Preferences Based Customized Trust Model for Assessment of Cloud Services

Shilpa Deshpande and Rajesh Ingle
Department of Computer Engineering, College of Engineering Pune, Savitribai Phule Pune University, India

Article Info

Article history:
Received May 13, 2017
Revised Nov 23, 2017
Accepted Dec 7, 2017

Keyword:
Cloud computing
Customized trust assessment
Dynamic trust
Elastic trust computation
Quality of Service (QoS)

ABSTRACT

In cloud environment, many functionally similar cloud services are available. But, the services differ in Quality of Service (QoS) levels, offered by them. There is a diversity in user requirements about the expected qualities of cloud services. Trust is a measure to understand whether a cloud service can adequately meet the user requirements. Consequently, trust assessment plays a significant role in selecting the suitable cloud service. This paper proposes preferences based customized trust model (PBCTM) for trust assessment of cloud services. PBCTM takes into account user requirements about the expected quality of services in the form of preferences. Accordingly, it performs customized trust assessment based on the evidences of various attributes of cloud service. PBCTM enables elastic trust computation, which is responsive to dynamically changing user preferences with time. The model facilitates dynamic trust based periodic selection of cloud services according to varying user preferences. Experimental results demonstrate that the proposed preferences based customized trust model outperforms the other model in respect of accuracy and degree of satisfaction.

Copyright © 2018 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:
Shilpa Deshpande,
Department of Computer Engineering,
College of Engineering Pune, Savitribai Phule Pune University,
Pune, Maharashtra, India
Email: shilpshree@yahoo.com

1. INTRODUCTION

Cloud computing has entered mainstream and received wider acceptance. It is increasingly adopted by individuals, small and medium scale enterprises (SMEs) and government organizations to run their critical applications. The reason for this acceptance is the characteristics of cloud like scalability, on demand service, anytime-anywhere access, economic benefits of pay-per-use, delegation of maintenance and administration, performance and disaster recovery. Cloud services have proliferated to include software as a service, database as a service, platform as a service, infrastructure as a service, security as a service and storage as a service [1]. Cloud environment still remains challenging to rely on because of factors like loss of control over applications and data, increased threats of security [2], performance issues related to virtualization [3], enterprise grade availability requirements [4, 5, 6] and adequately meeting Quality of Service (QoS) expectations of users [7].

Cloud computing has compelling advantages yet challenges too. For an enterprise to adopt cloud, it is important that enterprise has a certain belief that advantages of cloud can be realized. Trust is a measure of this belief [8]. Conventionally, people rely on reputation [4, 8], service level agreement (SLA) [6, 9], self-assessment [8, 9] and cloud auditing [8, 9] for trust assessment in cloud environment. However, trust assessment in cloud environment poses further important issues, which are revealed as part of the following discussion.

Reputation based traditional trust assessment technique relies on the opinions of cloud users. The opinions taken in the form of ratings or feedbacks may be subjective in nature [8]. Therefore, reputation cannot be an exact reflection of realistic capabilities of the cloud service. A service level agreement (SLA) established between a cloud service consumer and a provider consists of functional and QoS facets of the offered service [10]. Levels of SLA are not consistent among the cloud service providers offering analogous services. Moreover, for a service provider, promises made in SLA and actual QoS delivered are not consistent. Consequently, it makes hard for consumers, to evaluate the trust of a cloud service, solely based on the SLA [6, 9]. Cloud service provider may announce the self-assessment of the offered cloud services, based on cloud transparency mechanisms [8]. However, such evaluation of cloud services reflects merely a generalized trust assessment of cloud services from the viewpoint of provider. The mechanism of self-assessment does not take into consideration cloud user's perspective. A formal cloud audit based trust evaluation is an another method which providers may use to ensure the quality of offered services. However, audit report typically represents only a static trust assessment of the service at the time when auditing is done [9].

Cloud QoS attributes such as performance, availability, reliability and security are significant for user and hence for trust assessment of a cloud service [9]. Past recorded evidences of QoS attributes signify the actual values and they represent the realistic capabilities of a cloud service [8]. Therefore, the evidences of cloud QoS attributes are needed to be taken into account by the trust evaluation mechanism. There is a diversity in requirements of cloud users about the expected qualities of cloud services. Hence, customized trust assessment [9] of a cloud service which takes into consideration the user preferences for the cloud QoS attributes, is needed to enable the personalized selection of suitable cloud service [11].

Cloud service provider's capacity to provide services varies with time. As a result, the QoS levels of offered services also change with time. Therefore, trust evaluation based on one-time evidences of QoS attributes is not enough and it has to be a constant dynamic process [8]. Requirements of the user about the expected QoS may change dynamically with time [12]. Cloud service provider's ability to meet user requirements is not always constant. Therefore, trust assessment which includes one-time checking of requirements of the user is not adequate. Hence, trust assessment needs to be responsive to the changes in requirements of the user. This implies the need for elastic trust assessment as per the changes in requirements of the user.

In this paper, we present preferences based customized trust model (PBCTM), addressing the above mentioned issues. More specifically, the contributions are:

1. A novel method for trust computation of a cloud service based on the distances of various service evidences from the user preferences.

2. Customized trust assessment mechanism containing mathematical formulation of weights which are computed based on the relative importance of cloud service attributes with respect to QoS expectations of user.

3. Introduction of the concept of elastic trust computation of a cloud service and an algorithm for it.

4. Mechanism for ranking of cloud services based on trust computation which is dynamic, elastic and considers preferences of users.

5. Comparison of the proposed trust model with other model with regard to accuracy and a new measure of degree of satisfaction of trust assessment.

The paper is organized as follows. Section 2 presents a review of related work. In Section 3, the architecture of the system meant for the proposed trust model and the functional overview of trust assessment are described. Section 4 defines the preferences based customized trust model (PBCTM) and presents the details of customized and dynamic trust assessment. Section 5 presents the algorithm for elastic trust computation of a cloud service. Section 6 depicts the method for ranking of cloud services based on the proposed trust model. Section 7 presents the qualitative comparison of PBCTM with other models. Section 8 covers the performance evaluation of the proposed trust model including the results and analysis. Section 9 concludes the paper.

2. RELATED WORK

Reputation based approaches make use of feedbacks from many cloud users to evaluate trust of a cloud service. Trust assessment approaches proposed by [13, 14, 15] are based on reputation. These approaches do not take into account requirements of user for trust evaluation. Moreover, these reputation based approaches fall short in performing dynamic assessment of trust [8].

Besides user feedbacks, few of the approaches in literature, take into consideration additional factors such as provider's self-declarations and expert's ratings, for trust assessment [16]. However, credibility [4] of the factors included in trust evaluation is a main concern in these approaches. Habib et al. [10] proposed an architecture to enable trust assessment of cloud service providers using various factors such as provider statements, user feedbacks and certificates. A trust model based on service level agreement (SLA) parameters is proposed by Pawar et al. [17]. Ghosh et al. [18] proposed a framework for assessment of risk of interaction with cloud service provider. The approach in turn includes evaluating trust of the service provider. The trust is estimated on the basis of direct and indirect interactions between customer and cloud provider. The approaches [10, 17, 18] do not offer dynamic trust update along a period of time. Also, these approaches do not consider QoS requirements of user for trust assessment. A model is recommended by Moyano et al. [19] to evaluate trust of cloud providers. Although, the approach is simple, trust assessment mainly depends on the accessibility to the information released by the cloud providers.

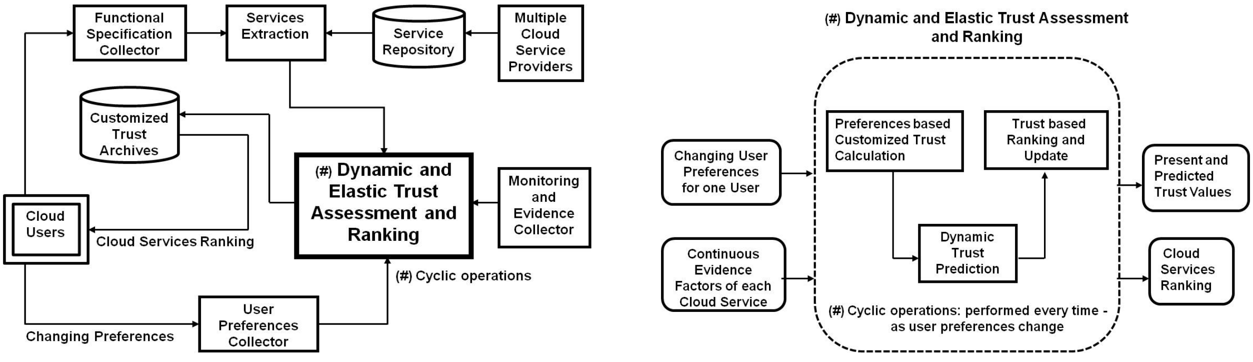
Few of the approaches do take into account QoS attributes for trust evaluation. The approach proposed by Manuel et al. [20] evaluates the trust of a cloud resource in terms of summation of values assigned to user feedbacks, security level and reputation. A model is suggested by Manuel et al. [21] to compute the reputation based trust of a resource. The model makes use of identity, capability and behavior values of a resource to obtain its trust value. The approaches [20, 21] do not consider requirements of users in trust estimation of resources. Also, these approaches do not reflect dynamic trust assessment of resources along a period of time. A fuzzy trust evaluation approach for cloud services is suggested by Huo et al. [22]. The approach takes into consideration a set of cloud service attributes to assess the reputation based trust value. Fan et al. [23] suggested a mechanism for evaluating dynamic trust of a cloud service using multiple attributes. The mechanism of trust computation relies on the feedbacks given by the users. However, authenticity of feedbacks is not addressed by the authors. The approach facilitates selection of a service according to the user requirements for various attributes. However, the approaches [21, 22, 23] are dependent on subjectively allocated weights to the various factors.

The QoS based mechanisms in literature, make use of availability, performance, security and reliability as the general attributes of cloud service for trust assessment. Throughput, response time, network bandwidth and capability are the usually considered performance related factors in trust estimation. Li et al. [24] proposed a method for dynamic trust evaluation of cloud resources. It makes use of recorded values of various attributes for computation of trust. The authors do not focus on consideration of user requirements for attributes, in evaluating trust value of a resource. Frameworks are proposed by [25, 26] for trust evaluation of cloud service providers based on QoS attributes. The approaches are based on monitoring QoS attributes and evaluating the compliance with regard to the SLA. System suggested by [26] incorporates perspectives of different entities such as cloud users, auditor and peers in the process of trust evaluation. Supriya et al. [27] proposed to employ multi-criteria based decision making methods for evaluating trust of cloud service providers. The work facilitates ranking of providers based on their trust values. It offers personalized computation of trust by considering priorities for the various attributes of cloud provider. However, priority based weights assigned to the different attributes are static and subjective. System is proposed by Qu and Buyya [11] for trust estimation of a cloud service based on its performance in terms of various QoS attributes. The approach takes into account QoS requirements of user and computes the trust of a service based on fulfillment of the requirements. However, the approaches [11, 25, 26, 27] do not offer dynamic trust update in cloud environment. A model is proposed by Manuel [28] to evaluate trust of a resource based on its capabilities and measured QoS attributes. Trust update is indicated only by algorithmic steps. The model enables matching the QoS requirements of users to the resources according to their computed trust values. However, static weights based on pre-decided priorities are assigned to the various attributes.

In summary, consideration of user requirements in trust assessment is essential to enable the personalized selection of appropriate cloud services. However, the above review of the related work signifies that only few of the approaches [11, 23, 27, 28] consider requirements of cloud users for trust assessment. Cloud QoS attributes are significant for trust evaluation of a cloud service. Evidences of QoS attributes obtained through monitoring are unbiased in nature and are more dependable factors for trust estimation. However, the approach [23] does not take into account evidences of QoS attributes and trust assessment solely relies on the feedbacks of users. Dynamic cloud environment implies the need for trust to be assessed continuously with time. However, the approaches [11, 27] do not offer dynamic trust evaluation of cloud services. Although, the approach [28] takes into consideration requirements of users, weights calculation for various attributes in trust assessment does not reflect preferences of users. Moreover, assessment of trust according to the dynamically changing requirements of the user, is not addressed by any of the above approaches. Our trust model PBCTM, aims to address these limitations in the earlier work. PBCTM performs customized trust assessment of a cloud service by taking into account evidences of service attributes and preferences of user for attributes. Our model facilitates elastic trust computation of a cloud service according to the dynamically changing user preferences of attributes with time. PBCTM enables computation of weights for the multiple attributes of a service by considering the relative utility of attributes with respect to the user preferences. Dynamic trust prediction used in our model, allows ranking of cloud services to assist the user in periodic selection of suitable service.

3. ARCHITECTURE OF TRUST ASSESSMENT SYSTEM

Figure 1a shows the overall layout of the system meant for the proposed trust model. It depicts the main trust assessment and ranking module which is connected with the other supplementary modules. The functional specification collector compiles the functional requirements of the cloud service, submitted by cloud user. Multiple service providers register their services into the service repository. Services Extraction module finds the services from service repository whose functional specifications match with the required one. The user preferences collector compiles the preference values for cloud service attributes such as availability, throughput and response time, which are submitted by the cloud user.


Functional Specification Collector
Services Extraction
Service Repository
Multiple Cloud Service Providers
Customized Trust Archives
(#) Dynamic and Elastic Trust Assessment and Ranking
Monitoring and Evidence Collector
Cloud Users
Cloud Services Ranking
(#) Cyclic operations
User Preferences Collector
Changing Preferences
(#) Dynamic and Elastic Trust Assessment and Ranking
Changing User Preferences for one User
Preferences based Customized Trust Calculation
Trust based Ranking and Update
Present and Predicted Trust Values
Dynamic Trust Prediction
Continuous Evidence Factors of each Cloud Service
Cloud Services Ranking
(#) Cyclic operations: performed every time - as user preferences change

(a) Architecture

(b) Functional overview

Figure 1. Trust assessment system for preferences based customized trust model (PBCTM)

Trust assessment and ranking module is the core component performing dynamic and elastic trust computation of the cloud services. For each of the matching cloud services, the trust assessment is carried out by taking into account the user preferences and the evidences of service attributes. The results of trust assessment and ranking are recorded in the customized trust archives. The cloud user can select the appropriate cloud service based on the ranking of cloud services.

The process of monitoring, continuously observes and records the values of attributes such as response time, throughput, availability and security, for each of the cloud services. The evidence collector collects the evidence factors, recorded as part of continuous monitoring process. These evidence factors are then used for trust assessment of cloud services.

Trust assessment and ranking is the main focus of this paper. Hence, the details of other modules which include services extraction, monitoring and related functionalities, are not discussed further, in this paper. We assume these as the already existing valid services and are available in the form of external interfaces to the trust assessment and ranking module.

Figure 1b shows the high-level functional overview for trust assessment and ranking of cloud services. The user preferences for various service attributes, are taken as input for the trust assessment. Evidence factors for each of the matching cloud services, over the period of time, are taken as another input by the trust assessment module. The module calculates customized present trust of services at an instant of time, by considering the user preferences and the corresponding service evidence factors. Subsequently, the module performs dynamic prediction of trust values of cloud services over a period of time. The customized present trust and predicted trust values are returned to the cloud user. The ranking of cloud services is performed by the module, based on the predicted trust values of the services. The resultant ranking sequence of cloud services, which is then returned to the cloud user, facilitates the customized selection of suitable cloud service for the user.

The preferences of a particular cloud user may change dynamically with time. Accordingly, the operations of trust assessment and ranking of cloud services are performed repetitively with changing preferences of the user and the continuous evidences of each cloud service. This reflects the dynamic and elastic trust computation of cloud services. The cloud user can revise the selection of a suitable service based on the updated ranking of cloud services. The details of customized and dynamic trust assessments of a cloud service are described in Section 4. The steps depicting the control flow for elastic trust computation are presented in Section 5 in the form of algorithm. The trust based ranking of cloud services is elaborated in Section 6.

4. PREFERENCES BASED CUSTOMIZED TRUST MODEL

Trust assessment of a cloud service is performed based on the preferences of a cloud user for service attributes and the evidence factors of the service. Evidence factors of a cloud service signify the recorded values of service attributes.

Definition 1 *Preferences Based Customized Trust Model (PBCTM) is defined by a 12-tuple:* $(L, AC, TI, PR, C, NC, PDP, NDP, CPT, CT, E, D)$ *where*

L: Set of v cloud services: $\{s_1, s_2, ..., s_v\}$

AC: Set of m cloud service attributes: $\{R_1, R_2, ..., R_m\}$

TI: Ordered discrete set of n time instances, in a time window: $\{1, 2, ..., n\}$

PR: Set of preferences of a user for the values of cloud service attributes: $\{pr_1, pr_2, ..., pr_m\}$

C: An evidence matrix which depicts m evidence factors at each of the n time instances.

NC: Normalized augmented evidence matrix with preferences.

PDP: Normalized matrix for positive distances from preferences.

NDP: Normalized matrix for negative distances from preferences.

CPT: Customized Present Trust of a cloud service at a particular time instant.

CT: Cumulative Trust of a cloud service over a period of time.

E: A set of core trust assessment functions:$\{f_{CPT}, f_{CT}\}$*; where* f_{CPT} *indicates a function to compute Customized Present Trust (CPT) and* f_{CT} *is a function to assess Cumulative Trust (CT).*

D: A set of allied functions: $\{f_{NE}, f_{PD}, f_{ND}, f_{CW}\}$*; where* f_{NE} *is a function to normalize evidence factors and preferences;* f_{PD} *and* f_{ND} *are the functions to compute summative positive and negative distances from preferences;* f_{CW} *indicates a function to compute weights of cloud service attributes.*

Evidence factors of a cloud service are retrieved after every fixed time interval. Representation of the evidence factors is shown by an evidence matrix as:

$$C = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1m} \\ c_{21} & c_{22} & \cdots & c_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nm} \end{bmatrix} \tag{1}$$

In Equation (1), at a particular time instant *i* in a time window, such that $1 \leq i \leq n$, a row in the matrix indicates a sample of evidence factors as $\{c_{i1}, c_{i2}, ..., c_{im}\}$ and each value c_{ij} in the sample, denotes a value of an attribute R_j. Thus there are *n* samples of evidence factors. Column position in the matrix indicates a specific attribute within the sample.

Preferences for the values of cloud service attributes, as specified by the user, are combined with the original evidence matrix, to obtain the augmented matrix, as shown below.

$$CP = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1m} \\ c_{21} & c_{22} & \cdots & c_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nm} \\ pr_1 & pr_2 & \cdots & pr_m \end{bmatrix} \tag{2}$$

In Equation (2), the last row in the matrix indicates a sample of preferences as $\{pr_1, pr_2, ..., pr_m\}$ and each value pr_j in the sample denotes a preference value of an attribute R_j. For a cloud service, higher values for attributes such as availability and throughput are desired. Whereas, lower values for attributes such as response time and security violation incidents are expected. If the preference value for any of the attributes is not specified by the user, then it reflects that, a minimum quality level for that service attribute is acceptable to the user. Hence, in such case the preference value for the attribute in matrix CP is set to a minimum or maximum value of the service attribute in the time window, based on the higher-value type of attribute (e. g. availability) or the lower-value type of the attribute (e. g. response time), respectively. In order to transform all the values in matrix CP to uniform range and to make them independent of units, values of the matrix CP need to be normalized. Normalization includes scaling of the values. Thus, for further processing of distance computation, each value in the matrix CP is normalized in the range denoted by $[R^{new\_min}, R^{new\_max}]$. From the perspective of desired performance of a cloud service, attributes can be categorized in two types: one where higher values of an attribute R_j are desired and the other where lower values of R_j are desired. The category where higher values of R_j are desired, the corresponding normalized values x_{ij} and y_j for c_{ij} and pr_j respectively, are formulated as:

$$x_{ij} = \frac{(c_{ij} - R_j^{min})(R^{new\_max} - R^{new\_min})}{(R_j^{max} - R_j^{min})} + R^{new\_min} \tag{3}$$

$$y_j = \frac{(pr_j - R_j^{min})(R^{new\_max} - R^{new\_min})}{(R_j^{max} - R_j^{min})} + R^{new\_min} \tag{4}$$

The other category where lower values of R_j are desired, the corresponding normalized values x_{ij} and y_j for c_{ij} and pr_j respectively, are devised as:

$$x_{ij} = \frac{(R_j^{max} - c_{ij})(R^{new\_max} - R^{new\_min})}{(R_j^{max} - R_j^{min})} + R^{new\_min} \tag{5}$$

$$y_j = \frac{(R_j^{max} - pr_j)(R^{new\_max} - R^{new\_min})}{(R_j^{max} - R_j^{min})} + R^{new\_min} \tag{6}$$

In Equations (3) to (6), R_j^{min} is the minimum value of the attribute R_j and R_j^{max} is the maximum value of R_j in matrix CP. The normalized augmented matrix is:

$$NC = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} & \cdots & x_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nm} \\ y_1 & y_2 & \cdots & y_m \end{bmatrix} \tag{7}$$

In normalized matrix NC, greater value for any service attribute R_j where $1 \leq j \leq m$, indicates a higher quality of a cloud service than the quality of a cloud service corresponding to the lower value of the attribute.

4.1. Computation of Distances from Preferences

If the values of service attributes are higher as compared to the corresponding preference values, it reflects a more trustworthiness of a cloud service. Here we introduce, the new terms, Positive Distance (PD) and Negative Distance (ND) to define the comparison of the service attribute values and the associated preference values. PD and ND are the measures for assessment of how closely a cloud service meets or fails to meet the user expectations.

Definition 2 *Positive Distance (PD) and Negative Distance (ND) for any value a_{ij} in matrix NC, where $1 \leq i \leq (n+1)$, of attribute R_j from its corresponding preference value y_j, are formulated as shown in Table 1.*

Table 1. Distances from Preferences

Scenarios for a_{ij}	PD	ND
Attribute value (a_{ij}) = Preference value (y_j)	y_j	0
Attribute value (a_{ij}) > Preference value (y_j)	$y_j + a_{ij}$	$y_j - a_{ij}$
Attribute value (a_{ij}) < Preference value (y_j)	$a_{ij} - y_j$	$y_j - a_{ij}$

As defined in Table 1, if the attribute value is greater than or equal to the preference value, then its (PD) is higher than its (ND). If the attribute value is lesser than the preference value, then its (PD) is lesser than its (ND). Also, when the attribute value is greater than the preference value, then: i) its (PD) is higher than the (PD) for an attribute whose value equals the preference value. ii) its (ND) is lesser than the (ND) for an attribute whose value equals the preference value. Whereas, when the attribute value is lesser than the preference value, then: i) its (PD) is lesser than the (PD) for an attribute whose value equals the preference value. ii) its (ND) is higher than the (ND) for an attribute whose value equals the preference value.

Thus, for the values of all the attributes in matrix NC, which include both, normalized service evidence factors and preference values, computations of PD and ND values are performed. The computed PD and ND values are represented in the form of Positive Distance and Negative Distance matrices respectively, as:

$$PS = \begin{bmatrix} ps_{11} & ps_{12} & \cdots & ps_{1m} \\ ps_{21} & ps_{22} & \cdots & ps_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ ps_{n1} & ps_{n2} & \cdots & ps_{nm} \\ ps_{(n+1)1} & ps_{(n+1)2} & \cdots & ps_{(n+1)m} \end{bmatrix} \tag{8}$$

$$NS = \begin{bmatrix} ns_{11} & ns_{12} & \dots & ns_{1m} \\ ns_{21} & ns_{22} & \dots & ns_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ ns_{n1} & ns_{n2} & \dots & ns_{nm} \\ ns_{(n+1)1} & ns_{(n+1)2} & \dots & ns_{(n+1)m} \end{bmatrix} \tag{9}$$

In Equation (8), at position i such that $1 \leq i \leq n$, a row in the matrix PS indicates a sample of positive distances as $\{ps_{i1}, ps_{i2}, ..., ps_{im}\}$ corresponding to evidence sample $\{x_{i1}, x_{i2}, ..., x_{im}\}$ of matrix NC. Here, ps_{ij} denotes a PD value for an evidence factor x_{ij} of an attribute R_j from its preference value y_j. Similarly, in Equation (9), at position i such that $1 \leq i \leq n$, a row in the matrix NS indicates a sample of negative distances as $\{ns_{i1}, ns_{i2}, ..., ns_{im}\}$ corresponding to evidence sample $\{x_{i1}, x_{i2}, ..., x_{im}\}$ of matrix NC. Here, ns_{ij} denotes a ND value for an evidence factor x_{ij} of an attribute R_j from its preference value y_j. The $(n+1)^{th}$ rows in matrices PS and NS represent the samples of positive and negative distances respectively, for the sample $\{y_1, y_2, ..., y_m\}$ of preferences in matrix NC.

For next processing of customized trust computation, all the distance values in the matrices PS and NS are normalized in the range denoted by $[D^{new\_min}, D^{new\_max}]$. This conversion of all the distance values to uniform range is made by preserving the original relative ordering among the distance values for each of the attributes. For each value ps_{ij} in matrix PS, where $1 \leq i \leq (n+1)$, the normalized value pd_{ij} is formulated as shown below.

$$pd_{ij} = \frac{(ps_{ij} - P_j^{min})(D^{new\_max} - D^{new\_min})}{(P_j^{max} - P_j^{min})} + D^{new\_min} \tag{10}$$

where P_j^{min} is the minimum value of positive distance and P_j^{max} is the maximum value of positive distance for attribute R_j in matrix PS. The normalized positive distance matrix is:

$$PDP = \begin{bmatrix} pd_{11} & pd_{12} & \dots & pd_{1m} \\ pd_{21} & pd_{22} & \dots & pd_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ pd_{n1} & pd_{n2} & \dots & pd_{nm} \\ pd_{(n+1)1} & pd_{(n+1)2} & \dots & pd_{(n+1)m} \end{bmatrix} \tag{11}$$

For each value ns_{ij} in matrix NS, where $1 \leq i \leq (n+1)$, the normalized value nd_{ij} is formulated as shown below.

$$nd_{ij} = \frac{(ns_{ij} - G_j^{min})(D^{new\_max} - D^{new\_min})}{(G_j^{max} - G_j^{min})} + D^{new\_min} \tag{12}$$

where G_j^{min} is the minimum value of negative distance and G_j^{max} is the maximum value of negative distance for attribute R_j in matrix NS. The normalized negative distance matrix is:

$$NDP = \begin{bmatrix} nd_{11} & nd_{12} & \dots & nd_{1m} \\ nd_{21} & nd_{22} & \dots & nd_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ nd_{n1} & nd_{n2} & \dots & nd_{nm} \\ nd_{(n+1)1} & nd_{(n+1)2} & \dots & nd_{(n+1)m} \end{bmatrix} \tag{13}$$

4.2. Distance based Calculation of Customized Present Trust

Customized present trust of a cloud service is an indication of relative quality of the service at an instant of time, with regard to the expectations of the user. Hence, for effective customized trust assessment of a cloud service, evidence factors need to be evaluated on the basis of their positive and negative distances from the preference values. Consequently, all the m positive distance values in sample i such that $1 \leq i \leq (n+1)$, of matrix PDP, are aggregated based on weights of attributes, to form a summative measure of positive distances, as shown below.

$$SP_i = \sum\nolimits_{j=1}^{m} w_j pd_{ij} \tag{14}$$

where pd_{ij} is a normalized positive distance for attribute R_j in sample i. Similarly, all the m negative distance values in sample i such that $1 \leq i \leq (n+1)$, of matrix NDP, are aggregated based on weights of attributes, to form a summative measure of negative distances, as shown below.

$$SN_i = \sum\nolimits_{j=1}^{m} w_j nd_{ij} \tag{15}$$

where nd_{ij} is a normalized negative distance for attribute R_j in sample i. In Equations (14) and (15), w_j is a weight assigned to cloud service attribute R_j such that $0 < w_j < 1$ and $\sum_{j=1}^{m} w_j = 1$. Static weights are not suitable for effective customized trust assessment of a cloud service. Hence, weights are needed to be computed by taking into consideration the user preferences for various attributes of a cloud service. The details of computation of weights for various cloud service attributes, are described in Section 4.3.

For an evidence sample at time instant i such that $1 \leq i \leq n$, corresponding SP_i from Equation (14) indicates a weighted sum of positive distances of all m evidence factors and corresponding SN_i from Equation (15) indicates a weighted sum of negative distances of all m evidence factors in the sample. When values of evidence factors of a cloud service match the user preferences, then it indicates a good cloud service in terms of meeting the user expectations. If positive distances of evidence factors are higher than the corresponding negative distances, then the cloud service meets the requirements of the user.

Consequently, for an evidence sample at time instant i such that $1 \leq i \leq n$, higher value of summative positive distance (SP_i) signifies the better trustworthiness of a cloud service. Therefore, customized present trust of a cloud service at time instant i, is formulated as a relative share of summative positive distance (SP_i) over SP_i and SN_i.

Definition 3 *Customized Trust value of a cloud service (s_l), at a time instant i, termed as Customized Present Trust (CPT) is defined as:*

$$CPT^i(s_l) = \frac{SP_i}{SP_i + SN_i} \tag{16}$$

where SP_i is a summative positive distance and SN_i is a summative negative distance of evidence factors for all the m attributes of the service, in sample i such that $1 \leq i \leq n$ *and* $0 < CPT^i(s_l) < 1$.

4.3. Computation of Weights

Weight assigned to an attribute signifies the importance of the attribute in trust calculation. Weight of an attribute is computed based on the relative utility of the attribute with respect to preference value of the attribute.

Definition 4 *Utility degree of an attribute R_j, in a time window containing n evidence samples, is formulated as given below.*

$$U(R_j) = (\sum_{i=1}^{n} x_{ij})/y_j \tag{17}$$

where x_{ij} is a normalized evidence factor of attribute R_j at time instant i and y_j is a corresponding normalized preference value for the attribute.

From Equation (17), when all the evidence factors of an attribute in a time window of size n, exactly match with the preference value, utility degree of the attribute becomes equal to n. When one or more evidence factors are less than the specified preference value, utility degree of the attribute reduces to a value which is less than n. Whereas, when utility degree of the attribute goes beyond n, it implies that one or more evidence factors are greater than the preference value. This is the most desirable situation, where the cloud service attribute meets the expected quality requirements. Thus, the values of utility degree for various attributes within a sample, signify the proportionate effect on the weights of cloud service attributes.
Accordingly, weight w_j of an attribute R_j is computed as shown below.

$$w_j = U(R_j)/\sum_{k=1}^{m} U(R_k) \tag{18}$$

where $0 < w_j < 1$ and $\sum_{j=1}^{m} w_j = 1$. Higher is the utility degree $U(R_j)$ of the attribute, greater is its resultant weight. The weights computed using Equation (18), are substituted in Equations (14) and (15), which subsequently results in customized trust estimation of a cloud service, from Equation (16).

4.4. Calculation of Threshold Trust

The preferences for various attributes are in turn used to derive the minimum expected trust value for a cloud service. This trust value is termed as threshold trust value, which serves as a baseline with which computed trust values can be compared. From Equation (14), $SP_{(n+1)}$ indicates a weighted sum of positive distances of preference values of all m attributes and corresponding $SN_{(n+1)}$ from Equation (15), represents a weighted sum of negative distances of preference values of all m attributes. On the lines of CPT in Equation (16), a threshold trust value of a cloud service at the specified preferences, is formulated as a relative share of $SP_{(n+1)}$ over $SP_{(n+1)}$ and $SN_{(n+1)}$, as shown below.

$$T^{pr}(s_l) = \frac{SP_{(n+1)}}{SP_{(n+1)} + SN_{(n+1)}} \tag{19}$$

4.5. Prediction of Cumulative Trust from Customized Present Trust

A set of customized present trust (CPT) values computed at different time instances forms a time series. From Equation (16), at time instant n, time series (CTS) is:

$$CTS = \{CPT^1(s_l), CPT^2(s_l), ..., CPT^n(s_l)\} \tag{20}$$

The time series in Equation (20) is used to predict the future value of trust, termed as cumulative trust.

Definition 5 *Cumulative Trust (CT) of a cloud service (s_l), predicted at a time instant n is defined as:*

$$CT^n(s_l) = \sum\nolimits_{i=1}^{n} w_i^{'} CPT^i(s_l) \tag{21}$$

where $CPT^i(s_l)$ is a customized present trust of cloud service (s_l) at time instant i, $w_i^{'}$ is a weight assigned to it such that $0 < w_i^{'} < 1$ and $\sum_{i=1}^{n} w_i^{'} = 1$.

CPT values at latest time instances, which represent recent quality of a cloud service, are more relevant in prediction of CT, than the CPT values at prior time instances, which represent earlier quality of a cloud service. Hence, exponentially decreasing weights are assigned to the CPT values, starting from the latest CPT value to the CPT values at prior time instances. This is done using a smoothing factor α such that $0 < \alpha < 1$. Thus, the various weights assigned to corresponding CPT values are: $w_n^{'} = \alpha$,$w_{n-1}^{'} = \alpha(1-\alpha)$,. . .,$w_2^{'} = \alpha(1-\alpha)^{n-2}$ and $w_1^{'} = (1-\alpha)^{n-1}$. It is recommended that the value of α should be set in the range from 0.1 to 0.4. This allows the predicted cumulative trust to match closely with the computed customized present trust of the service.

5. ALGORITHM FOR ELASTIC TRUST COMPUTATION

Algorithm 1 shows the steps for elastic trust computation of a cloud service over multiple time windows. The algorithm takes a set of cloud service attributes, a number of time instances and the number of time windows as input for trust assessment of a cloud service. A set of preferences taken as another input indicates the requirements of a particular user about the values of various attributes of a cloud service. The algorithm gives the output as sets of customized present trust and cumulative trust values for service s_l over the time windows. The steps of Algorithm 1 for each time window, are explained as below.

Step 1. (line 7) The evidence factors for the cloud service are acquired and the resultant evidence matrix C is formed, as shown in Equation (1).
Step 2. (line 8) The preferences for service attributes are combined with the evidence matrix, to obtain the augmented matrix CP, as indicated in Equation (2).
Step 3. (line 9) Normalization function takes the augmented matrix as input and transforms all the values in the matrix to uniform range as specified by Equations (3) to (6). It results into the normalized augmented matrix NC as given by Equation (7).
Step 4. (line 10) At this point, the algorithm invokes a function to compute weights for various attributes of the cloud service. The details of the function to compute weights are specified by Algorithm 2 in Section 5.1.
Step 5. (line 11) Here, a function is invoked for computation of distances for the various attributes of the cloud service, from the specified preferences of attributes. The details of the function to compute distances are given by Algorithm 3 in Section 5.2.
Step 6. (lines 12 - 17) At each instant of time, computation of customized present trust is performed based on the

Algorithm 1 Elastic Trust Computation for cloud service s_l

```
 1: Input:
      a. Set of m cloud service attributes, $(AC) = \{R_1, R_2, ..., R_m\}$
      b. Number of time instances (n)
      c. User preferences, $(PR) = \{pr_1, pr_2, ..., pr_m\}$   // Preferences for service attributes
      d. Number of time windows for trust assessment (num_timewindows)
 2: Output:
      a. Set of Customized Present Trust values for service $s_l$, $LP = \{CPT[1], CPT[2], ..., CPT[n]\}$
      b. Set of Cumulative Trust values for service $s_l$, $LC = \{CT[1], CT[2], ..., CT[num\_timewindows]\}$
 3: Begin
 4: $step = n$;
 5: $j = 1$;
 6: while $j \leq num\_timewindows$ do
 7:     Matrix C = Get_evidences($s_l$,AC,n);
 8:     Matrix CP = Get_augmat(C,AC,PR);
 9:     Matrix NC = Normalize_augmat(CP,AC);        // Function $f_{NE}$ in Definition 1
10:     Set W = Compute_weights(NC,AC,n);          // From Algorithm 2, W is a set of weights of m attributes
11:     Matrix PN = Compute_sumdist(NC,AC,n,W);   // Matrix PN of summative distances computed by Algorithm 3
12:     $i = 1$;
13:     while $i \leq n$ do
14:         Compute Customized Present Trust of service $s_l$ at time instant i as: $CPT[i] = \frac{SP_i}{SP_i+SN_i}$;
                          // Function $f_{CPT}$ in Definition 1 and $SP_i$, $SN_i$ are elements of matrix PN
15:         Add $CPT[i]$ in set $LP$;
16:         $i = i + 1$;
17:     end while
18:     Compute Cumulative Trust of service $s_l$ as: $CT[j] = \sum_{i=1}^{n} w_i^{'} CPT[i]$;
                          // Function $f_{CT}$ in Definition 1, $w_i^{'}$ is a weight assigned to $CPT[i]$
19:     Add $CT[j]$ in set $LC$;
20:     PR = Get_updatepref(AC);
21:     $n = n + step$;
22:     $j = j + 1$;
23: end while
24: End
```

summative positive and negative distances of evidence factors. The computed value is added to the output set of customized present trust values. The details of computation of customized present trust are presented in Section 4.2.
Step 7. (lines 18 - 19) Consequently, assessment of cumulative trust is performed for the next time instant by using the customized present trust values of different time instances within a time window. The computed value is added to the output set of cumulative trust values. The details of computation of cumulative trust are elaborated in Section 4.5.
Step 8. (lines 20 - 23) The algorithm, invokes a function to get the changes in preferences of the particular user, for the attributes of a service. The number of time instances for the trust assessment in next time window is updated. Accordingly, the algorithm continues for the reassessment of the trust of the cloud service over subsequent time windows. Thus, the algorithm reflects elastic trust computation of a cloud service according to the dynamically changing preferences of the user over multiple time windows.

5.1. Algorithm for Computation of Weights

Algorithm 2 takes a normalized augmented matrix, a set of cloud service attributes and a number of time instances as input. The algorithm returns the set of weights for the attributes of a cloud service, as the output. As shown in the algorithm, the utility degree for each attribute, is computed. From the values of utility degree, weight of each attribute is computed. The details of computation of weights are presented in Section 4.3.

5.2. Algorithm for Computation of Distances from Preferences

Algorithm 3 takes a normalized augmented matrix, a set of cloud service attributes, a number of time instances and a set of weights for the attributes as input. It in turn, gives a matrix PN of summative positive and negative

Algorithm 2 Computation of weights for the attributes of a cloud service: *Compute_weights(NC,AC,n)*

```
Input:
    a. Matrix $NC = \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1m} \\ x_{21} & x_{22} & \dots & x_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \dots & x_{nm} \\ y_1 & y_2 & \dots & y_m \end{bmatrix}$    // Normalized preference-augmented matrix
    b. Set of m cloud service attributes $(AC) = \{R_1, R_2, ..., R_m\}$
    c. Number of time instances (n)
Output: Set of weights of $m$ attributes, $W = \{w_1, w_2, ..., w_m\}$
Begin
$sum = 0$;
foreach $R_j \in AC$ do
    Compute utility degree as: $UD[j] = (\sum_{i=1}^{n} x_{ij})/y_j$;
    $sum = sum + UD[j]$;
end
$j = 1$;
while $j \leq m$ do
    Compute weight of an attribute $R_j$ as: $w_j = UD[j]/sum$;    // Function $f_{CW}$ in Definition 1
    Add $w_j$ in set W;
    $j = j + 1$;
end while
End
```

distances for the samples of evidences, as the output. The details of computation of summative positive and negative distances are presented in Sections 4.1 and 4.2.

Algorithm 3 Computation of summative distances for cloud service attributes: *Compute_sumdist(NC,AC,n,W)*

```
Input:
    a. Normalized preference-augmented matrix (NC)
    b. Set of m cloud service attributes, $(AC) = \{R_1, R_2, ..., R_m\}$
    c. Number of time instances (n)
    d. Set $W = \{w_1, w_2, ..., w_m\}$    // Weights of m attributes from Algorithm 2
Output: Matrix of summative distances, $PN = \begin{bmatrix} SP_1 & SP_2 & \dots & SP_n & SP_{(n+1)} \\ SN_1 & SN_2 & \dots & SN_n & SN_{(n+1)} \end{bmatrix}$
Begin
Compute positive distances from preferences as: Matrix PS = Compute_pdist(NC,AC);
Compute negative distances from preferences as: Matrix NS = Compute_ndist(NC,AC);
Matrix PDP = Normalize_pdist(PS,AC);
Matrix NDP = Normalize_ndist(NS,AC);
$i = 1$;
while $i \leq (n + 1)$ do
    Compute summative positive distance as: $SP_i = \sum_{j=1}^{m} w_j pd_{ij}$;    // $pd_{ij}$ is an element of matrix PDP
    Compute summative negative distance as: $SN_i = \sum_{j=1}^{m} w_j nd_{ij}$;    // $nd_{ij}$ is an element of matrix NDP
    Add $SP_i$ and $SN_i$ in matrix PN;
    $i = i + 1$;
end while    // Functions $f_{PD}$, $f_{ND}$ in Definition 1
End
```

5.3. Computational Complexity of Trust Assessment

For a given time window, the details of computational complexity of various operations in Algorithm 1, are explained as follows. The computational complexity of a function to get the evidence factors is $O(mn)$. The computational complexity of a function to form the augmented matrix is $O(m)$. The function for normalization of augmented matrix has the complexity of $O(mn)$. Computation of customized present trust has the complexity of $O(n)$. The computational complexity for assessment of cumulative trust is $O(n)$. The function to get changes in user preferences has the complexity of $O(m)$. From Algorithm 2, computation of weights has the complexity of $O(mn)$. As shown by the steps in Algorithm 3, computation of summative positive and negative distances has the complexity of $O(mn)$. Hence, the overall computational complexity (CC) of trust assessment (including Algorithm 1, Algorithm 2 and Algorithm 3) is given as below:

$$CC = O(mn) + O(m) + O(n) = O(mn) \tag{22}$$

From Equation (22), the computational complexity of trust assessment is fairly good and it depends on the number of cloud service attributes (m) and the number of time instances (n).

6. TRUST BASED RANKING OF CLOUD SERVICES

As described in Section 4, the proposed trust model PBCTM computes the customized present trust of a cloud service based on the user preferences for various service attributes. Cumulative trust of a cloud service at a certain time instant is predicted using the customized present trust values of the service at different time instances. Consequently, the functionally equivalent cloud services can be compared based on the corresponding cumulative trust values. The cloud services are ranked based on the cumulative trust values where the service with the highest trust value, is assigned the first rank position. Thus, PBCTM can be applied for the trust based ranking of services, which in turn facilitates the user to select the most trustworthy cloud service.

Table 2 shows the customized present trust values, computed for functionally similar cloud services. At position l such that $1 \leq l \leq v$, a row in the table indicates a sample of customized present trust values for cloud service (s_l) as $\{CPT^1(s_l), CPT^2(s_l), ..., CPT^n(s_l)\}$ and each value $CPT^i(s_l)$, in the sample denotes a customized present trust at time instant i in a time window, such that $1 \leq i \leq n$.

Table 2. Customized Present Trust (CPT) for Cloud Services

Cloud Service	CPT at time instant 1	CPT at time instant 2	...	CPT at time instant n
s_1	$CPT^1(s_1)$	$CPT^2(s_1)$	...	$CPT^n(s_1)$
s_2	$CPT^1(s_2)$	$CPT^2(s_2)$	...	$CPT^n(s_2)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
s_v	$CPT^1(s_v)$	$CPT^2(s_v)$	...	$CPT^n(s_v)$

The cumulative trust for each cloud service (s_l) where $1 \leq l \leq v$, in Table 2, is computed using Equation (21), where for all n time instances, the corresponding CPT values with associated weights are aggregated. Thus, Table 3 shows the cumulative trust values for the cloud services. The services can now be compared and ranked on the basis of predicted cumulative trust values. This reflects a customized ranking of cloud services with respect to the current preferences of the user which enables the user to select the suitable cloud service which closely meets the user expectations. Over a period of time, with changes in the preferences of the user, PBCTM enables to perform the revised ranking of cloud services. This facilitates the user to revise the selection of a suitable service based on the updated ranking of cloud services.

Table 3. Cumulative Trust for Cloud Services

Cloud Service	Cumulative Trust
s_1	$CT^n(s_1)$
s_2	$CT^n(s_2)$
$\vdots$	$\vdots$
s_v	$CT^n(s_v)$

7. QUALITATIVE COMPARISON OF PBCTM WITH OTHER TRUST MODELS

The details of our proposed trust model PBCTM are elaborated at length in Sections 4, 5 and 6. The qualitative comparison of PBCTM with other QoS based models [23, 24, 25, 27, 28] is presented in Table 4. These trust models [23, 24, 25, 27, 28] are discussed in Section 2.

Table 4. Qualitative Comparison of Cloud Trust Models

Reference	Factors used for trust assessment	Dynamic trust update	Customized trust assessment	Elastic trust computation
Fan et al. 2015 [23]	Subjective user feedbacks	Considered	With user assigned subjective weights to service attributes.	Not considered
Li et al. 2015 [24]	Monitoring based multiple attributes	Considered	Not considered	Not considered
Sidhu and Singh 2016 [25]	Monitoring based QoS attributes	Not considered	Not considered	Not considered
Supriya et al. 2016 [27]	Service provider attributes	Not considered	With user priority based subjective weights for attributes.	Not considered
Manuel 2013 [28]	Measurement based QoS attributes	Considered	With pre-decided user priority based static weights for QoS attributes.	Not considered
Our model - PBCTM	Evidence factors of multiple QoS attributes	Prediction of cumulative trust over a period of time, enables ranking and periodic selection of cloud services.	Trust computation is based on the distances of service evidences from user preferences. Weights of attributes are computed dynamically, based on relative utility of attributes with respect to user preferences.	The model enables trust computation according to elastic input, which means as per dynamically changing preferences of the user with time.

PBCTM performs customized trust assessment of a cloud service by taking into account the preferences of a cloud user for service attributes and the evidence factors of the service. Table 4 indicates that, user preferences based customized trust assessment, periodic ranking of cloud services based on dynamic trust prediction and elastic trust computation are the distinguishing features of PBCTM, in comparison to the other models. Section 8 presents the quantitative comparison of PBCTM with the other model.

8. PERFORMANCE EVALUATION

A prototype is developed in Java for our trust model PBCTM, which facilitates the computation of CPT and CT values by calculating the weights and distances for service attributes. This prototype is used for experimentation and performance evaluation. As discussed in Section 2, attributes which include availability, throughput, response time and security are the relevant attributes of a cloud service, used for trust assessment. Typically, these are the quality attributes, which user commonly expects from a cloud service. Hence, these four attributes are used during the experimentation. For the values of throughput (kbps) and response time (seconds), real world QoS data set [29] is referred. The availability implies the percentage of time the cloud service is accessible. Security attribute is considered as the percentage of the number of violation incidents related to authentication or authorization. Weibull distribution is the suitable theoretical distribution for modeling failure time and can also be employed for modeling inputs in the absence of real data [30]. Hence, values of availability (%) and security violation incidents (%) are generated using the Weibull distribution. Various values of the attributes are normalized in the range [0.01, 0.99]. For a cloud service, higher values of availability and throughput are desired. Hence, values of these attributes along with the corresponding specified preferences are normalized using Equations (3) and (4). Whereas, lower values of response time and security violation incidents are expected. Hence, values of these attributes as well as the corresponding given preferences are normalized using Equations (5) and (6).

8.1. Evaluation Metrics

The effectiveness of trust evaluation method depends on the accuracy of trust assessment. Mean Absolute Error (MAE) [31] is a metric to assess an error in the prediction process. Here it is applied to compute an error in the prediction of cumulative trust and thus, to evaluate the accuracy of trust assessment. Consequently, MAE is formulated as below.

$$MAE = \frac{1}{n}(\sum_{i=1}^{n} |P^{i+1}(s_l) - C^i(s_l)|) \tag{23}$$

where $P^{i+1}(s_l)$ is customized present trust of a cloud service (s_l) at time instant $(i+1)$, $C^i(s_l)$ is a predicted cumulative trust of a cloud service (s_l) at time instant *i* and n is the total number of time instances for assessment of MAE. Smaller value of MAE indicates higher accuracy of trust assessment and hence better performance of the trust model.

Along with the accuracy in the calculation, trust model should comply to user requirements about the expected quality of cloud service. Accordingly, trust model should be able to accomplish the task of efficient trust assessment by taking into account the preferences of user for the various attributes of a cloud service. Hence, Satisfaction Index (SI) is defined as a metric to assess the degree to which the predicted cumulative trust of a cloud service meets the minimum expected trust value with regard to the specified preferences.

Definition 6 *Satisfaction Index (SI) for trust assessment of a cloud service (s_l) at time instant n is defined as below.*

$$SI = \frac{C^n(s_l)}{TH(s_l)} \tag{24}$$

where $C^n(s_l)$ is a predicted cumulative trust of a cloud service (s_l) at time instant n and $TH(s_l)$ is a threshold trust value at the specified preferences for service (s_l). When cumulative trust exactly matches the threshold trust value, then SI becomes equal to 1. When cumulative trust exceeds the threshold trust value, then SI value goes beyond 1. A higher value of SI implies a better degree of satisfaction and hence effective trust estimation of a cloud service from the perspective of a user.

8.2. Trust Model for Comparison

In addition to our trust model PBCTM, one more trust model, called averaging based trust model (ABTM) has also been implemented for comparative assessment. This trust model also makes use of multiple cloud QoS attributes for trust evaluation. ABTM is based on the methods, which coincide with the existing trust models in the literature. The selection of ABTM model has been done to facilitate the comparison of performance of PBCTM with other relevant models from two perspectives: i) To compare with the model where weights assigned to the various factors for trust assessment are static and subjective in nature. Thus, in ABTM, equal weights are assigned to all the factors. Here, ABTM is analogous to the model proposed by Manuel [28]. ii) To compare with the model where trust values of multiple services are computed with the commonly used method called Technique for Ordering Preference by Similarity to Ideal Solution (TOPSIS) [27]. Thus, in ABTM, TOPSIS method is used for assessment of cumulative trust values of services. Here, ABTM corresponds to the model proposed by Supriya et al. [27]. The trust models [27, 28] are discussed in Section 2. In ABTM, customized present trust (CPT) of a cloud service (s_l) is computed as an average of all m evidence factors at a time instant i. It is given by:

$$AT^i(s_l) = (\sum_{j=1}^{m} x_{ij})/m \tag{25}$$

where x_{ij} is a normalized evidence factor of attribute R_j at time instant *i*, such that $1 \leq i \leq n$. Threshold Trust value is calculated as an average of preference values of all m attributes, given as:

$$T(s_l) = (\sum_{j=1}^{m} y_j)/m \tag{26}$$

where y_j is a normalized preference value of attribute R_j. From all the n distinct CPT values, each represented by $AT^i(s_l)$ such that $1 \leq i \leq n$, Cumulative Trust (CT) at time instant n is calculated using the TOPSIS [27] method. Here, an average weight $(\frac{1}{n})$ is assigned to each of the n values of CPT of a cloud service.

8.3. Results and Analysis

The performance of our trust model PBCTM is evaluated in terms of the accuracy and degree of satisfaction of trust assessment, in absolute and comparative forms. For this purpose, four experiments are conducted. In experiments 1 and 2, the number of evidence samples for a cloud service is varied from 20 to 200. The preferences for cloud service attributes are assigned representative values for illustration. The values for availability (%), throughput (kbps), response time (seconds) and security violation incidents (%) are considered, respectively in set PR of preferences. PR is taken as $\{90, 1.5, 1.8, 8\}$ for first three experiments. The details of experiments are discussed in the following subsections.

8.3.1. Assessment of Accuracy of Trust Estimation

The evaluation of accuracy of trust estimation is performed by observing MAE values of PBCTM and comparing them with those of ABTM. The results of first experiment are shown in Figure 2. The MAE values of PBCTM range from 0.1139 to 0.1804. Consequently, accuracy of PBCTM ranges from 81.96 to 88.61%. Thus, it is clear that accuracy of our trust model is significantly high. The MAE values of ABTM range from 0.1947 to 0.2834. Consequently, accuracy of ABTM ranges from 71.66 to 80.53%. This implies that MAE values of our trust model are much less than those of ABTM and accuracy of PBCTM is higher than ABTM by 12.32% on an average. This signifies that, the performance of PBCTM in terms of accuracy is better than that of the other model for various number of samples of service attributes.

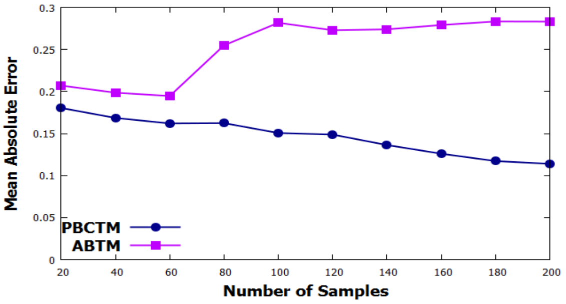


Figure 2. MAE for trust estimation of cloud service (Experiment 1)

8.3.2. Assessment of Degree of Satisfaction of Trust Estimation

The evaluation of degree of satisfaction of trust estimation is performed by observing SI values of PBCTM and comparing them with those of ABTM. The results of second experiment are shown in Figure 3. The SI values of PBCTM range from 1.0235 to 1.6038. Thus, it is clear that degree of satisfaction of our trust model is significantly high, as SI value goes beyond 1.0. The SI values of ABTM range from 0.4775 to 0.8283. This implies that SI of our trust model is higher than that of ABTM by 43.91% on an average. Hence, degree of satisfaction of trust estimation for PBCTM is much better than ABTM. This signifies that, the performance of PBCTM in terms of degree of satisfaction is better than that of ABTM for various number of samples of service attributes.

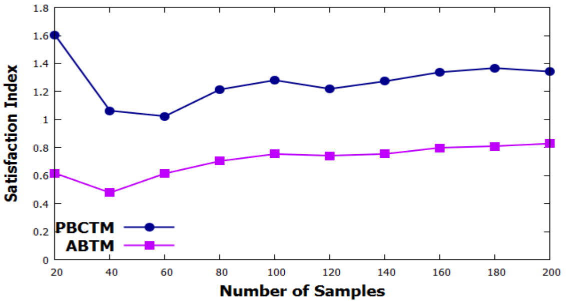


Figure 3. SI for trust estimation of cloud service (Experiment 2)

8.3.3. Validation of Trust based Ranking of Cloud Services

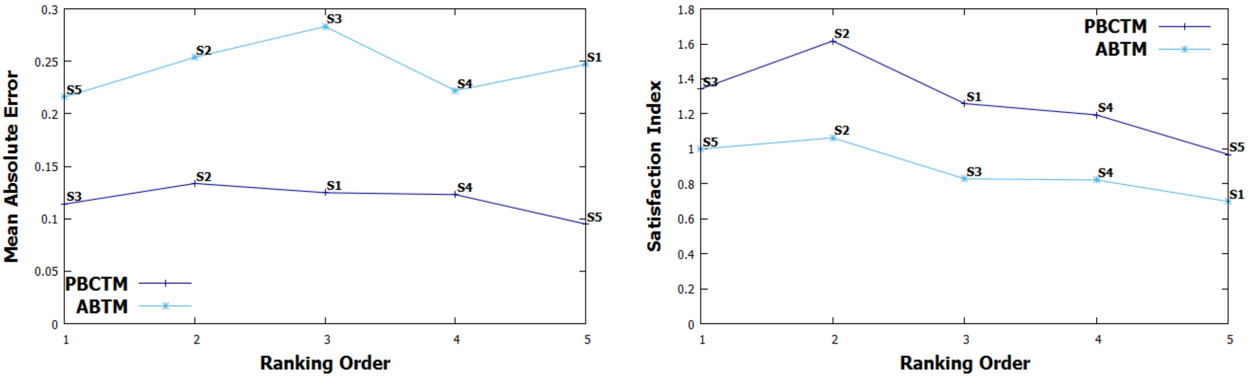
The effectiveness of PBCTM for trust based ranking of cloud services is validated in terms accuracy and degree of satisfaction of trust estimation at each rank position. For the third experiment, five cloud services are considered and 200 evidence samples for each of the services are taken for trust assessment. At a sample count 200, Table 5 shows the calculated cumulative trust (CT) values of cloud services by the two trust models.

Table 5. Cumulative Trust

Cloud Service	CT by PBCTM	CT by ABTM
s_1	0.818829	0.489494
s_2	0.858223	0.601331
s_3	0.862221	0.580572
s_4	0.721482	0.532119
s_5	0.58538	0.656096

Based on the respective CT values of the two trust models in Table 5, the ranking of services is done. Here, s_3 is the highest ranked service by PBCTM, whereas s_5 is the highest ranked service by ABTM.

In part (A) of third experiment, comparative evaluation of accuracy of trust estimation is performed by observing MAE values of two trust models for cloud services at each rank position. Figure 4a shows the observed MAE values for rank wise ordered services of two trust models. The MAE value of PBCTM at rank position 1 is 0.1139, consequently, accuracy is 88.61%. Whereas, the MAE value of ABTM is 0.2159, consequently, accuracy is 78.41%. Thus, accuracy of our model is higher than that of the other model by 11.51%. Similar calculations are done for other rank positions and % comparative values for accuracy are given in Table 6.



(a) MAE

(b) SI

Figure 4. MAE and SI for trust based ranking (Experiment 3A and 3B)

In part (B) of third experiment, comparative evaluation of degree of satisfaction of trust estimation is performed by observing SI values of two trust models for cloud services at each rank position. Figure 4b shows the observed SI values for rank wise ordered services of two trust models. The SI value of PBCTM at rank position 1 is 1.3425 and that of ABTM is 0.9986. Thus, SI of our model is higher than that of the other model by 25.62%. Similar calculations are done for other rank positions and % comparative values for SI are given in Table 6.

Table 6. Comparative Results for Figures 4a and 4b

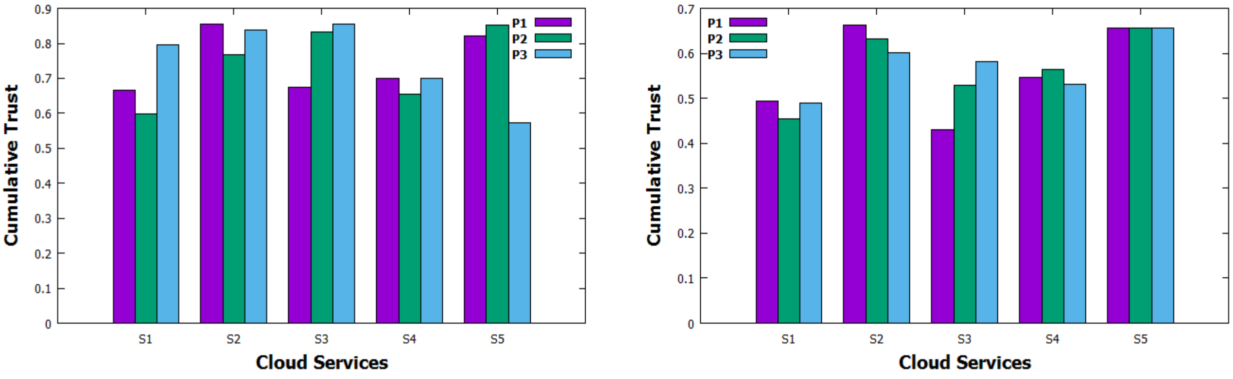
Rank	Cloud Service by PBCTM	Cloud Service by ABTM	Higher Accuracy % over ABTM	Higher SI % over ABTM
1	s_3	s_5	11.51	25.62
2	s_2	s_2	13.88	34.28
3	s_1	s_3	18.10	34.18
4	s_4	s_4	11.30	31.19
5	s_5	s_1	16.80	27.80

The results in Table 6 show that accuracy of PBCTM at each rank position is much higher than that of ABTM. Also, SI of PBCTM at each rank position is much higher than that of ABTM and hence degree of satisfaction of trust estimation for PBCTM is much better than that of ABTM. Therefore, PBCTM is effective for trust based ranking of cloud services over ABTM. The above results of better degree of satisfaction for PBCTM, depict that if PBCTM is used for service selection, then the selected cloud service closely matches the user expectations.

8.3.4. Validation of Trust based Ranking with Changing Requirements

In the fourth experiment, changes in requirements of the user are demonstrated by considering three sets (PR) of preferences at three distinct sample counts (n). The three groups are categorized as below.

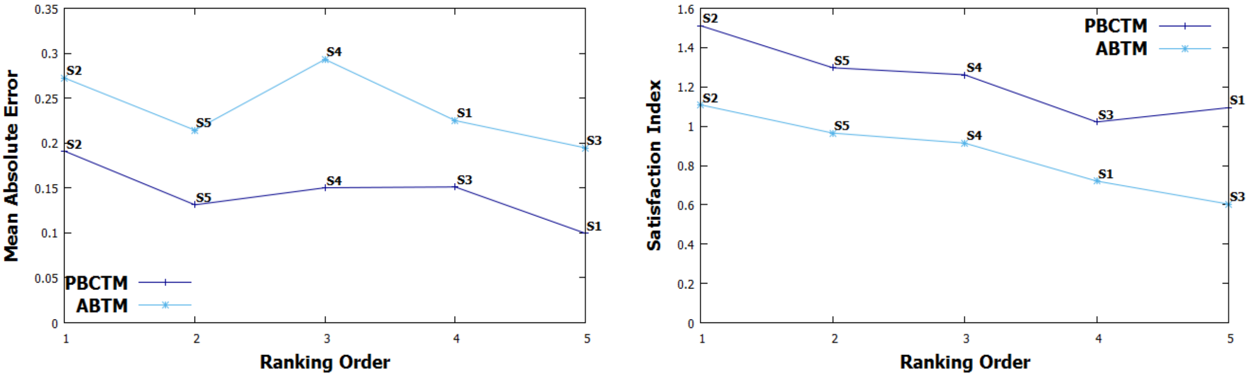
Experiment 4A - Group P1: $n = 60$, $PR = \{92, 1.8, 1.5, 10\}$
Experiment 4B - Group P2: $n = 100$, $PR = \{95, 2, 1.2, 8\}$
Experiment 4C - Group P3: $n = 200$, $PR = \{98, 2.1, 1, 6\}$



(a) PBCTM (b) ABTM

Figure 5. CT of services for PBCTM and ABTM with Groups P1, P2, P3

During experimentation, five cloud services are considered. For each of these services, the number of samples is selected as 60, 100 and 200, as specified above, in the three parts of the experiment. The cumulative trust (CT) values of cloud services are calculated, by the two trust models for groups P1, P2, and P3. Accordingly graphs of Figures 5a and 5b are plotted. Based on respective CT values of the two trust models, as shown in Figures 5a and 5b, the ranking of services is carried out.



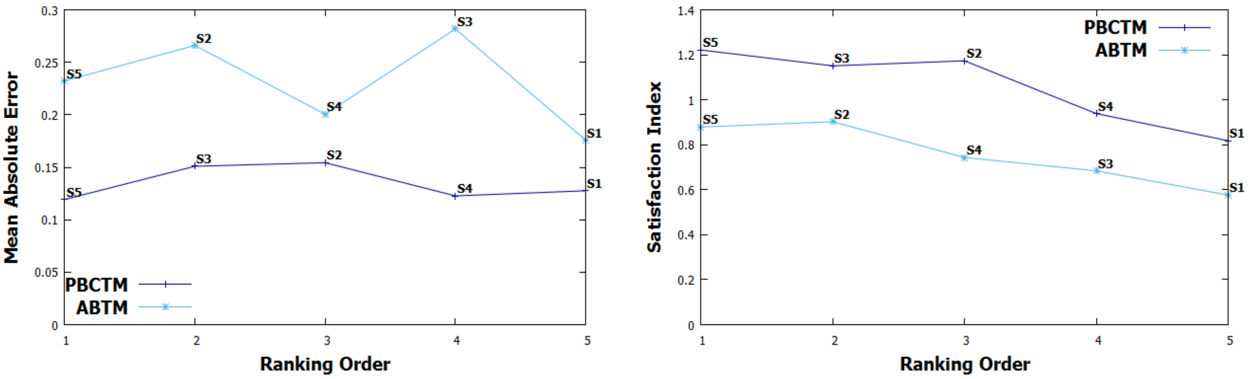
(a) MAE (b) SI

Figure 6. MAE and SI for Group P1 (Experiment 4A)

In part (A) of forth experiment, group P1 is considered. Comparative evaluation of accuracy of trust estimation is performed by observing MAE values of two trust models for cloud services at each rank position. Figure 6a shows the observed MAE values for rank wise ordered services of two trust models. The MAE value of PBCTM at rank position 1 is 0.1910, consequently, accuracy is 80.9%. Whereas, the MAE value of ABTM is 0.2724, consequently, accuracy is 72.76%. Thus, accuracy of our model is higher than that of the other model by 10.06%. The same method is followed for calculations at other rank positions and % comparative values for accuracy are given in Table 7. Similar to group P1, Figures 7a and 8a show the observed MAE values for rank wise ordered services of two trust models, for groups P2 and P3, in part (B) and (C) respectively. On the lines of group P1, calculations for accuracy are done at all the rank positions and % comparative values for accuracy are given in Tables 8 and 9 respectively.

Table 7. Comparative Results for Group P1 (Experiment 4A)

Rank	Cloud Service by PBCTM	Cloud Service by ABTM	Higher Accuracy % over ABTM	Higher SI % over ABTM
1	s_2	s_2	10.06	26.64
2	s_5	s_5	9.57	25.64
3	s_4	s_4	16.82	27.56
4	s_3	s_1	8.71	29.46
5	s_1	s_3	10.57	44.83



(a) MAE

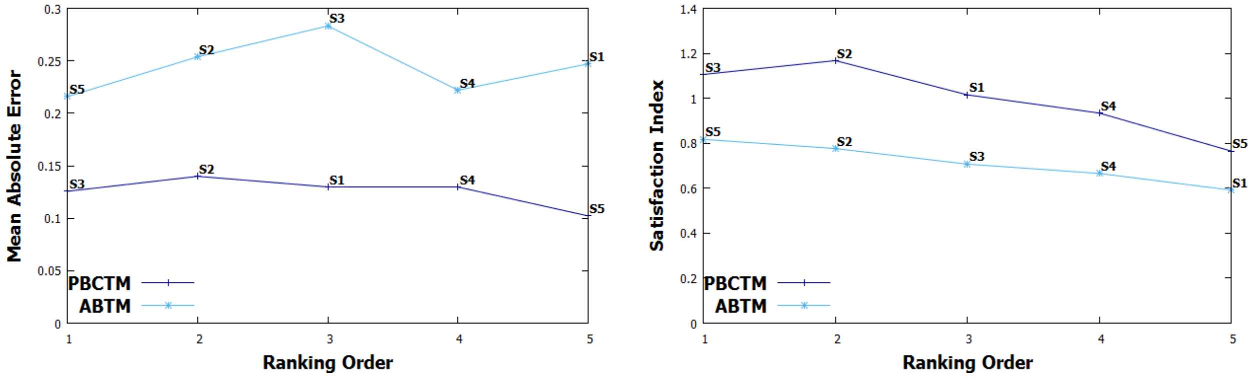
(b) SI

Figure 7. MAE and SI for Group P2 (Experiment 4B)

Comparative evaluation of degree of satisfaction of trust estimation is performed by observing SI values of two trust models for cloud services at each rank position. Figure 6b shows the observed SI values for rank wise ordered services of two trust models, for group P1. The SI value of PBCTM at rank position 1 is 1.5112 and that of ABTM is 1.1086. Thus, SI of our model is higher than that of the other model by 26.64%. The same method is followed for calculations at other rank positions and % comparative values for SI are given in Table 7. Similar to group P1, Figures 7b and 8b show the observed SI values for rank wise ordered services of two trust models, for groups P2 and P3 respectively. On the lines of group P1, calculations for SI are done at all the rank positions and % comparative values for SI are given in Tables 8 and 9 respectively.

Table 8. Comparative Results for Group P2 (Experiment 4B)

Rank	Cloud Service by PBCTM	Cloud Service by ABTM	Higher Accuracy % over ABTM	Higher SI % over ABTM
1	s_5	s_5	12.84	28.05
2	s_3	s_2	13.56	21.59
3	s_2	s_4	5.46	36.63
4	s_4	s_3	18.13	27.12
5	s_1	s_1	5.54	29.51



(a) MAE (b) SI

Figure 8. MAE and SI for Group P3 (Experiment 4C)

Table 9. Comparative Results for Group P3 (Experiment 4C)

Rank	Cloud Service by PBCTM	Cloud Service by ABTM	Higher Accuracy % over ABTM	Higher SI % over ABTM
1	s_3	s_5	10.33	26.12
2	s_2	s_2	13.25	33.50
3	s_1	s_3	17.65	30.35
4	s_4	s_4	10.62	28.73
5	s_5	s_1	16.13	22.69

The results in each of the Tables 7, 8 and 9 show that i) Accuracy of PBCTM at each rank position is much higher than that of ABTM ii) SI of PBCTM at each rank position is much higher than that of ABTM and hence degree of satisfaction of trust estimation for PBCTM is much better than that of ABTM. This confirms the effectiveness of PBCTM for trust based ranking of cloud services, for the varying combinations of sample counts and preferences, corresponding to the groups P1, P2 and P3.

Summary of results of experiments 4A, 4B and 4C is shown in Table 10. Table 10 is derived from average values of relative accuracy and SI in Tables 7, 8 and 9. From Table 10, it is clear that our model PBCTM is superior to ABTM in terms of accuracy and degree of satisfaction of trust assessment.

Table 10. Summary of Results

Group	n	PR	Ranking by PBCTM	Ranking by ABTM	Higher Accuracy % over ABTM	Higher SI % over ABTM
P1	60	$\{92, 1.8, 1.5, 10\}$	$s_2\ s_5\ s_4\ s_3\ s_1$	$s_2\ s_5\ s_4\ s_1\ s_3$	11.15	30.83
P2	100	$\{95, 2, 1.2, 8\}$	$s_5\ s_3\ s_2\ s_4\ s_1$	$s_5\ s_2\ s_4\ s_3\ s_1$	11.12	28.58
P3	200	$\{98, 2.1, 1, 6\}$	$s_3\ s_2\ s_1\ s_4\ s_5$	$s_5\ s_2\ s_3\ s_4\ s_1$	13.6	28.28

The results in Table 10 show that, with each combination of sample count and preferences, a distinct ranking sequence of cloud services is obtained by PBCTM. This distinct ranking sequence is a more closely match to user requirements. This is due to the methodology of our trust model which incorporates the dynamically varying user preferences in computation of weights of various service attributes. It can be inferred that user preferences based weights are significant and need to be considered in trust assessment to enable the selection of suitable cloud service which closely matches the user expectations.

Figure 5a clearly shows the updated cumulative trust (CT) values of the services for PBCTM, with changes in sample count and preferences. Thus, for group P1, S2 is the most trustworthy cloud service, whereas S5 is for group P2 and for group P3, S3 is the highest trustworthy cloud service. This exhibits a better degree of responsiveness of our trust model to the changing requirements of the user, implying the advantage of elastic trust computation capability. Thus, at every combination of sample count and preferences, PBCTM facilitates the selection of suitable service on the basis of dynamic and elastic trust assessment. On the other hand, in ABTM, from Figure 5b, changes in the CT

values of the services with changes in sample count and preferences, are not clearly distinguishable. This is due to the averaging approach used in ABTM, which is independent of the preferences. Consequently, as indicated by the results in Table 10, ABTM ranks the same S5 and S2 services as the first two trustworthy services, for both, group P2 as well as P3. Moreover, from Table 10, although, services S2, S5 and S4 are the first three services in ranking for group P1 by both, PBCTM and ABTM, the corresponding accuracy and degree of satisfaction of PBCTM are much higher than those of ABTM.

For the purpose of experimentation and performance analysis, five cloud services have been considered in trust based ranking. However, as elaborated in Sections 4 and 6, the methodology of PBCTM is independent of number of services. Similarly, for the purpose of demonstration, we have used three combinations of sample counts and set of preferences. However, preferences can change dynamically with time, over a long duration. Therefore, PBCTM incorporates these changing preferences over time and facilitates the elastic trust computation of a cloud service.

In summary, experimental results have shown that, performance of PBCTM is superior to the other model, in terms of accuracy and degree of satisfaction of trust assessment of a cloud service. When applied for trust based ranking of multiple cloud services, results have demonstrated that, accuracy and degree of satisfaction of trust estimation for PBCTM, at each rank position are much better than those of the other model. Moreover, PBCTM demonstrates a better degree of responsiveness to the changing requirements of the user. Results have also shown that, even with the dynamically varying preferences of the user, accuracy and degree of satisfaction of trust assessment for PBCTM are superior to the other model. This implies that, PBCTM can be effectively applied in practice to enable the periodic selection of appropriate cloud services, based on dynamic and elastic trust computation.

9. CONCLUSION

In this paper, we presented the preferences based customized trust model (PBCTM) and the mechanism for trust based ranking of cloud services. The model offers customized trust assessment of a cloud service where weights assigned to the various QoS attributes are computed based on the user preferences for the attributes. A novel method based on the positive and negative distances of various evidence factors from the preferences, is presented for computation of customized present trust of a cloud service. The newly introduced notion of elastic trust computation depicts the trust assessment of a cloud service according to dynamically changing user preferences with time. The algorithm has been presented for elastic trust computation of a cloud service. Dynamic prediction of trust in the form of cumulative trust over a period of time, is used to rank the cloud services. The cloud user can select the suitable cloud service based on ranking of the services.

Experimental results have shown that, performance of PBCTM is significantly high and is superior to the other model in terms of accuracy and newly proposed metric of degree of satisfaction of trust assessment. In conclusion, our trust model PBCTM depicts effective trust assessment and ranking of cloud services which enable to closely meet the user expectations.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the anonymous reviewers for their valuable comments. Sincere thanks are also due to College of Engineering Pune and Cummins College of Engineering for Women, Pune, India.

REFERENCES

[1] S. Roy, P. K. Pattnaik, and R. Mall, “A cognitive approach for evaluating the usability of storage as a service in cloud computing environment,” *International Journal of Electrical and Computer Engineering*, vol. 6, no. 2, p. 759, 2016.

[2] S. N. Ogirala, T. Kumar, and V. R. Vedula, “A survey on security aspects of server virtualization in cloud computing,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 3, 2017.

[3] C. N. Sahoo and V. Goswami, “Dynamic control and resource management for mission critical multi-tier applications in cloud data center,” *International Journal of Electrical and Computer Engineering*, vol. 6, no. 3, p. 1023, 2016.

[4] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, “Trust management of services in cloud environments: Obstacles and solutions,” *ACM Computing Surveys (CSUR)*, vol. 46, no. 1, p. 12, 2013.

[5] I. M. Abbadi and A. Martin, “Trust in the cloud,” *information security technical report*, vol. 16, no. 3, pp. 108–114, 2011.

[6] S. M. Habib, S. Ries, and M. Mühlhäuser, “Cloud computing landscape and research challenges regarding trust and reputation,” in *Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic &*

Trusted Computing (UIC/ATC'10). IEEE, 2010, pp. 410–415.

[7] S. Potluri and K. S. Rao, "Quality of service based task scheduling algorithms in cloud computing," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 2, 2017.

[8] J. Huang and D. M. Nicol, "Trust mechanisms for cloud computing," *Journal of Cloud Computing*, vol. 2, no. 1, pp. 1–14, 2013.

[9] S. M. Habib, S. Hauke, S. Ries, and M. Mühlhäuser, "Trust as a facilitator in cloud computing: a survey," *Journal of Cloud Computing*, vol. 1, no. 1, pp. 1–18, 2012.

[10] S. M. Habib, S. Ries, and M. Mühlhäuser, "Towards a trust management system for cloud computing," in *10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'11).* IEEE, 2011, pp. 933–939.

[11] C. Qu and R. Buyya, "A cloud trust evaluation system using hierarchical fuzzy inference system for service selection," in *28th International Conference on Advanced Information Networking and Applications (AINA'14).* IEEE, 2014, pp. 850–857.

[12] A. V. Dastjerdi and R. Buyya, "A taxonomy of qos management and service selection methodologies for cloud computing," *Cloud Computing: Methodology, Systems, and Applications*, pp. 109–131, 2011.

[13] T. H. Noor and Q. Z. Sheng, "Credibility-based trust management for services in cloud environments," in *9th International Conference on Service-Oriented Computing (ICSOC'11).* Springer, 2011, pp. 328–343.

[14] ——, "Trust as a service: a framework for trust management in cloud environments," in *12th International Conference on Web Information System Engineering (WISE'11).* Springer, 2011, pp. 314–321.

[15] J. Abawajy, "Establishing trust in hybrid cloud computing environments," in *10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'11).* IEEE, 2011, pp. 118–125.

[16] S. Deshpande and R. Ingle, "Trust assessment in cloud environment: Taxonomy and analysis," in *International Conference on Computing, Analytics and Security Trends (CAST).* IEEE, 2016, pp. 627–631.

[17] P. S. Pawar, M. Rajarajan, S. K. Nair, and A. Zisman, "Trust model for optimized cloud services," in *Trust Management VI.* Springer, 2012, pp. 97–112.

[18] N. Ghosh, S. K. Ghosh, and S. K. Das, "Selcsp: A framework to facilitate selection of cloud service providers," *Cloud Computing, IEEE Transactions on*, vol. 3, no. 1, pp. 66–79, 2015.

[19] F. Moyano, K. Beckers, and C. Fernandez-Gago, "Trust-aware decision-making methodology for cloud sourcing," in *26th International Conference on Advanced Information Systems Engineering (CAiSE'14).* Springer, 2014, pp. 136–149.

[20] P. D. Manuel, S. T. Selvi, and M. I. Abd-El Barr, "Trust management system for grid and cloud resources," in *First International Conference on Advanced Computing (ICAC'09).* IEEE, 2009, pp. 176–181.

[21] P. D. Manuel, M. I. Abd-El Barr, and S. T. Selvi, "A novel trust management system for cloud computing iaas providers," *JCMCC-Journal of Combinatorial Mathematicsand Combinatorial Computing*, vol. 79, p. 3, 2011.

[22] Y. Huo, Y. Zhuang, and S. Ni, "Fuzzy trust evaluation based on consistency intensity for cloud services," *Kybernetes*, vol. 44, no. 1, pp. 7–24, 2015.

[23] W. J. Fan, S. L. Yang, H. Perros, and J. Pei, "A multi-dimensional trust-aware cloud service selection mechanism based on evidential reasoning approach," *International Journal of Automation and Computing*, vol. 12, no. 2, pp. 208–219, 2015.

[24] X. Li, H. Ma, F. Zhou, and X. Gui, "Service operator-aware trust scheme for resource matchmaking across multiple clouds," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1419–1429, 2015.

[25] J. Sidhu and S. Singh, "Improved topsis method based trust evaluation framework for determining trustworthiness of cloud service providers," *Journal of Grid Computing*, pp. 1–25, 2016.

[26] S. Singh and J. Sidhu, "Compliance-based multi-dimensional trust evaluation system for determining trustworthiness of cloud service providers," *Future Generation Computer Systems*, vol. 67, pp. 109–132, 2017.

[27] M. Supriya, K. Sangeeta, and G. K. Patra, "Trustworthy cloud service provider selection using multi criteria decision making methods." *Engineering Letters*, vol. 24, no. 1, 2016.

[28] P. Manuel, "A trust model of cloud computing based on quality of service," *Annals of Operations Research*, pp. 1–12, 2013.

[29] Y. Zhang, Z. Zheng, and M. R. Lyu, "Wspred: A time-aware personalized qos prediction framework for web services," in *22nd International Symposium on Software Reliability Engineering (ISSRE'11).* IEEE, 2011, pp. 210–219.

[30] A. M. Law, *Simulation modeling and analysis*, 4th ed. McGraw-Hill, 2015.

[31] C. Chatfield, *Time-series forecasting*. CRC Press, 2000.

BIOGRAPHIES OF AUTHORS

Shilpa Deshpande is a research scholar at College of Engineering Pune, Savitribai Phule Pune University, India. She is currently an Assistant Professor with the Computer Engineering Department, Cummins College of Engineering for Women, Pune. She has received the Bachelor's degree and the Master's degree in Computer Engineering from Savitribai Phule Pune University, in 1996 and in 2002 respectively. Her research interests are in the area of cloud computing and distributed systems.

Rajesh Ingle is an Adjunct Professor at Department of Computer Engineering, College of Engineering Pune, India. He is a Professor at Department of Computer Engineering, Pune Institute of Computer Technology, Pune. He has received Ph.D. Computer Science and Engineering from Department of Computer Science and Engineering, Indian Institute of Technology Bombay, Powai, Mumbai. He has received the B.E. Computer Engineering from Pune Institute of Computer Technology and M.E. Computer Engineering from Government College of Engineering, Savitribai Phule Pune University. He has also received M.S. Software Systems from BITS, Pilani, India. His research interests include Distributed system security and Cloud security. He is a senior member of the IEEE, IEEE Communications Society and IEEE Computer Society. He is also a chairman IEEE R10 SAC.