I. J. Computer Network and Information Security, 2015, 5, 41-50
Published Online April 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2015.05.06

Global Trust: A Trust Model for Cloud Service Selection

Fatima Zohra Filali
Department of Computer Science,
University of Oran1 Ahmed Benbella, Oran, Algeria
Email: filalifz7@gmail.com

Belabbes Yagoubi
Department of Computer Science,
University of Oran1 Ahmed Benbella, Oran, Algeria
Email: byagoubi@gmail.com

Abstract—Cloud Computing refers to network-based service provided by a large number of computers, sharing computing and storage resources. Combined with on-demand provisioning mechanisms and relied on a pay-per-use business model.

The Cloud Computing offers the possibilities to scale rapidly, to store data remotely and to share services in a dynamic environment. However, these benefits can be seen as weaknesses for assuring trust, and providing confidence to the users of service. In this case, some traditional mechanisms to guarantee reliable services are no longer suitable or dynamic enough, and new models need to be developed to fit this paradigm.

This study describes the assessment of the trust in the context of Cloud Computing, proposes a new trust model adapted to Cloud environments, and shows some experiments in regards of the proposed solution.

Index Terms—Trust, Cloud Computing, service selection, Cloud Service Provider, Certain Logic, Direct Trust, Recommended Trust.

I. Introduction

Trust and security remain ones of the greatest challenges in Cloud Computing. Globally, the users do not have enough knowledge about the trust and the reliability of service providers. In Cloud environments, the consumers make complex decisions, requiring trust for several services and various reasons. These decisions require many aspects that cannot be combined in isolation, but all the features impact each other's in a dynamic way.

Therefore, trust-computing systems [10, 17] are used to predict the trust of service providers. Diverse parameters and characteristics are aggregated, filtered and offered to users, to minimize the risks.

In trust research, most existing works use the simple average [18], the Bayesian [32, 36] or the belief models [12, 35] to compute the trust as statistical values. However, the consumers cannot decide how much to rely on the prediction for selecting a reliable provider based only on these probabilistic mechanisms. Another value must be integrated to the accuracy of the feedback.

For assessing Cloud Computing service selection, dynamic based trust mechanisms need to be used, in combination with social mechanisms for providing persistent trust. This way, when information about the performance of the Cloud service is offered, that information can only be trusted.

In this paper, a solution based on CertainLogic [21] and performance values of the service providers is proposed.

The remainder of this paper is organized as follows. Section 2 introduces what is known about trust in computing, and how it affects the design decisions for trust computing. Section 3 describes the contribution of our work and section 4 presents the proposed trust model. Experimental results are presented in Section 5. At last, section 6 concludes the paper.

II. Literature Review

The way in which individuals form beliefs about trustworthiness has been predominantly studied through surveys [3, 5, 26, 27, 30]. The role of trust has been acknowledged in IT domain, and it has been shown that trust is among the main concern in the adoption of Cloud Computing [3, 18, 19].

Although, the trust has been studied in different fields, there is not a global agreement on its definition among researchers. Trust can be defined as "the subjective probability by which a party expects another to perform a given action" [10].

It can also be defined as "the degree to which one entity is eager to rely on something or someone, in a situation with the concept of relative security" [10].

Several studies have been made about the trust, covering various features:

The trust can be represented by its information and feedback sources: it can be direct values from users, or it can be recommendations from others parties. However, these two sides cannot be dissociated for a total overview

of the situation. And must be combined to reach a reliable trust model.

Trust can also be formalized using logical or quantitative approach, the logical approach focuses mainly on the semantic structure of trust and effects of trust. The quantitative approach focuses on the uncertainty of trust, trust quantification, and the models and algorithms of trust computing. Our research have been pointed to quantitative approaches since the trust in Cloud environment is mostly based on social interactions and certainty. Therefore, the semantic of the trust structure is not sufficient to represent realistic interactions as trust represents the confidence of users in using cloud services by mitigating technical and social factors.

In other works, trust has been classified as soft and hard trust [28]. Hard trust represents the trust relationships, which is derived from cryptography based on security mechanisms, and soft trust is based on relationships through social control mechanisms to derive from the localized and external of system behaviour. In our point, these aspects can be used as a set in different contexts.

Finally, to model a trust system two main parties must be included: the trust measures and the mathematical model (metrics) used to aggregate ratings. Trust can be measured using discrete or continuous values. Metrics can be based on a simple summation or an average of ratings [22], fuzzy logic [1, 7, 24, 25, 37], flow-based models [2, 6, 13, 14, 29], probabilistic models such as Bayesian systems [31, 32, 34, 36], or beta probability density [17, 33] and subjective Logic [9, 12, 35].

A lot of research have used these properties to represent compute trust.

In March formalism [16], trust is quantified as three values: -1, 0, +1. Where +1 represents complete trust, -1 represents completely distrust, and 0 represents no trust (un-trust). In these representation Marsh clearly defines un-trust and distrust, but the relation between trust, un-trust and distrust is rather simplified. A trust value is either among trust and un-trust or among un-trust and distrust. This representation doesn't characterize realistic interactions, especially in Cloud environments.

In the most of quantitative trust models [13] the trust rate is represented by a real value in interval [0, 1].

Jøsang [11] described uncertain belief representation by using subjective logic. In subjective logic, an opinion is represented as a triple (b; d; u), with b, d, and u refer to the rates of belief, disbelief, and uncertainty. Their sums is equal to 1 (b+d+u=1). Later, Jøsang [8] applied the subjective logic to represent uncertain trust. The concrete formalization of uncertainty u permits to express and explain degrees of distrust, un-trust and trust; which takes into account incomplete knowledge about a trustee.

Song [24] developed a reputation system based on a fuzzy-logic approach. They used fuzzy-logic's ability to handle uncertainty, fuzziness, and incomplete information adaptively. The proposed system uses fuzzy logic inference rules to calculate local trust scores and to compute global reputation.

The Bayesian reputation [36] computes values of the trust depending on the beta probability density functions. The reputation value is decided by $\alpha+\beta+2$, where α and β are two parameters denoting the number of positive and negative results.

Wang and Singh [35] modelled the reputation as a three dimension belief (b, d, u), representing the probabilities of positive, negative and uncertain outcomes.

Huang [6] proposed a method to aggregate heterogeneous social networks and used the enhanced topology of the trust graph to predict the reputation.

All these models quantify the trust as a probability value based on direct trust or recommended trust. However, they ignore the objective factors for the provided service (QoS).

So, these trust models cannot assess the accuracy of the trust value made by itself. In contrast, the performance value is considered to give a more accurate evaluation in our model, and both the trust and performance values are used for selecting the best service.

In [21] the author proposed a model for the assessment of propositional logic terms under uncertainty. The model have been proved to be compliant with the standard probabilistic evaluation of propositional logic terms and with subjective logic, which provides the justification for the mathematical validity of the model. The proposed approach is more expressive than the standard probabilistic approach, and although it is as expressive as subjective logic. It provides simpler representation since it is based on independent parameters and provides a more intuitive and more expressive graphical representation. Furthermore, it has been shown that the parameters for assessing opinions in Certain-Logic can be derived using multiple approaches and sources. Finally, they have shown the applicability and the benefits of the model in a use case. They have evaluated the trustworthiness of their system in Cloud Computing scenario. This trust measure is adopted, to represent the proposed model.

III. Contribution

In this paper, we introduce a general trust model. This model is based on QoS selection and CertainTrust model, proposed in [21], which extends the Opinion model. The main contributions of our work are as follows:

- Selecting a Cloud provider based on different sources: direct trust, user feedback, QoS parameters, and user preference.
- Representing the trust by two attributes: trust value and performance value, in contrast to existing trust models. The model is tracked by a performance value, so that a more comprehensive and accurate trust can be evaluated. The assessment of the performance can help to achieve a better local decision.
- Considering consumers' preferences in selecting reliable sources of opinions.

- Including to the model, consumer's behaviour for the selection of reliable cloud providers independently of rating, which was presented as an effective factor for computation of trustworthiness in [20].
- Calculating the bias of the trust estimation, to defend against malicious feedbacks automatically without any previous experience (the difference between the value expectations and the true value of the factor being estimated.), so that inexact ratings will have low trust degree, making it have less or even no influence in the final evaluation.
- Comparing the proposed solution to well-known trust computing models as Eigen trust [13] or subjective logic [9], and implementing it in a simulated Cloud environment.

IV. Proposed Solution

In Cloud Computing, the entities are divided into Cloud Server Provider (CSP) and Cloud User (CU). Computing trust depends on interactions evidences between the CSP and the CU.

In Section 2, various approaches for computing the trust value have been discussed. However, these approaches are not appropriate to the modelling of our solution.

First, the probabilistic approaches, allow representing uncertainty of the next evidence but the probabilities are assumed to be known, which, is most likely difficult in a Cloud environment. The approaches based on Bayesian probabilities suppose the use of the probability density function, which bring to complex mathematical distributions and hard interpretations. The approaches based on fuzzy logic models represent a different type of certainty, more oriented to linguistic uncertainty or fuzziness.

Finally, the approaches based on subjective logic are more appropriates, but the parameters of belief, disbelief and certainty are dependent with each other. So, the CertainTrust [23] model and the CertainLogic [21] operators as the basis of our proposed solution have been used in this paper.

For future mention, the notation that is used through this paper are recapitulated in Table 1.

Table 1. Definitions of Notation

Notation	Definition
x	Consumer;
O(x)	Opinion Model for a user x;
E(x)	Expectation value for a user x;
r(x)	Average rating for a user x;
c(x)	Certainty for a user x;
f(x)	Initial expectation for a user x;
p	Amount of positive evidences;
n	Amount of negative evidences;
t	Total of rating given as t = p + n;
N	Total of evidences given as N = p + n + NA;
NA	Evidences without rate (neutrals)

A. The CertainLogic Model

The proposed solution uses the CertainTrust model proposed in [23], and combine the opinions by the CertainLogic [21] operators. The opinion model is based on subjective logic [9] and is used to design the uncertainty of trust.

In the model, the trustworthiness of a service represents the belief that a proposition (or a combination of propositions) is true. For example, a service is trustworthy if it is expected to deliver a certain service with a certain quality.

Each opinion of a proposition x represented as O(x) = (t, c, f) is modelled as a triple of values: average rating, certainty and initial expectation:

- Average Rating r(x) or rx, degree of which past observation support the truth of a proposition,
- Certainty c(x) or cx, degree to which the belief is assumed representative for the future,
- Initial Expectation f(x) degree that provides the weight of certainty and uncertainty of a proposition

The Certain Logic model is given as follows:

$$O(x) = (rx, cx, fx) \tag{1}$$

$$rx = \begin{cases} 0.5 & if \quad p+n=0 \\ \frac{p}{n} \end{cases} \tag{2}$$

$$cx = \frac{N * t}{w*(N-t) + N*t} \tag{3}$$

$$fx = 0.99 \tag{4}$$

With w is a given weight to neutral evidences.

The probability expectation of an opinion is used to provide the trust rating. The expectation of an opinion is given as:

$$E(O(x)) = r*c + (1-c)*f \tag{5}$$

Where $E \in [0,1]$

B. Model Description

In trust selection process, three main steps can be described. At first, users send requests where the initial global trust value is computed. If the resulted value is more than the threshold, a transaction is established. Then, the selection process goes into an evolution step where, the value of the global trust value is updated. This value results by the computing of the performance and the trust values. The resulted degree is compared to a threshold, after every transaction. The service transaction between the user and the provider is concluded, if the rate of the trust is less than the threshold. This process is shown in Fig. 1.

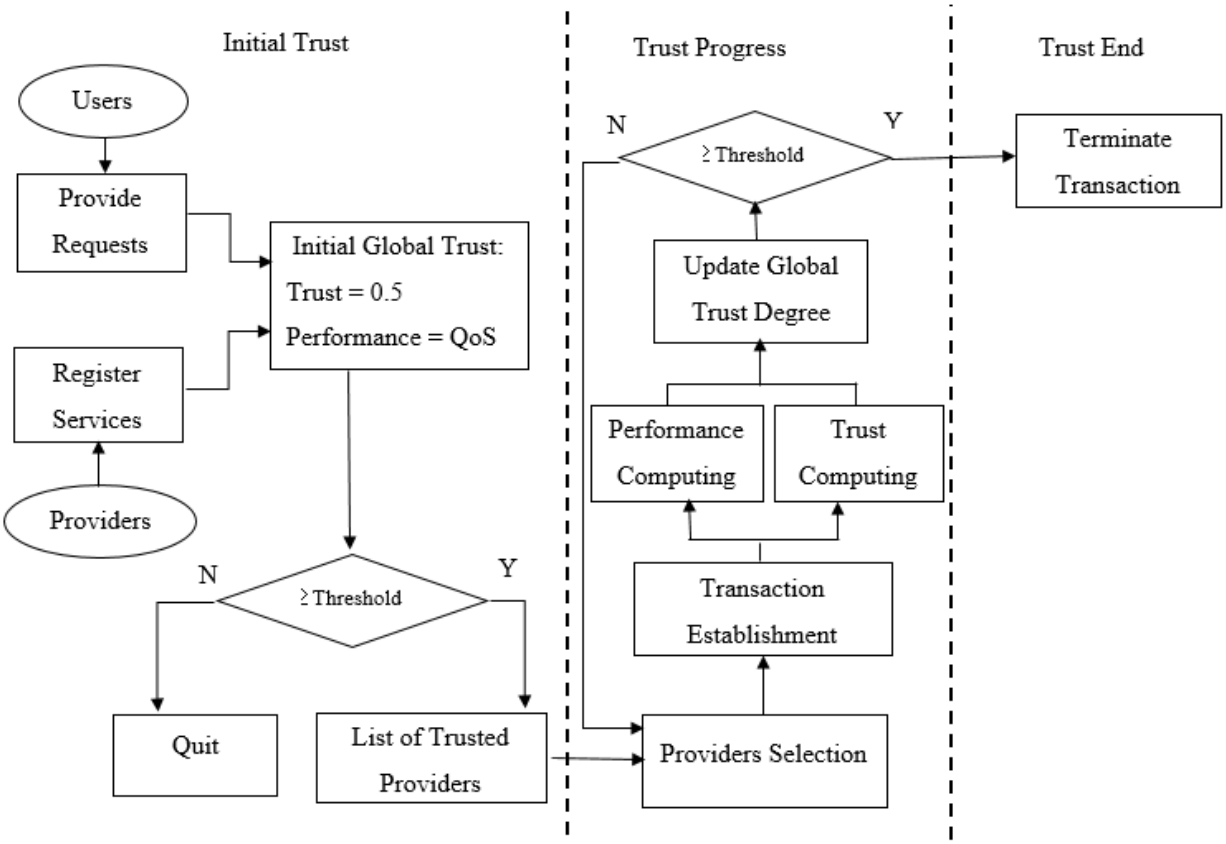

Fig. 1. Trust model process

C. Global Trust Computation

In this section, the proposed trust model for Cloud service selection is formally described. Our computing model concentrates on the estimation of the trust value for a provider in cloud computing and is based on the direct and other information.

In the model, information (evidences) are collected from different sources:

- User Interface,
- Cloud Service Provider,
- Recommendation from other sources,
- QoS values.

In the most proposed works, trust has been computed using user feedback by a certain formalism. All these methods are based on ratings. However, they neglect the fact that the provided performance of the service take an important part to win user confidence. Hence, a model that integrate these two parts to compute the global value of trust is proposed:

C.1 Performance Value

Several researchers have surveyed the existing trust models. They defined the trust as "the firm belief in the capability of an entity to act consistently, securely and reliably within a specified context". They also claim that the trust is the composition of multiple features such as reliability, honesty, truthfulness, dependability, security, competence, timeliness, QoS in the environment context.

In [15] the authors proposed a trust model based on QoS for Cloud Computing, based on four attributes: availability, reliability, data integrity and Turnaround Efficiency. However, computing performance based on these four attributes is insufficient to achieve a valid model. It must rely on standardized and approved measures in the context of Cloud Computing.

In order to form a performance model, attributes defined by Service Measurement Index (SMI) are used. Cloud Service Measurement Index Consortium (CSMIC) [4] proposes a framework based on common characteristics of cloud services. The purpose of this consortium is to express each of QoS attributes given in the framework and offer a methodology for computing a relative index for comparing different cloud services. CSMIC has designed the Service Measurement Index (SMI), which consists of a set of Key Performance Indicators (KPI) that aids to standardize the measurement of services.

The attributes (a_i) used in our model include power, cost, response time, efficiency, transparency, interoperability, reliability, availability, security. Each of these features is included in a set of Key Performance Indicators (KPIs), which describe the data to be gathered for measurement.

The performance value for Cloud Service (x) is computed by a utility function used with the described objective attributes.

$$P(x) = \sum_{i=0}^{9} w_i * x_i \quad (6)$$

w_i is a weight for each attribute with $\sum w_i = 1$

x_i is the attribute i for the service x.

C.2 Trust Value

The trust is a term that describes how much one believes in another. Evaluating trust for service can help users to predict its future behaviour [17]. For service selection, the trust value is denoted as T(x).

In our opinion, the three main features that a reliable service must offer besides the performance values are the time, the cost and the overall satisfaction of the service. Thus, to compute the final value of the trust, these three factors: time, cost, satisfaction that are presented in the SMI framework [4] have been used.

For each transaction, the trust value is computed as a combination of these factors.

$$T = \begin{cases} 0.5 & initial \\ \alpha \dfrac{\sum_{k=1}^{n} (f(t_k) * f(c_k) * f(s_k)}{n} \end{cases} \quad (7)$$

k: the k^{th} use of the service.

α: represent the adjustment factor, and is calculated by:

$$\alpha = \sqrt{\frac{n}{T+1}} \quad (8)$$

n: Number of satisfactory service use,

T: Total use of the service

$f(t_k)$: Attenuation factor.

$$f(t_k) = \frac{e^{-(t_0 - t_{k-1})}}{T} \quad (9)$$

$f(c_k)$: Cost factor [4].

$$f(c_k) = \frac{c_k}{cpu^a * net^b * vm^c * capacity^d} \quad (10)$$

With a + b + c + d = 1.

$f(s_k)$: Satisfaction factor.

$$f(s_k) = \begin{cases} 1 & if \quad user \quad satisfied \\ \dfrac{\sum Dissatisfaction \quad criteria}{Total \quad criteria} & else \end{cases} \quad (11)$$

The satisfaction criteria is defined by the performance attribute. The user gives a rate to each attribute defined in the Performance model. These values are normalized to give a final satisfaction factor.

To protect the system against malicious rating, the bias function for the satisfaction factor has been computed.

C.3 Selection Process

Our cloud service selection approach consists of six steps:

Step 1: (Initialize the values of Performance providers):
The initial values of performance represent the QoS delivered in the process of provider's registration.
The initial performance value is computed from the credentials of the resource provider.

Step 2: (Initialize the values of trust):
The initial Opinion model initializes the values of trust.

Step 3: (Computing the Performance values):
After a transaction, a performance value is computed for each use of the service.
The potential cloud consumer who asks for cloud service selection gives an importance weight to each attribute. Then, this value is converted into a normalized weight.

The opinion of the performance model is as follow:

$$O(P) = E(r, c, f) \quad (12)$$

$$rx = \begin{cases} 0 & if \quad p + n = 0 \\ \dfrac{p}{p+n} \end{cases} \quad (13)$$

$$c = \frac{N * (p+n)}{2 * NA + N * (p+n)} \quad (14)$$

$$f = P_0(x) \quad (15)$$

Where $P_0(x)$ represents the computed performance value for the user performing the selection, if none the credentials of the service provider are taken. NA represents the neutral assertions of the performance value.

In certain trust model, the authors set the initial expectation as a high value (0,99). In our model, we take the initial expectation as the initial performance based on the credentials of the service provider.

After each transaction, we collect the Performance value for the user. Then, we apply the opinion model for the total evidence of each value.

For the performance model, the evidence is positive if it complies with the expectation value of the total performance values.

The average rating t is calculated based on the number of performance value conforms to the expectation of the total performance values and the number of negative assertions.

The certainty c is calculated based on the total number of assertions N and the number of positive and negative

assertions. The c is 1 when all the assertions are "positive" or "negative" and 0 if no answer.

Step 4: (Filtering biased subjective satisfaction for the trust values):

The Euclidean distance between the feedbacks submitted by the user about the resource provider's service and the expectation for the ratings of the corresponding associated attribute is computed for each cloud service. When the distance exceeds the threshold, the biased subjective assessments having the exceeded distances are filter out. The allowable minimum threshold difference value is 0.05, and it is used as minimum threshold value.

The less similar is the rating, the less reliable is the subjective assessments and therefore the lower is the threshold.

1. Let the user feedback rating for the satisfaction criteria be $u_s = \{U_{s1}, U_{s2} \ldots U_{s9}\}$
2. Let the expectation for total feedback rating for the satisfaction criteria $e_s = \{E_{s1}, E_{s2} \ldots E_{s9}\}$
3. Compute the expectation values $E(u_s)$ and $E(e_s)$ of the sets us and e_s.
4. Compute the standard deviations of the set us and e_s of D_{us} and Des using the Equation (16) and Equation (17) respectively as follows.

$$D_{u_s} = \sqrt{E(u_s^2) - \left[E(u_s)\right]^2} \tag{16}$$

$$D_{e_s} = \sqrt{E(e_s^2) - \left[E(e_s)\right]^2} \tag{17}$$

5. Using the same expectation values and standard deviation formula from the previous algorithm, compute the regression line using Equation (18) as

$$\frac{u_s - E(u_s)}{D_{u_s}} = \frac{c*(e_s - E(e_s))}{D_{e_s}} \tag{18}$$

Where c is the correlation coefficient.

6. Assign the c value to u_{si} such as $u_{si} = c$.

If this correlation coefficient value of u_{si} > threshold value then the feedback from the consumer satisfaction is considered as biased one as it deviates from the total satisfaction threshold value of 0.05.

Step 5: (Computing Trust Value):

In the same way as the performance model, after each transaction, the Trust value for the user is collected. Then, the opinion model for the total evidence of each value is applied.

The opinion of the trust model is as follow:

$$O(T) = E(r, c, f) \tag{19}$$

$$rx = \begin{cases} 0 & if \quad p+n=0 \\ \dfrac{p}{p+n} \end{cases} \tag{20}$$

$$c = \frac{N*(p+n)}{2*NA + N*(p+n)} \tag{21}$$

$$f = T_0(x) \tag{22}$$

Where $T_0(x)$ represents the direct trust for the user performing the selection, and NA represents the neutral assertions of the trust values.

In certain trust model, the authors set the initial expectation as a high value (0,99). Hence, this is not accurate and does not represent realistic situations. Hence, the initial expectation in our model has been set as the computed direct trust for the user.

For the trust model, the evidence is positive if the trust value is over a certain threshold. The threshold is defined by the user preferences.

The average rating t is calculated based on the number of positive assertions and the number of negative assertions.

The certainty c is calculated based on the total number of assertions N and the number of positive and negative assertions. The c is 1 when all the assertions are "positive" or "negative" and 0 if no answer.

Step 6: (Determining the Global trust value):

The proposed model uses the Certain Logic model proposed in [23]. This model is based on the subjective logic operators [21] for combining the opinions.

In the proposed model, the trust of the cloud service provider is calculated in terms of its:

- Performance P(x), is provided by the service provider initially, then by the performance provided after each user's transaction.
- Trustworthiness T(x), is evaluated by direct experiences and feedback from other consumers.

The values of the two models are aggregated according to a consensus operator of CertainLogic [23] on the opinions obtained from each of these computations. Then the results of all services are ranked for selection.

The operators proposed in [21] are used to combine multiple opinions to form a single opinion using the operators such as conjunction, consensus that allows performing logical operations on opinions. The consensus operator ($\otimes$) provides means for aggregating opinions on the same statement from different and independent sources. Thus, the trust of a service x is:

$$R = O(O(P(x) \otimes O(T(x)))) \tag{23}$$

V. Experiments And Results

This section demonstrates the applicability of our developed trust model in a simulated cloud environment.

A. Simulation

Simulation is techniques for performing experiments on a system other than construct a real system. It is a simpler and effective approach for analysing and evaluating designed mechanisms, protocols, algorithms.

Cloud-Sim is a simulation toolkit developed by Buyya [38] for creating cloud simulation environment. The simulated cloud environment contains various resources to incorporate the heterogeneous concept. Each resource has different characteristics of computational factors such as processor speed, hard disk memory, ram memory and network values as bandwidth and latency.

The simulation has been performed using the latest version of cloudsim-3.0.3.

Inspired by various simulation works in the service trustworthiness evaluation, a prototype system was developed using the platform Netbeans. This Trust Management System is integrated with cloud simulation toolkit to select the resources based on the trust value other than time based and spaced based resource allocation.

A simulation experiment to demonstrate the effectiveness of our method has been conducted. The simulation is carried out with different user requirements of processor speed, ram memory, hard disk memory and number of services requirements.

Table 2. Simulation Parameters

No user	No provider	No DC/provider	No VM/DC	No service
100-1000	25	1-5	5-25	50

Experiment 1: Accuracy

100 rounds of simulation totally has been conducted. For each round, from 100 to 150 requests are generated randomly. Therefore, the request is an execution flow of different types of services. Then, three methods to select trustworthy providers are used:

1. Eigen Selection: based on EigenTrust algorithm as described by Hector Garcia-molina [13].
2. Subjective Logic Selection: Trust Network Analysis with Subjective Logic' approach of Jøsang [8].
3. Proposed Solution: It selects the provider by the proposed solution.

For the simulation rounds, the accuracy of the simulation are calculated. The accuracy of each method is equal to the total number of the successful transaction by the round of simulation.

The results are given in Fig 2. From the figure, it can be noted that our trust model can increase the number of successful transactions. During the 100 rounds of simulation, the successful number of transactions with the proposed solution increase significantly and remain stable at some point, in comparison to the Eigen algorithm and Subjective logic.

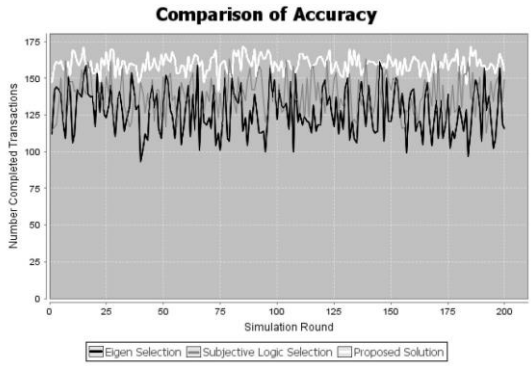

Fig. 2. Comparison of Accuracy

As the proposed solution is based on the user's rating but also on the performance value, it would be expected that the number of complete successful transactions have a higher ratio of accuracy compared to the others solutions.

Experiment 2: Execution time

250 rounds of simulation totally has been conducted. For each round, requests are issued randomly. Then three methods to select trustworthy providers are used:

1. Random Selection: It selects a random provider among the providers that fit all the functional SLA service requirements.
2. Performance Selection: It selects the provider that fits all the functional SLA service requirements.
3. Proposed Solution: It selects the provider by the proposed solution.

The results are shown in Fig 3. Given a certain number of transactions, all the propositions present a similar execution time. However with the overloading of the services demand, the exaction time of the random and performance selection increase where the proposed solution maintain a certain level. The major reason why the solution is better is that the proposed solution performs the selection of the provider based not only on the QoS, but also on the overall feedback of users, increasing the reliability of the provided service and minimizing along the execution time.

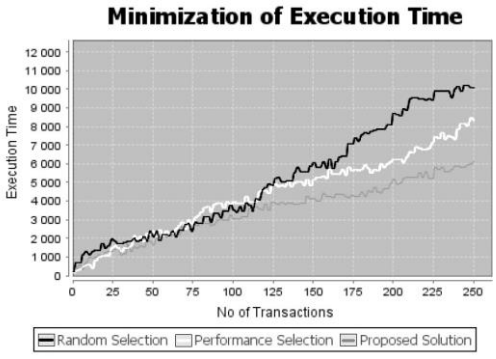

Fig. 3. Minimization of Execution Time

Experiment 3: The effectiveness of proposed model

In this experiment, the efficiency of our model is evaluated with Eigen algorithm and Subjective Logic, given 200 transactions.

The experimental result is as follows. Fig 4 reveals that the number of completed transaction is higher than the other strategies. At the same time, the proposed solution can averagely perform more valid transaction as the number of failed committed transaction is the lowest.

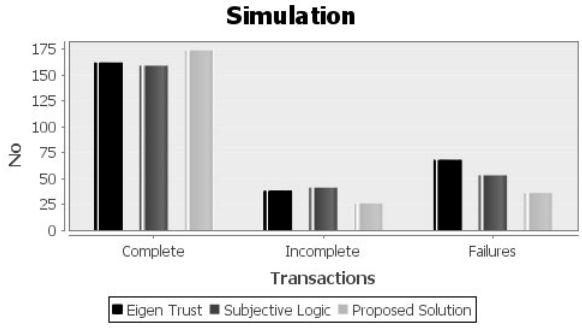

Fig. 4. Effectiveness of the transactions

Experiment 4: User Satisfaction

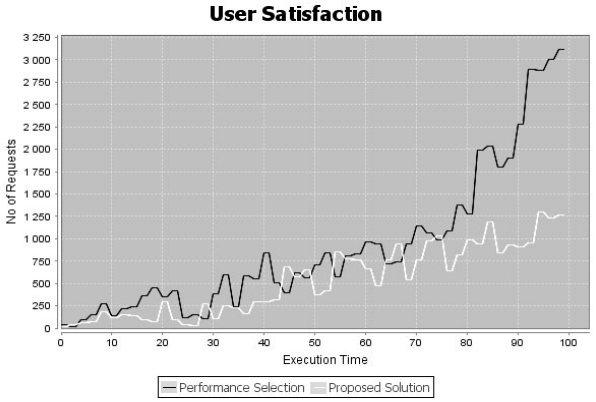

Fig. 5. User Satisfaction

In the fig 5, the comparative study of request numbers served with time, between the proposed solution and the Performance model is given. It can be seen, as the time of VMs creation is reduced in the proposed model additional requests can be served compared to the Performance model. Hence, user satisfaction and economic profit can be achieved. Here, as the time of service increases, the difference in serving requests between our proposition and performance model also increases.

B. Discussion

In order, to validate the Global Trust model we have implemented the system and two other strategies (Eigen Trust and Subjective Logic). We believe that our results confirm the accuracy and performance of our solution.

Eigen Trust [13] is a reputation algorithm described by Hector Garcia-molina. The algorithm was proposed for a p2p network. This solution was extended to be performed in cloud services and application. The algorithm calculate for each node in the network a global trust value based on the history of the consumer.

Subjective Logic [8] is an approach proposed by Josang. It is based on probabilities and takes into account the belief and uncertainty to providing a trustful selection.

The proposed solution aims to provide good performance and trusted selection for diverse services customers.

Clearly, the proposed solution offers a more accurate selection as a result of computing the trust and the performance of the selected service, in comparison to Eigen Trust and Subjective Logic which are based only on trust values (Fig. 2). Like the presented results (Fig. 4), the proposed solution fulfils the highest amount of transactions.

Furthermore, we have implemented and tested the proposed solution with a performance selection based only on the QoS of the provided service, and a random selection which consists a selecting randomly the services.

As presented in Figure 3, the proposed model achieves much less than the performance and random selection in execution time. The performance selection performs lowest execution time when the number of transaction is least, but with the overload of the services demand the execution time rise significantly. Where, the proposed solution tends to a more stable execution time.

Hence, the solution can concurrently support numerous services demands with maintaining accurate selection and user satisfaction (Fig 5.).

These results clearly show that the service selection used by the proposed model is quite higher compared to other algorithms. These values demonstrate the feasibility of Global Trust model.

VI. Conclusion And Future Work

Trust is the basis of the service relationships in cloud computing. In this paper, some trust models have been reviewed and the issues of these models have been shown. A trust model which aims at providing a truthful access to users has been presented. It can dynamically evaluate QoS for Cloud services according to effective performance and users ratings in the context of Cloud Computing. The improved solution is efficient because of the convergence speed and stability compared to other propositions. Furthermore, the feasibility of our approach has been validated by various simulations and comparisons with approved strategies as Eigen Trust or Subjective Logic. The results of simulations show that the service selection model can decide on an appropriate service for user from various Cloud services. Currently the overall system for this model is being developed. This system integrates additional requirements for Cloud Security as authentication, SLA technology... Finally, it would be interesting to examine how the presented trust model can be integrated to treat the security requirements of a real Cloud environment.

References

[1] Kamal K. Bharadwaj and Mohammad Yahya H. Al-Shamri. Fuzzy computational models for trust and

reputation systems. Electronic Commerce Research and Applications, 8(1):37-47, 2009.

[2] Sergey Brin and Lawrence Page. Reprint of:The anatomy of a large-scale hypertextual web search engine. Computer Networks, 56(18):3825-3833, 2012.

[3] Diogo A. B. Fernandes, Liliana F. B. Soares, João V. P. Gomes, Mário M. Freire, and Pedro R. M. Inácio. Security issues in cloud environments: a survey. Int. J. Inf. Sec., 13(2):113-170, 2014.

[4] Saurabh Kumar Garg, Steven Versteeg, and Rajkumar Buyya. A framework for ranking of cloud computing services. Future Generation Comp. Syst., 29(4):1012-1023, 2013.

[5] Guangjie Han, Jinfang Jiang, Lei Shu, Jianwei Niu, and Han-Chieh Chao. Management and applications of trust in wireless sensor networks: A survey. J. Comput. Syst. Sci., 80(3):602-617, 2014.

[6] Jin Huang, Feiping Nie, Heng Huang, and Yi-Cheng Tu. Trust prediction via aggregating heterogeneous social networks. In 21st ACM International Conference on Information and Knowledge Management, CIKM'12, Maui, HI, USA, October 29 - November 02, 2012, pages 1774-1778, 2012.

[7] Naima Iltaf and Abdul Ghafoor. A fuzzy based credibility evaluation of recommended trust in pervasive computing environment. In 10th IEEE Consumer Communications and Networking Conference, CCNC 2013, Las Vegas, NV, USA, January 11-14, 2013, pages 617-620, 2013.

[8] Audun Jøsang, Elizabeth Gray, and Michael Kinateder. Simplification and analysis of transitive trust networks. Web Intelligence and Agent Systems, 4(2):139-161, 2006.

[9] Audun Jøsang, Ross Hayward, and Simon Pope. Trust network analysis with subjective logic. In Computer Science 2006, Twenty-Nineth Australasian Computer Science Conference (ACSC2006), Hobart, Tasmania, Australia, January 16-19 2006, pages 85-94, 2006.

[10] Audun Jøsang, Roslan Ismail, and Colin Boyd. A survey of trust and reputation systems for online service provision. Decision Support Systems, 43(2):618-644, 2007.

[11] Audun Jøsang. A logic for uncertain probabilities. International Journal of Uncertainty, Fuzziness and Knowledge- Based Systems, 9(3):279-212, 2001.

[12] Audun Jøsang. Subjective logic. Technical report, University of Oslo, 2013.

[13] Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina. The eigentrust algorithm for reputation management in P2P networks. In Proceedings of the Twelfth International World Wide Web Conference, WWW 2003, Budapest, Hungary, May 20-24, 2003, pages 640-651, 2003.

[14] Ronny Lempel and Shlomo Moran. The stochastic approach for link-structure analysis (SALSA) and the TKC effect. Computer Networks, 33(1-6):387-401, 2000.

[15] Paul Manuel. A trust model of cloud computing based on quality of service. Annals of Operations Research, pages 1-12, 2013.

[16] Stephen Paul Marsh. Formalising trust as a computational concept. Technical report, 1994.

[17] Tim Muller and Patrick Schweitzer. On beta models with trust chains. In Trust Management VII - 7th IFIP WG 11.11 International Conference, IFIPTM 2013, Malaga, Spain, June 3-7, 2013. Proceedings, pages 49-65, 2013.

[18] Talal H. Noor, Quan Z. Sheng, Sherali Zeadally, and Jian Yu. Trust management of services in cloud environments: Obstacles and solutions. ACM Comput. Surv. 46(1):12, 2013.

[19] Siani Pearson and Azzedine Benameur. Privacy, security and trust issues arising from cloud computing. In Cloud Computing, Second International Conference, CloudCom 2010, November 30 - December 3, 2010, Indianapolis, Indiana, USA, Proceedings, pages 693-702, 2010.

[20] Pramod S. Pawar, Muttukrishnan Rajarajan, Srijith Krishnan Nair, and Andrea Zisman. Trust model for optimized cloud services. In Trust Management VI - 6th IFIP WG 11.11 International Conference, IFIPTM 2012, Surat, India, May 21-25, 2012. Proceedings, pages 97-112, 2012.

[21] Sebastian Ries, Sheikh Mahbub Habib, Max Mühlhäuser, and Vijay Varadharajan. Certainlogic: A logic for modeling trust and uncertainty - (short paper). In Trust and Trustworthy Computing - 4th International Conference, TRUST 2011, Pittsburgh, PA, USA, June 22-24, 2011. Proceedings, pages 254-261, 2011.

[22] Paul Resnick and Richard Zeckhauser. Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System. Elsevier Science, November 2002.

[23] Sebastian Ries. Extending bayesian trust models regarding context-dependence and user friendly representation. In Proceedings of the ACM SAC, New York, USA, 2009.

[24] Shanshan Song, Kai Hwang, and Yu-Kwong Kwok. Risk-resilient heuristics and genetic algorithms for security-assured grid job scheduling. IEEE Trans. Computers, 55(6):703-719, 2006.

[25] Shanshan Song, Kai Hwang, Runfang Zhou, and Yu-Kwong Kwok. Trusted P2P transactions with fuzzy reputation aggregation. IEEE Internet Computing, 9(6):24-34, 2005.

[26] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. J. Network and Computer Applications, 34(1):1-11, 2011.

[27] Wanita Sherchan, Surya Nepal, and Cécile Paris. A survey of trust in social networks. ACM Comput. Surv., 45(4):47, 2013.

[28] Ahmad-Reza Sadeghi and Christian Stüble. Property-based attestation for computing platforms: caring about properties, not mechanisms. In Proceedings of the New Security Paradigms Workshop 2004, September 20-23, 2004, Nova Scotia, Canada, pages 67-77, 2004.

[29] Antonino Simone, Boris Skoric, and Nicola Zannone. Flow-based reputation: More than just ranking. International Journal of Information Technology and Decision Making, 11(3):551-578, 2012.

[30] Adel Nadjaran Toosi, Rodrigo N. Calheiros, and Rajkumar Buyya. Interconnected cloud computing environments: Challenges, taxonomy, and survey. ACM Comput. Surv., 47(1):7, 2014.

[31] Mozhgan Tavakolifard and Svein J. Knapskog. A probabilistic reputation algorithm for decentralized multi-agent environments. Electr. Notes Theor. Comput. Sci., 244:139-149, 2009.

[32] W. T. Luke Teacy, Michael Luck, Alex Rogers, and Nicholas R. Jennings. An efficient and versatile approach to trust and reputation using hierarchical Bayesian modelling. Artif. Intell., 193:149-185, 2012.

[33] Ton van Deursen, Paul Koster, and Milan Petkovic. Hedaquin: A reputation-based health data quality indicator. Electr. Notes Theor. Comput. Sci., 197(2):159-167, 2008.

[34] Andrew Whitby, Audun JAsang, and Jadwiga Indulska. Filtering Out Unfair Ratings in Bayesian Reputation Systems. 2004.

[35] Yonghong Wang and Munindar P. Singh. Trust representation and aggregation in a distributed agent

system. In Proceedings of the 21st National Conference on Artificial Intelligence - Volume 2, AAAI'06, pages 1425-1430. AAAI Press, 2006.

[36] Yanchao Zhang and Yuguang Fang. A fine grained reputation system for reliable service selection in peer-to-peer networks. IEEE Trans. Parallel Distrib. Syst., 18(8):1134-1145, 2007.

[37] Partha Sarathi Banerjee, J. Paulchoudhury, S. R. Bhadra Chaudhuri. Fuzzy Membership Function in a Trust Based AODV for MANET. Intern. Journal of Computer Network and Information Security (IJCNIS), 5(12), 27. 2013.

[38] Calheiros, R. N., Ranjan, R., Beloglazov, A., De Rose, C. A., & Buyya, R. CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. Software: Practice and Experience, 41(1), 23-50. 2011.

Authors' profiles

Fatima Zohra Filali, born in 1987. Ph. D. candidate in the University of Oran1 Ahmed Benbella from Algeria. Her main research interests include distributed system, cloud computing and network security. Her current work concerns the management of trust in cloud environments, and service selection.

Belabbas Yagoubi, PhD in Computer Science, is a professor at the University of Oran1 Ahmed Benbella (Algeria). He is interested in research in the field of large-scale distributed systems including security, replication, load balancing and task scheduling.

How to cite this paper: Fatima Zohra Filali, Belabbes Yagoubi,"Global Trust: A Trust Model for Cloud Service Selection ", IJCNIS, vol.7, no.5, pp.41-50, 2015.DOI: 10.5815/ijcnis.2015.05.06

