversing values of $\boldsymbol{w}_2$, we can get a new weight vector $\boldsymbol{w}$ = [0.6832, 0.1708, 0.0759, 0.0427, 0.0273]. Using $\boldsymbol{w}$, the values of Fig.5(b) will change as shown in Fig.6.

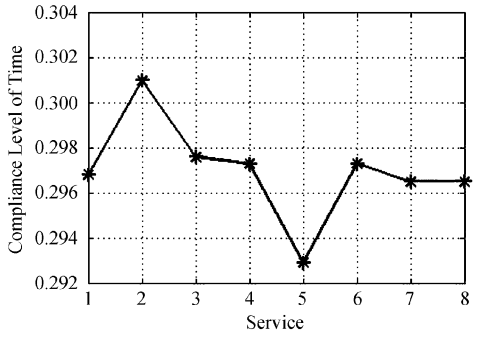


Fig.6. SLA excursion of response time of $\boldsymbol{w}$.

From Fig.6, the value of the fifth service is less than that of the fourth. Therefore, we think the reason for the difference between Figs. 5(a) and 5(b) is that the method based on Verity does not consider the impact of time on trust.

Through comparison of existing methods, using *Ex* and *He* of the Cloud Model by (10), we can see that the evaluation of computable factors can effectively reflect dynamicity of trust decision. After achieving the scores of all computable factors, the final trust degree of each Web service can be calculated by (11) and the results are shown in Fig.7.

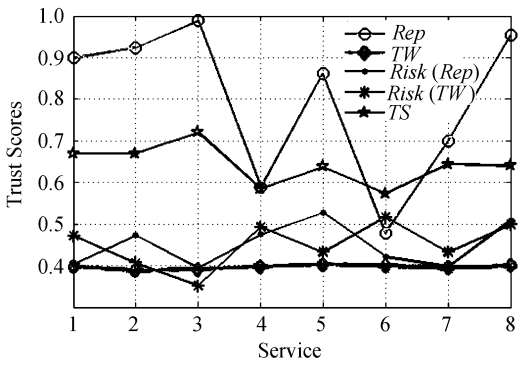


Fig.7. Result of evaluating trust.

In Fig.7, the x-coordinates represent the eight instances of Web services, while the y-coordinates are the measurement results of *Rep*, *TW*, *Risk*(*Rep*), *Risk*(*TW*) and trust scores (*TS*). From Fig.7, different trust factors have different trend curves. For example, reputations of Services 2, 3, 8 are higher than others; trustworthiness of Service 5 is better than others; *Risk*(*Rep*) and *Risk*(*Com*) of Services 1, 4, 8 are relatively higher. Therefore it is not reasonable to decide the trust degree of Web services independently according to each factor. The final trust degree of truster in Web services depends on the values of reputation, dependability, and risk as a whole. From the curve of *TS*, Service 3 has a higher reputation, moderate trustworthiness and lower risk. So taking all factors into consideration the third service is better than the others.

To sum up, through analyzing the results of experiment, our method can reasonably represent the uncertainty and dynamicity of trust, and make a more comprehensive analysis of the trust degree of Web services according to reputation, dependability and risk.

7 Conclusion

Selecting Web services from the viewpoint of trust has been a research emphasis in the context of Web services. In this paper, we modeled the trust relation and evaluated trust degree from perspectives of both characteristics of trust and domain characteristics of service-oriented computing. In our trust model, the reputation, trustworthiness, and risk compose the key computable factors supporting for trust-decision. To deal with the subjective uncertainty of trust, we take advantage of Cloud Model to define the computable factors. At the same time, we present a new time-related backward cloud generation algorithm to generate the numerical characteristics of Cloud Model to express the dynamism of subjective belief of requestors. These numerical characteristics can rationally express the randomness and fuzziness of trust. According to the numerical characteristics, we propose some quantitative equations to compute the scores of computable factors and trust degrees. The final trust-decision can be achieved through scores of the trust degree of services.

However, our work is still preliminary and can be improved in the following aspects.

1) The weighting method of temporal windows can be further improved to borrow some theory such as Recency Effect theory from the discipline of psychology.

2) There may be malicious behavior during the rating of reputation by some requestors. Some methods may be applied in our future work to identify and avoid these behaviors.

3) A trust-decision-making system will be developed to integrate the trust model and evaluation approach in the future.

References

[1] Curbera F *et al.* Unraveling the Web Services Web: An

introduction to SOAP, WSDL, and UDDI. *IEEE Internet Computing*, 2002, 6(2): 86-93.

[2] Menasce D A. QoS issues in Web Services. *IEEE Internet Computing*, 2002, 6(6): 72-75.

[3] Bouch A, Kuchinsky A, Bhatti N. Quality is in the eye of the beholder: Meeting users' requirements for Internet quality of service. In *Proc. the SIGCHI Conference on Human Factors in Computing Systems*, The Hague, The Netherlands, Apr. 1-6, 2000, pp.297-304.

[4] Majithia S, Ali A S, Rana O F, Walker D W. Reputation-based semantic service discovery. In *Proc. the 13th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises* (*WET ICE 2004*), Modena, Italy, Jun. 14-16, 2004, pp.297-302.

[5] Xu Z, Martin P, Powley W, Zulkemine F. Reputation-enhanced QoS-based Web Services discovery. In *Proc. IEEE International Conference on Web Services*, Salt Lake City, USA, July 9-13, 2007, pp.249-256.

[6] Wishart R, Robinson R, Indulska J. SuperstringRep: Reputation-enhanced service discovery. In *Proc. the 28th Australasian Conf. Computer Science*, Newcastle, Australia, Jan./Feb., 2005, Vol.38, pp.49-57.

[7] Zeng L, Benatallah B *et al.* QoS-aware middleware for Web Services composition. *IEEE Transactions on Software Engineering*, 2004, 30(5): 311-327.

[8] Tan Y H, Thoen W. Toward a generic model of trust for electronic commerce. *International Journal of Electronic Commerce*, 2000, 5(2): 61-74.

[9] Elosfson G. Developing trust with intelligent agents: An exploratory study. In *Proc. 1st International Workshop on Trust*, Jul. 15-20, 1998, pp.125-139.

[10] Miquel Montaner, Beatriz Lopez, Josep Lluis *et al.* Opinion-based filtering through trust. In *Proc. the 6th International Workshop on Cooperative Information Agents*, Madrid, Spain, Sept. 18-20, 2002, pp.164-178.

[11] Maximilien E M, Singh M P. Reputation and endorsement for Web services. *ACM SIGecom Exchanges*, 2002, 3(1): 24-31.

[12] Maximilien E M, Singh M P. Conceptual model of Web services reputation. *ACM SIGMOD*, Special Section on Semantic Web and Data Management, 2002, 31(4): 36-41.

[13] Kalepu S, Krishnaswamy S, Loke S W. Verity: A QoS metric for selection Web Services and providers. In *IEEE Proc. the 4th Conference on Web Information Systems Engineering Workshops*, Helsinki, Finland, Dec. 10-12, 2003, pp.131-139.

[14] McKnight D H, Chervany N L. The Meanings of Trust. Technical Report 94-04, Carlson School of Management, University of Minnesota, 1996.

[15] Chang E, Thomson P, Dillon T, Hussain F. The fuzzy and dynamic nature of trust. In *Proc. the 2nd Int. Conf. Trust, Privacy and Security*, Copenhagen, Demark, Aug. 22-26, 2005, pp.161-174.

[16] Tang W, Hu J B, Chen Z. Research on a fuzzy logic-based subjective trust management model. *Computer Research and Development*, 2005, 42(10): 1654-1659.

[17] Abdul-Rahman A, Hailes S. Supporting trust in virtual communities. In *Proc. the Hawaii International Conference on System Sciences*, Maui, Hawaii, Jan. 4-7, 2000, p.6007.

[18] van der Heijden H, Verhagen T, Creemers M. Understanding online purchase intentions: Contributions from technology and trust perspectives. *European Journal of Information Systems*, 2003, 12(1): 41-48.

[19] Josang A. The right type of trust for distributed systems. In *Proc. Workshop on New Security Paradigms*, Lake Arrowhead, USA, Sept. 17-20, 1996, pp.119-131.

[20] Greg Elosfson. Developing trust with intelligent agents: An exploratory study. In *Proc. the 1st International Workshop on Trust*, 1998, pp.125-139.

[21] Montaner M, Lopez B, Lluis J *et al.* Opinion-based filtering through trust. In *Proc. the 6th International Workshop on Cooperative Information Agents*, Madrid, Spain, Sept. 18-20, 2002, pp.164-178.

[22] Koutrouli E, Tsalgatidou A. Reputation-based trust systems for P2P applications: Design issues and comparison framework. In *Proc. TrustBus 2006*, Krakow, Poland, Sept. 4-8, 2006, pp.152-161.

[23] Chang E, Dillon T S, Hussain F K. Trust and reputation relationships in service-oriented environments. In *Proc. the 3th International Conference on Information Technology and Applications, Keynote*, Sydney, Australia, Jul. 4-7, 2005, pp.4-14.

[24] Wang Y, Vassileva J. Trust and reputation model in peer-to-peer networks. In *Proc. the 3rd International Conference on Peer-to-Peer Computing*, Linköping, Sweden, Sept. 1-3, 2003, pp. 150-157.

[25] Manchala D W. E-commerce trust metrics and models. *IEEE Internet Computing*, 2000, 4(2): 36-44.

[26] Marsh S. Formalising trust as a computational concept [Ph.D. Dissertation]. Department of Mathematics and Computer Science, University of Stirling, 1994.

[27] Mowbray A H, Blanchard R H, Williams C A. Insurance. 4th ed, New York: MC Graw Hill, 1995.

[28] Williams C A, Heins R M. Risk Management and Insurance. New York: MC Graw Hill, 1985.

[29] Josang A, Ismail R, Boyd C. A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 2007, 43(2): 618-644.

[30] Zadeh L A. Fuzzy sets. *Information and Control*, 1996, 8: 338-353.

[31] Zadeh L A. Fuzzy sets as a basis for a theory of possibility. *Fuzzy Sets and System*, 1978, 1: 3-28.

[32] Li D Y, Du Y. Artificial Intelligence with Uncertainty. Chapman & Hall/CRC Taylor & Francis Group. 2008.

[33] Meng X, Zhang G, Kang J, Li H, Li D. A new subjective trust model based on cloud model. In *Proc. IEEE International Conference on Networking, Sensing and Control*, Sanya, China, April 5-9, 2008, pp.1125-1130.

[34] Wang S, Zhang L, Ma N, Wang S. An evaluation approach of subjective trust based on cloud model. *Journal of Software Engineering & Applications*, 2008, 1: 44-52.

[35] Li D Y, Liu C Y. The universality of normal cloud model. *Engineering Science*, 2004, 6(8): 28-34.

[36] Loewenstein G, Prelec D. Anomalies in intertemporal choice: Evidence and an interpretation. *The Quarterly Journal of Economics*, 1992, 107(2): 573-597.

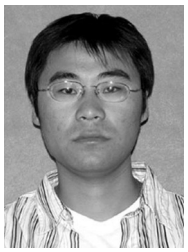
[37] Moser O, Rosenberg F, Dustdar S. Non-intrusive monitoring and service adaptation for WS-BPEL. In *Proc. the 17th International Conference on World Wide Web*, Beijing, China, April 21-25, 2008, pp.815-824.

[38] Jurca R, Faltings B. Towards incentive-compatible reputation management. In *Proc. Int. Workshop Trust, Reputation and Security: Theories and Practice*, Bologna, Italy, Jul. 15, 2002, pp.138-147.

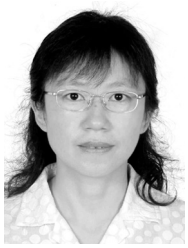
[39] Schillo M, Funk P, Rovatsos M. Using trust for detecting deceptive agents in artificial societies. *Applied Artificial Intelligence*, Special Issue on Trust, Deception, and Fraud in Agent Societies, 2000, pp.825-848.

[40] Huynh T D. Trust and reputation in open multi-agent systems [Ph.D. Dissertation]. Southampton: Electronics and Computer Science, University of Southampton, 2006.

[41] Viljanen L. Towards an ontology of trust. LNCS 3592. Berlin: Springer-Verlag, 2005, pp.175-184.



Shou-Xin Wang is a Ph.D. candidate of School of Computer Science and Engineering, Beihang University (BUAA), and member of China Computer Federation. His research interests focus on software engineering, software architecture, trust modeling and evaluating on Internet.



Li Zhang, Ph.D., professor in School of Computer Science and Engineering, Beihang University (BUAA). She is a committee member of Software Engineering in CCF (China Computer Federation), committee member of education in CCF and committee member of computer application in CSA (Chinese Society of Astronautics). She is interested in software engineering, business process/system modeling, software architecture modeling, visual modeling language and requirement engineering.

Shuai Wang is a Master candidate of School of Computer Science and Engineering, Beihang University. His research interests focus on requirements engineering, trust modeling and evaluating on internet.

Xiang Qiu is a Ph.D. candidate of School of Computer Science and Engineering, Beihang University. His major field of study includes requirement engineering and software architecture.