IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 8, 2020, accepted February 25, 2020, date of publication March 4, 2020, date of current version March 12, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2978452

Enhanced QoS-Based Model for Trust Assessment in Cloud Computing Environment

HALA HASSAN[1], ALI IBRAHIM EL-DESOUKY[1], ABDELHAMEED IBRAHIM[1], EL-SAYED M. EL-KENAWY[2], (Member, IEEE), AND REHAM ARNOUS[2]

[1]Computer Engineering and Control Systems Department, Faculty of Engineering, Mansoura University, Mansoura 35516, Egypt
[2]Computer and Systems Engineering Department, Delta Higher Institute for Engineering and Technology (DHIET), Mansoura 35111, Egypt

Corresponding author: Abdelhameed Ibrahim (afai79@mans.edu.eg)

ABSTRACT Trust management becomes an urgent requirement in the cloud environment and a trust relationship between service user and service provider is required. Trust is the estimation of the ability of cloud resources in completing a task based on some criteria such as availability, reliability, and resource processing power. In this paper, an enhanced QoS-based model for evaluating the trustworthiness of the cloud provider is introduced. The proposed model calculates the accumulative trust value which is updated dynamically at each transaction and reflects the current or latest transaction of the provider in the cloud. The trustworthiness of a cloud resource is evaluated based on its provider reputation history from user feedback ratings based on the covariance mathematical technique to evaluate the credibility of the user's feedback. The trustworthiness of a cloud resource is also evaluated by calculating the computing power of resources at run-time. Experimental results confirm the effect of user opinion and resources processing speed on trust value calculation, which in turn assesses the trustworthiness of the cloud provider. The simulation has been performed using the CloudSim with the platform Eclipse for developing the proposed model.

INDEX TERMS Cloud service selection, quality of service, user credibility, security, trust evaluation.

I. INTRODUCTION

In cloud computing, the user can access the shared resources through the network in a service-based environment. The on-request access to computing resources such as servers, networks, and applications is the principal idea of cloud computing. In the cloud environment, the service delivery models that can be established are software as a service, platform as a service, and infrastructure as a service. The models of deployment in cloud technology are public, private, hybrid and community cloud [1]. Public infrastructure as a service providers offer a variety of services such as storage, configurable virtual machines, and bandwidth around the world [2]–[4].

The competition between service providers by improving their performance while lowering their prices attracts service users. Currently, the contest can be found between various cloud service providers that have similar functional properties. For example, Amazon, Google, and IBM have provided storage services to cloud users. Thus, the best service selection becomes an urgent challenge for the users of the cloud. Quality of Service (QoS) based techniques used to identify the leading cloud provider [5], [6]. The QoS such as throughput, reliability, response time, cost and security can be considered as a set of service attributes. The critical index for the selection of service in the cloud is trust [7]. The trust is usually defined as ''the confidence levels in something or someone''. E-business companies such as Amazon, E-bay, and Google have implemented their trust management model based on reputation. A trust relationship between service user and cloud service provider is required. An accurate assessment model in the performance evaluation of a cloud service is needed [8].

The sophisticated mechanisms for service selection in the cloud, based on trust evaluation, depend on estimating the QoS of each service and matching these QoS parameters with user's preferences then recommend a service according to the matching degree [9], [10]. The evaluation of QoS parameters for specific cloud service to ensure the trustworthiness of a Cloud Service Provider (CSP) depends on objective and subjective trust assessment [11]. The objective trust assessment is evaluated to determine trustworthy of a cloud service depending on comparing the claimed service QoS offered in Service Level Agreement (SLA) by a service provider with

The associate editor coordinating the review of this manuscript and approving it for publication was Chunsheng Zhu.

the actual QoS parameters of that service monitored at run-time [12]. The subjective trust assessment depends on the reputation of the provider of a service which is based on feedback rating supplied by the user to assess the requested service [13]. Reputation-based trust evaluation is used in e-commerce companies. Earlier work depends on objective trust evaluation or subjective trust evaluation to identify trustworthy cloud providers [14]. It is rare to find an evaluation model of trust which combines information of QoS monitoring with user's feedback and computing power of resources to assess the service provider trustworthy in the cloud.

This paper proposes an enhanced QoS-based trust assessment model to enable the cloud user to select the optimal cloud provider who will execute his job based on the user's preferences. In the proposed model, the trustworthiness of the cloud provider is evaluated by calculating the Accumulative/Computed Trust Value (ATV) for each cloud provider who will provide individual service S in a time interval $1 \leq t \leq k$. The value of ATV is updated dynamically at each transaction, and it reflects the current or latest transaction of the provider in the cloud. The computing power/processing speed of a resource is also estimated at run-time and is used in the calculation of trust value at each time window k. Also, the user's feedback ratings are integrated into the calculation of trust value for the provider of the requested service. The covariance mathematical technique is used to verify the credibility of the user's feedback.

The paper is organized as follows. Section II introduces related work about trust evaluation models. The basic assessment model, SLA parameters, and covariance mathematical technique are presented in Section III. Section IV shows the proposed assessment model architecture, and the proposed model algorithm is shown in Section V. Section VI reports on the performance evaluation of the proposed model. The discussion is explained in Section VII. Finally, the conclusion is presented in Section VIII.

II. RELATED WORK

Recently, a high requirement topic is the selection of a trustworthy service provider in cloud computing. The QoS is widely considering in provider selection. Thus, some QoS-based service selection methods have been proposed [15], [16]. The work in [17], [18] introduced a trust management framework named ''Cloud Armor'' based on a reputation in which the trust value is evaluated based on users' feedback. Their method has depending on the feedback density and majority consensus to decide about the users' feedback credibility, however, the feedback uncertainty evaluation was neglected. The authors in [19] introduced an approach for reputation measurement, based on feedback from users, of cloud services. In this approach, the fuzzy set theory was used for calculating the service reputation score. In this model, the trust value and reputation have been calculated based on the aggregated information of a cloud provider from other customers. However, the trustworthiness of user feedback, if fake users affect it, is the main drawback of this model. Other researches, for the selection of cloud services based on fuzzy logic trust evaluation, have been proposed [20], [21].

A hybrid trust evaluation model for cloud services was introduced in [22]. The authors defend the user feedback in the calculation of trust value. In [23], the authors proposed a trust assessment system to model the relationship between users and services; the drawback in this research is that the authors neglect the influences of services QoS values on evaluating services trustworthiness. Authors in [24] present a trustworthiness evaluation model based on QoS prediction and user satisfaction. However, the influence of time factor and unfair ratings was not considered in the evaluation. Authors in [25] present a trust reputation model based on the cloud providers' reputation to help cloud users to make a decision. This reputation value was based on the objective QoS indicators and the subjective users' feedback.

The authors in [26] suggested a selection framework for cloud services based on trust. In this framework, the authors measure the trust based on a monitoring QoS parameters technique with a user's feedback technique to evaluate the cloud provider's trustworthiness. The work in [27] has proposed a trust model based on QoS for a cloud environment. This model evaluates the trust value using data integrity, turnaround efficiency, reliability, and availability features. The authors showed that their model performance was better than the conventional model [28]. The model has improved integrity, reliability, safety, and scalability. However, it had a drawback of improving features such as confidentiality and security.

A selection method for a cloud service using trust and user preference clustering was suggested in [29]. The model was based on a user preference similarity to build a hierarchical clustering algorithm. A multi-dimensional trust model was proposed in [30] for big data workflow processing. The trustworthiness of cloud providers was evaluated from the cloud resource capabilities, the neighboring users' reputation evidence, and the experiences' history of the service provider. However, the computing power of a resource is not considered in the calculation of trust value at run-time.

Compared to the cloud provider selection models in the literature, the proposed enhanced trust assessment model has advantages. It proposes a model based on QoS parameters, user preference similarity, and computing power/processing speed of a resource. The covariance technique is used to verify the credibility of the user's feedback. The trustworthiness of user feedback, in case of fake users, will affect the trust model and the feedback uncertainty evaluation should not be neglected. The computing power of the cloud resource is estimated and is used in the calculation of trust value to be more accurate.

III. BACKGROUND

This section presents an overview of the SLA parameters of availability, reliability, data integrity, and turnaround efficiency, the basic QoS trust assessment model [27], and the

covariance mathematical technique which will be employed in the proposed model.

A. SLA PARAMETERS

Trust is composed of multiple attributes such as truthfulness, security, reliability, honesty, and QoS in an environment context. The trust parameter is for evaluating the cloud resource trust value and it is manipulated in the form of SLA parameter. The CSP will be trusted if it is able to achieve the user's requirements according to the SLA [1], [31], [32]. The SLA parameters, which are considered in the evaluation of cloud resource trust value in the proposed model, can be defined as follow:

- Resource Availability (AV): It means that the system should be accessible and operational when required by users. A resource is called unavailable or inaccessible if it is shutdown, or too busy to process the following request, or under attackers control. Let cloud resources are denoted as $Y_1, Y_2, \ldots, Y_m$. Let N_k for $k = 1, 2, \ldots, m$ be number of submitted jobs over a time period T to resource Y_k. Let A_k, out of N_k, be number of jobs accepted over a time period T by resource Y_k. Thus, the availability can be calculated as

$$AV(Y_k) = \frac{A_k}{N_k} \tag{1}$$

- Resource Success Rate (SR): It is the number of successful tasks executed by a resource Y_k. Let C_k, out of A_k, be the number of completed jobs over time T by resource Y_k. Thus, the success rate can be calculated as

$$SR(Y_k) = \frac{C_k}{A_k} \tag{2}$$

- Turnaround Efficiency (TE): Turnaround time can be shown as the difference between T_{end} and T_{start} as illustrated in Fig. 1. TE is defined as the average of turnaround efficiency for all submitted jobs during a time of T of a resource Y_k. Let $T_{estimat}$ is the estimated turnaround time by CSP in SLA and T_{actual} be the actual turnaround time. Thus, the turnaround efficiency can be calculated as

$$TE(Y_k) = \frac{T_{estimate}}{T_{actual}} \tag{3}$$

- Data Integrity (DI): It defines the accuracy, security, privacy, and consistency of data. Let D_k denotes the number of jobs that conserved the integrity of data output of the C_k completed jobs by a resource Y_k. Thus, data integrity can be calculated as

$$DI(Y_k) = \frac{D_k}{C_k} \tag{4}$$

B. BASIC ASSESSMENT MODEL

The model introduced in [27] is called the basic assessment model and the main components are described as following

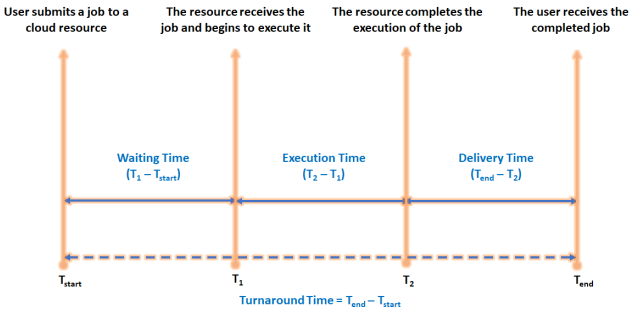


FIGURE 1. Turnaround Time.

- User Interface, Authentication, and Authorization Services involve browsing, registration, and security aspects.
- Catalog Service: provides a cloud resources list.
- System Manager: coordinates the system components.
- SLA Manager: mainly preserves SLA between cloud users and resource providers.
- Provisioning Service: links System Manager and Middleware Agents.
- Governance Service: has the job of monitoring, metering, and billing.
- Middleware Agent: manages virtual machines operations such as creation, customization, and sharing.
- Trust Repository: stores resources trust values.
- Trust Manager: processes and stores the trust values of the trusted repository.

The authors of this model calculate the trust value of a resource, based on the SLA parameters, as T_{QoS}:

$$T_{QoS} = X_1 * AV + X_2 * SR + X_3 * TE + X_4 * DI \tag{5}$$

where $X = \{X_1, X_2, X_3, X_4\}$ are positive weights for the SLA parameters. These weights are predetermined in the SLA relating to user's preferences so that $\sum_{i=1}^{4} X_i = 1$ and $\forall X_i \in [0, 1]$. The user may give the availability of a resource the highest priority and give turnaround efficiency the lowest weight, thus, the weight can be $X_1 = 0.5$, $X_2 = 0.2$, $X_3 = 0.1$, and $X_4 = 0.2$. User's preferences changed from one user to another and may be changed for the same user at different time. Thus, SLA parameters relating to the user are considered as QoS parameters. The algorithm in [33], that is shown in Algorithm 1, is used to calculate the set of weights $X = \{X_1, X_2, X_3, X_4\}$.

C. COVARIANCE MATHEMATICAL TECHNIQUE

The covariance technique is used to verify the credibility of the user's feedback by describing the linear regression relationship between two users. Thus based on this technique, the proposed model can evaluate the fake user. Suppose there are two random variables i and j. The Joint Probability Distribution Function (PDF), normal distribution, is calculated for

Algorithm 1 Weight Calculation Algorithm

1: **Input**: (ω, n), for n number of factors and ω for calculating the most important factor
2: **Output**: Weight $X = \{X_1, X_2, \ldots, X_n\}$
3: Initialize $n = 4$
4: **if** $\omega < 0.5$ **then**
5: $\omega = 1 - \omega$
6: **end if**
7: **if** $\omega \geq 0.5$ **then**
8: **Calculate** X_1 from: $X_1\left[(n-1)\,\omega + 1 - nX_1\right]^n = \left[(n-1)\,\omega\right]^{n-1} * \left[\left((n-1)\,\omega - n\right)X_1 + 1\right]$
9: **Calculate** X_n from: $X_n = \dfrac{\left((n-1)\,\omega - n\right)X_1 + 1}{\left((n-1)\,\omega + 1\right) - nX_1}$
10: **for** i = 2 to (n-1) **do**
11: **Calculate** X_i from: $X_i = \sqrt[n-1]{X_1^{n-i} * X_n^{i-1}}$
12: **end for**
13: **end if**

the variables i and j as:

$$F_{i,j}(i,j) = \frac{d_2}{didj} F_{i,j}(i,j) \tag{6}$$

Covariance (COV): It is the degree of variation between variables i and j and is used to calculate the correlation between variables [34]. Also, it is a measure of the joint PDF of variables i, j. The covariance between i and j with a finite second moment is the product of variables deviations from their expected values individually. $COV(i,j)$ can be defined as:

$$COV(i,j) = E[i,j] - E[i] * E[j] \tag{7}$$

Variance $Var(i)$: Standard Deviation (SD) of a dataset is a measure of how spread out the data is. The variance is another measure of the spread of data in a dataset which can be defined as $Var(i) = SD^2$. It is the expectation of the squared deviation of a random variable from its mean. The variance of a variable is the covariance of that variable and itself. Consequently, when this covariance is standardized (by dividing it by the square root of the product of the $Var(i)$), it will give a correlation of 1. Thus, the correlation coefficient, μ, can be defined as:

$$\mu = \frac{COV(i,j)}{\sqrt{Var(i)Var(j)}} = \frac{E[i,j] - E[i] * E[j]}{SD_i * SD_j} \tag{8}$$

where SD_i is the standard deviation of a variable i and SD_j is the standard deviation of a variable j.

IV. PROPOSED TRUST ASSESSMENT MODEL

The proposed enhanced QoS-based trust assessment model is presented in this section. Feedback service and a proposed approach to verify the user's feedback credibility are explained in detail. The Accumulative Trust Value calculation and the cloud service selection are shown with an example.

A. PROPOSED MODEL ARCHITECTURE

The proposed QoS-based model architecture is shown in Fig. 2. This model is an enhancement version of the model introduced in [27]. The proposed model can be examined as an architecture of four layers which are Cloud Service User (CU), Cloud Service Provider (CSP), Cloud Service Broker (CSB) and System Manager (SM). CSP deploys its services and publishes service QoS information in the cloud via SLA. Through SLA, a user is able to determine a suitable service that satisfies his QoS requirements.

Cloud Service Broker is composed of different submodules [35], [36]. Directory Service is responsible for saving registration information of service along with their SLA parameters provided by CSP when registers its services. Also, it matches the user's QoS requirements with other services and prepares the candidate services list whose SLA parameters satisfy the user's preferences provided in the QoS requirements. This is not the main purpose of this work, and there are many kinds of research used for cloud service selection based on the user's QoS requirements. The SLA management saves the agreement between a service user and the selected service provider to execute a user's task. It is a node to connect CSB with the Trust Assessment Module (TAM) and the system manager. It gets a candidate services list sorted according to trust values from the TAM and informs the user with this shortlist of cloud services to select a specific CSP for task execution and gives the feedback rating to the invoked service. Feedback Service is one of the main contributions of this study. It is a component used for collecting authenticated user's feedback after receiving his invoked services. We will describe its details later in this section.

System Manager is the main component of this model which includes the TAM that is used to evaluate the ATV for each candidate CSP and prepare a list of service providers sorted by their ATV. Trust Catalog is a database for saving transaction information and computed trust value of the invoked service, the schema of this database contains a record for each invoked service in the cloud. The record structure includes information such as (Service identity, User identity, Provider identity, Transaction identity, and Computed Trust Value). When the CSP registers its services for the first time, the TAM evaluates it using Cloud Security Alliance (CSA) recommendations [1]. If the evaluation is accepted, the TAM inserts a trust catalog entry with an initial value to its services. This initial value of the trust is dynamically updated after each transaction invoked this service. ATV can help in enhance CSP performance and build its reputation by offering better QoS and good performance. Provisioning Service supplies a working environment in the form of a virtualized environment to the cloud user. Governance Service is responsible for mainly three jobs which are monitoring, metering and billing. Also, it manages and controls resource allocation and consumption.

The interaction between the components of the proposed model in Fig. 2 is illustrated in the following steps:

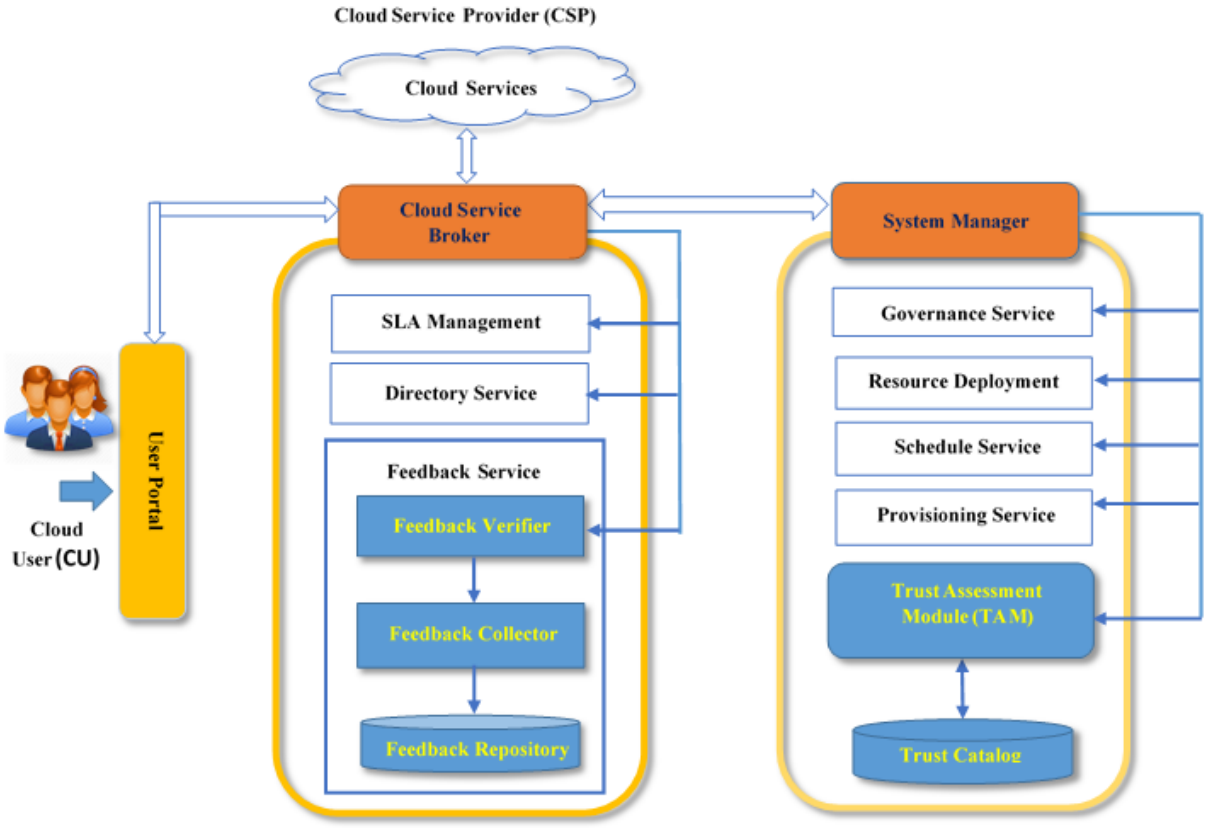


FIGURE 2. Proposed QoS-based model architecture.

1) The CU submits his service query and a list of QoS requirements to Directory Service.
2) The service information of CSP has been released to Directory Service in the form of SLA parameters.
3) The Directory Service prepares a candidate services list whose SLA meets the requirements of the user by matching the user QoS requirements with all registered services.
4) The SLA management sends a list of user's QoS requirements and a candidate services list whose SLA matches the requirements of the user to the TAM to calculate the trust value at a time window k for each candidate service. It returns a list of candidate services sorted by their trust value, and this list is available to the service user to determine a CSP from this list to execute his task. Then, after negotiation, an agreement is established through SLA management between the service user and selected CSP.
5) The SLA management informs System Manager with the selected service provider which in turn reviews the availability of the requested resources based on the Directory Service.
6) The System Manager schedules resources by the Scheduling adviser. It is considered that the request with the least Turnaround Time can be executed first.
7) The System Manager provides SLA to Resource Deployment. It provides and marks the requested resources. For the user, a working environment is virtualized. It creates, customizes, manages and expands the virtual system if needed.
8) Concurrently, the Governance Service has been provided by SLA through the System Manager. Governance Service manages and controls allocated resources. Also, it performs the billing of services in the cloud.
9) Trust attributes of the requested job execution are delivered to the TAM based on the System Manager. The TAM is responsible for updating data in the Trust Catalog.
10) The user checks the data and evaluates the invoked service provided by CSP and sends his feedback to feedback service. Also, the user evaluates data integrity and sent data integrity values in the feedback.
11) The Feedback service evaluates the data from the user then forwards the accurate feedback to the SLA Manager which in turn sends checked feedback values to the Trust Assessment Module to store it in Trust Catalog.

B. FEEDBACK SERVICE OPERATION

Feedback service contains three components which are feedback collector, feedback verifier, and feedback repository.

TABLE 1. QoS attributes required by Cloud User *X* and Capabilities of candidates Cloud providers.

QoS attributes		Cloud User X	Provider P1	Provider P2	Provider P3
Performance	Availability (%)	99.9 %	99.90	99.94	99.99
	Response Time (sec)	85 sec	83	81	62
	Turnaround time (sec)	100 minutes	120	115	100
Capacity	Number of CPUs (4 core each)	4	4	4	8
	CPU speed (GHz)	3.40 GHz	3.40 GHz	3.40 GHz	3.70 GHz
	Disk (TB)	800 GB	1 TB	1.2 TB	4 TB
	Memory (GB)	32 GB	32	32	64
Cost	Cost/task ($)	1000$	1100$	1400$	1700$
Security	Data confidentiality & integrity	Enabled	Enabled	Enabled	Enabled
Network QoS	Latency (milliseconds)	3.5	4.2	3.9	3.1
	Bandwidth (Gbit/s)	10	10	10.21	10.45

TABLE 2. SLA between Cloud User *X* and Service Provider P2.

QoS attributes		QoS of Provider P2 matches User X
Performance	Availability	99.94 %
	Response Time	85 sec
	Turnaround time	100 minutes
Capacity	Number of CPUs	4
	CPU speed	3.40 GHz Clock Speed
	Disk	800 GB
	Memory	32 GB
Cost	Cost/task	1200$
Security	Data confidentiality & integrity	Enabled
Network QoS	Latency	3.5 ms
	Bandwidth	10 Gbit/s

Feedback collector used to collect the user's feedback via a web form through a user portal which is a web-based interface to interact with CSB. The user's feedback evaluates the resource provider's quality of service and the user's satisfaction through a series of questions (e.g., reliability of the network, resource availability, response time, cost whether the cost of a transaction is affordable or not, whether the user satisfied with a particular transaction). The answer to each question from above can be evaluated as not accepted, moderate, reasonable and accepted. The answer is mapped to be from 0 to 1., then it is saved in the feedback repository. The user answer to each question reflects his opinion toward the Quality of service that has been delivered and used to enhance service provider performance. Feedback verifier in which we introduce a new approach to detect malicious user's feedback ratings based on covariance technique, creditable user detected using covariance and fake users extracted.

Feedback Repository is a database that contains the user's feedback. The model classifies a cloud user as Known Cloud User (KCU) or Fake Cloud User (FCU). The KCU has previous records for the same service in the feedback repository, while the FCU does not have any transaction history. Feedback Repository saves a record for each transaction; this record contains information about Transaction ID, CU ID, CSP ID, Service ID, feedback rating for each QoS parameter. This database contains a feedback history provided by the user for each service he invoked, and it will be used in the proposed approach to evaluate the trustworthiness of the current user's feedback.

C. CLOUD SERVICE PROVIDER SELECTION BASED ON COMPUTED TRUST VALUE

The WD-REAM dataset #2 [37] is used in this part. The dataset includes real-world QoS measurements from 142 users over 64-time slices [15-minute interval] on 4,500 Web services. This dataset contains only two attributes which are throughput and response time. Python library is used for generating synthetic dataset contain 11 QoS attributes and have the same format of WS-DREAM [37]. After the cloud user received the requested task, CU gives his feedback for QoS parameters.

Existing Cloud Monitoring Solutions (CMS) is used to dynamic QoS attributes tracking related to the virtualized cloud resources which can be used to improve CSP performance. CMS used to detect the performance fluctuations and account for the SLA breaches of QoS attributes [38], [39]. Existing CMS such as Amazon Cloud Watch [40] and Private Cloud Monitoring System (PCMONS) [41] can also be used. Cloud Harmony APIs [42] can be used to detect the current state of dynamic and Network layer QoS attributes of selected CSP. A random data can be generated for QoS monitoring data at run-time and Network layer QoS attributes within a range suitable to actual data from Cloud Monitoring Systems and practice in the industry. The simulation experiments and obtained results can be validated based on the generated synthetic dataset and the WD-REAM dataset. To explain the Cloud provider selection procedure, it is assumed that:

1) Cloud User X required QoS attributes as shown in table 1 and the Directory Service contains services information of registered CSP.
2) Cloud User X searches the Directory Services to find a cloud Provider P for providing a matching service. The Cloud User X finds m candidate service provider $(P_1, P_2 \ldots P_m)$ which can provide his requirements, suppose there are three providers (P_1, P_2, P_3) that can provide the required service for the user X.
3) The Cloud User X sends a list of candidate Service Providers (P_1, P_2, P_3) and a list of his QoS requirements to the Cloud Service Broker (CSB). CSB retrieves the capabilities of each cloud provider from the Directory Service and forwards the two lists to the SLA management. Table 1 contains an example of the lists information.
4) The SLA management connects with the System Manager and the Trust Assessment Module (TAM). TAM calculates a trust value for each candidate cloud provider (P_1, P_2, P_3) through Equation 13 and sort the

service providers based on the Computed Trust value (CTV).

5) TAM calculates the CTV from transaction history data saved in the Trust Catalog for each candidate cloud provider that can provide the required service S_i. The Trust Catalog contains the last transition data related to each provider supporting the required service. For example, TAM calculates CTV of Provider P_1 to be 0.421, Provider P_2 to be 0.872 and Provider P_3 to be 0.631.
6) Service selection depends on negotiation between the cloud user X and SLA management. SLA is prepared by the SLA management and is shown in table 2. By this SLA, the cloud provider P_2 executes the required task and delivers the executed data to cloud user X based on CSB.

V. PROPOSED MODEL ALGORITHM

Let FU_i is defined as the set of all feedback of similar users for the same service S_i and F_i is defined as all feedback records made by the user U_i for the same service S_i. The term "similar/comparable user" means the one who has a previous record in the feedback repository, where this record is saved when the user previously invoked the same service in the cloud. After the required task by the cloud user is executed by the selected cloud provider, the cloud user sent his feedback about QoS attributes of the received task. The current feedback value which is given by the cloud service S_i user should be compared with the other user's feedback value in the database. If there is a positive correlation for the current user's feedback with the other user's feedback value, it has to be considered as an identified user feedback rating and is used in the evaluation of the trustworthiness of the known cloud provider. Otherwise, the feedback should be considered as a fake user's feedback and be truncated by the feedback verifier module. Thus, the fake user is not fixed or assumed, it is evaluated by the covariance technique to evaluate the credibility of the user's feedback.

The proposed approach determines the variance or standard deviation of current feedback from both F_i and FU_i. Depend on the deviation, the verification of current feedback is assessed and the user's feedback parameter is considered in the evaluation of the trustworthiness of the cloud provider through ATV calculation. In the proposed approach, it is supposed that each feedback of a cloud user is treated as a random variable that follows the normal distribution and the correlation coefficient μ, which describes the linear regression relationship between two users and is calculated by equation 8. The value of μ is considered to be between 1 and -1. Zero value indicates that no relationship at all.

Let U_{corr} indicates the number of users they have a positive relationship with current user; FU is the total number of users feedback. The Similarity Ratio SR, number of users who have similar feedback as the current user, is defined as:

$$SR = U_{corr}/FU, \quad 0 \leq SR \leq 1 \tag{9}$$

Algorithm 2 Update Feedback Value of a Service

```
Input: User request R_i, Selected service S_i, Current user feedback UF_curr, and Feedback database FB_db.
Output: FB(S_i), Feedback value of a service S_i.
Initialize FU, F, SR, U_corr
for each CU ∈ current user and t ∈ K do
    Calculate FU, F, and U_corr
    Update SR from equation 9
    if SR > 0.5 then
        UF_curr ← current user feedback
        User is Identified
    else
        UF_curr = 0
        User is Unidentified
    end if
    if User is Identified then
        Update FB(S_i) from equation 10
    else
        FB(S_i) = 0
    end if
end for
```

If $SR \leq 0.5$, then the current user feedback deviated from the users who have similar feedback. Thus, it is treated as fake feedback and it will be discarded. Otherwise, the current feedback is used to evaluate the trustworthiness of CSP and updates feedback value for this service and its value in the feedback repository. Initially, the feedback value of the service S_i has been assigned to 0, with no trustworthy information available about the service S_i. After each transaction, the current feedback UF_{curr} is used to update the history feedback value in the feedback database for that service. The feedback value of a service S_i, for K time slots, is calculated as

$$FB(S_i) = (1-\alpha)\sum_{t=1}^{k} FU_i + \alpha UF_{curr} \tag{10}$$

The operator α is used to get a significant degree of current user feedback related to the feedback history for the same service and $\alpha \in [0, 1]$. The algorithm to calculate feedback value for service S_i is denoted by $FB(S_i)$ and is shown in Algorithm 2.

The current capacity of a cloud resource affects the performance of the cloud provider and transaction execution. Thus, the current resource capacity parameters such as CPU, RAM, and Network should be considered when evaluating trust value for a cloud resource to enable a system to estimate if the resource can execute the required job or not. In this work, the CPU of a resource as a resource capacity parameter is considered to calculate the Estimated Computing Power (ECP) of a resource R_k at runtime as follows:

$$ECP(R_k) = \frac{CPU_{job}}{CPU_{resource}} \tag{11}$$

ECP is CPU utilization. The CPU utilization depending on the computing tasks amount and type. When the user job is running, one can examine the CPU utilization from the computed resource directly by existing Cloud Monitoring Solutions (CMS). The information that is collected from the running job will help to estimate the CPU needs of similar jobs in the future [43].

In the proposed model, the trust value is calculated from three trust attributes. The first attribute is from QoS parameters and is calculated by equation 5. The second attribute is based on the user's feedback which is calculated by equation 10. The last attribute is from calculating the computing power of a resource at runtime which is calculated by equation 11. The Trust Assessment Module (TAM) is responsible for calculating the Trust Value T of a service S_i provided by a CSP_j at timestamp t as follow:

$$T(Si) = (1-\gamma) * T_{QoS} + ECP + \gamma * FB \tag{12}$$

The operator γ is a positive value used to know the effect of the user feedback on evaluating the trustworthy cloud provider. The preferred value of γ can be set from running experiments many times and monitor the impact of user feedback on trust value evaluation. From experiments, the suitable value for γ is between 0.4 and 0.6.

Trust evaluation is related to a service which in turn related to a cloud service provider. The trust value in equation 12 is calculated at a time window of K.For a better evaluation, the trust value calculated for each transaction occurred at a time of t for a service that is considered and stored in the trust catalog. The Accumulative/Computed Trust Value, ATV, for a service S_i is computed as:

$$ATV(S_i) = \frac{1}{N} \sum_{t=1}^{k} T(S_i) \tag{13}$$

where N is the number of transactions. The TAM calculates ATV for each cloud provider CSP_j which provides specific service S_i in the time interval $1 \leq t \leq k$. The value of ATV is updated dynamically at each transaction, and it reflects the current or latest transaction of the provider in the cloud. The TAM prepares a cloud providers list which is sorted according to Accumulative/Computed Trust Value. This sorted list enables the cloud user to select the optimal cloud provider who will execute his job.

The proposed enhanced QoS-based model algorithm is explained step by step in Algorithm 3. The current trust value of a cloud provider providing a certain service S_i at timestamp t or transaction trust value is represented by Equation 12. This equation is calculated for each transaction and the result trust value is saved in the Trust Catalog database. The accumulative or aggregation trust value which is computed from transaction data history saved in the Trust Catalog as represented in equation 13. The TAM calculates this equation for each cloud provider CSP_j which provides specific service S_i in the time interval $1 \leq t \leq k$. The computed trust value is updated automatically at each transaction.

Algorithm 3 Enhanced QoS-Based Model

1: **Input**: SLA parameters AV, SR, TE, and DI for a resource R_k, $CPU_{resource}$ for cloud provider CSP_j, Selected service S_i, Previous $ATV(S_i)$ for a service S_i
2: **Output**: Updated $ATV(S_i)$
3: Initialize γ, Number of transactions N, Estimated CPU_{job}
4: **for each** $t \in K$ **do**
5: **Calculate** Weight $X = \{X_1, X_2, \ldots, X_n\}$ from Algorithm 1
6: **Calculate** $T_{QoS}(R_k)$, Trust value of a resource R_k from equation 5
7: **Calculate** $ECP(R_k)$, Estimated Computing Power of a resource R_k from equation 11
8: **if** $\gamma = 0$ **then**
9: **Calculate** $T(Si)$ from: $T(Si) = T_{QoS}(R_k) + ECP(R_k)$
10: **else**
11: **Calculate** $FB(S_i)$, Feedback value of a service S_i from Algorithm 2
12: **Calculate** $T(Si)$ from: $T(Si) = (1-\gamma) * T_{QoS}(R_k) + ECP(R_k) + \gamma * FB(S_i)$
13: **end if**
14: **Update** $ATV(S_i)$ from: $ATV(S_i) = ATV(S_i) + T(Si)$
15: **end for**
16: **Calculate** Updated $ATV(S_i)$ from: $ATV(S_i) = ATV(S_i)/N$

VI. PERFORMANCE EVALUATION

Three main scenarios are presented in this section to show the effectiveness of the proposed model. The first scenario shows that the estimated computing power of a resource R_k can affect the performance of the proposed enhanced QoS-based model. The second scenario is done to show the impact of the user's feedback for service S_i in the trust value calculation which in turn evaluates the service provider's trustworthiness. The final scenario shows the proposed model performance in reducing the fake user's feedback effect on transaction completion.

Experiments are run on HP Elite Book 840p, 2.6 GHz Intel, Core i7 with 8 GB RAM on Windows operating system. Instead of using a large-scale of a real environment, since it is cost-effective, a simulation environment is used for testing the proposed model. The CloudSim [44], [45], which is a framework for the simulation and modeling the environment of the cloud, is used in these experiments. The simulated cloud contains a variety of resources to investigate the concept of heterogeneous cloud. Each resource has different computational and network characteristics. Simulation has been performed using the CloudSim and the platform Eclipse for developing the proposed model.

A. SCENARIO 1: EFFECT OF ESTIMATED COMPUTING POWER OF A RESOURCE

The enhanced trust value in this scenario, "Enhan_Trust", is calculated from Algorithm 3, by setting the value of the

FIGURE 3. Availability of the proposed enhanced model and the conventional QoS-based model.

FIGURE 4. Success Rate of the proposed enhanced model and the conventional QoS-based model.

operator $\gamma = 0$, to show the effect of the estimated computing power of a resource R_i on evaluating the proposed model performance. A sequence of 10 posts range from 500 to 5000 jobs with a step size of 500 jobs is used in this experiment. For each post, all the jobs are posted simultaneously. The service providers list which will provide services that match the user QoS needs is identified for each job. Then, a trust value for each service is calculated and saved in the trust catalog and sorted in a list according to their trust value. The service provider which has the highest trust value will be invoked to provide its service to execute the required job.

Figure 3 shows that the availability of resources in the proposed model outperformed the conventional QoS trust model. Figure 4 shows the success rate of the proposed model which is nearly the same as the compared model. Despite it shows a decrease in the performance when the number of jobs increases because some jobs may be failed due to the increase in the number of connections to a database server, some jobs may be failed due to restricted provisioning policy. There are many reasons for job failure in the cloud. Figure 5 shows the turnaround efficiency of the proposed enhanced model which is better than the conventional QoS-based model. The results are compared with Manuel's QoS trust model [27].

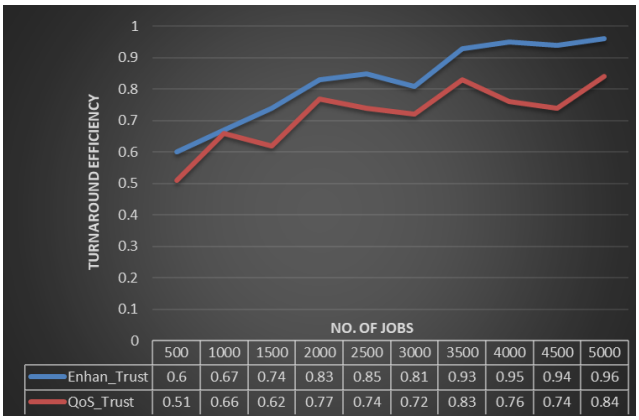


FIGURE 5. Turnaround Efficiency of the proposed enhanced model and the conventional QoS-based model.

B. SCENARIO 2: IMPACT OF USER'S FEEDBACK ON PERFORMANCE

This scenario is calculated from the proposed Algorithm 3, by setting the value of the operator $\gamma \neq 0$, which evaluates how accurately the proposed covariance-based approach verifies the user's feedback credibility. It indicates that the proposed approach is useful because the covariance is efficient in finding the similarity degree between the cloud users. This experiment is carried out by 100 independent runs. For each run, a service provider list matches the user needs is identified and TAM suggests the service provider with the highest trust value to execute the required job. Then the cloud user gives his feedback after each run. The approach analyzes the transaction history of the service provider and can identify the trustworthiness of the cloud providers as Trusted (85%), Untrusted (10%) or Unknown (5%). Also, the TAM identifies the cloud user as identified, fake, or unknown user. The ''Identified User'' is the one who almost gives feedback and is trusted, the ''Fake User'' is the one who provides false feedback all the time and is treated as untrusted, and the ''Unknown User'' who randomly switches between identified and fake.

Figure 6 shows that trusted service provider always has a high trust value. This figure illustrates the ability of the proposed algorithm to filter candidate service providers who will provide the requested service by cloud user based on calculation of Accumulative Trust Value (ATV) into trust cloud provider, ''Trust_CSP'', who has history feedback and transactions data saved in database and untrusted cloud provider, ''Untrust_CSP'', who does not have any transition history.

C. SCENARIO 3: EFFECT OF FAKE USER'S FEEDBACK ON TRANSACTION COMPLETION

The last scenario illustrates the proposed enhanced model efficiency to identify the fake user's feedback, then excludes the cloud provider of that service which in turn reflects on the transaction completion. Transaction Success Rate (*TSR*) can be calculated by dividing the number of successful or

FIGURE 6. Accuracy of the proposed enhanced model to verify the user's feedback credibility.

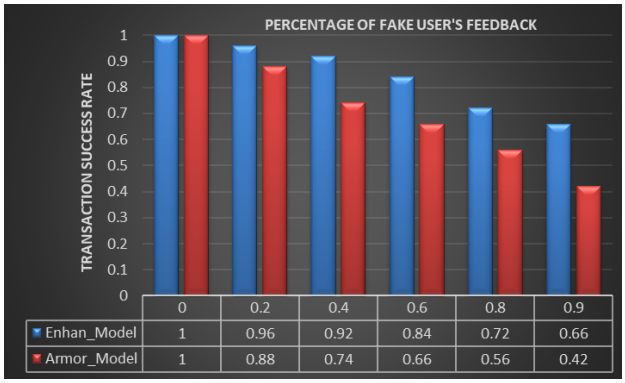


FIGURE 7. Proposed enhanced model efficiency to identify the fake user's feedback.

completed transactions by the total number of accepted transactions over a given time. For example, if we run 100 transactions, and 93 of them were successful, we would have a transaction success rate of 0.93. The *TSR* can be defined as:

$$TSR(t) = (Trans_{succ})/(Trans_{total}) \tag{14}$$

where $Trans_{succ}$ is the number of successful transactions completed in a period t and $Trans_{total}$ is the total number of transactions in the same period. The number of required transaction is determined from Algorithm 3.

Figure 7 shows that the proposed model, ''Enhan_Model'', has a better *TSR* than the conventional model. It is noted that, when the percentage of fake user's feedback increased, the proposed model can identify fake user's feedback and exclude it. In this experiment, the proposed model is compared to the Armor model proposed in [18], ''Armor_Model'', regarding the *TSR* indicator.

VII. DISCUSSION

The proposed model can be tested with real data in different operating systems environments. This framework can be used as ''Trust as a Service'' in which the trust management service layer can be located between the CSP layer and user layer. The Cloud Service Measurement Index Consortium (CSMIC) [46] and the Service Measurement Index (SMI) can be utilized. SMI can be used to design initial Catalog service with real data from different cloud service providers. The actual QoS monitoring values will be incorporated in this and the data from different sources including web sites of CSP will be involved. The Cloud Harmony API [47] can be used to collect data related to QoS attributes of the Network layer (Bandwidth and Latency). Data related to performance QoS attributes (Response time and CPU speed) can be collected using Cloud Monitoring solutions such as Amazon Cloud Watch [40]. For security and user feedback attributes, data can be generated randomly within a range suitable to practice data.

VIII. CONCLUSION

This paper presents a trust assessment model for evaluating the cloud provider using multiple factors such as SLA parameters provided by the cloud provider in the agreement with the cloud user. Also, this paper calculates the estimated computing power of the candidate resource to determine its ability to complete the required job. The reputation history of the cloud provider taken from the user's feedback rating from previous invocations is used. Also, this paper introduces a covariance-based approach to determine a user's feedback credibility. The proposed model calculates the accumulative trust value which is updated dynamically at each transaction and reflects the current or latest transaction of the provider in the cloud. The proposed model is compared with state-of-the-art trust assessment models. Experiments show that the proposed model is reliable and has a better transaction success rate than the compared models. In future work, a new framework for trust assessment can be introduced to evaluate the public and private cloud providers and the cloud user. The trusted cloud user can be evaluated based on user behavior parameters.

REFERENCES

[1] P. Mell and T. Grance, ''The nist definition of cloud computing,'' *Commun. ACM*, vol. 53, no. SP 800-145, pp. 1–7, 2011. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-145/final

[2] P. Casas and R. Schatz, ''Quality of experience in cloud services: Survey and measurements,'' *Comput. Netw.*, vol. 68, pp. 149–165, Aug. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128614000383

[3] M. Noshy, A. Ibrahim, and H. A. Ali, ''Optimization of live virtual machine migration in cloud computing: A survey and future directions,'' *J. Netw. Comput. Appl.*, vol. 110, pp. 1–10, May 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804518300833

[4] A. Sriv and P. G. Sorenson, ''Service selection based on customer rating of quality of service attributes,'' in *Proc. IEEE Int. Conf. Web Services*, Jul. 2010, pp. 1–8.

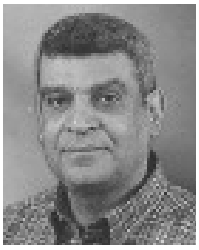
[5] J. Mateo-Fornes, F. Solsona-Tehas, J. Vilaplana-Mayoral, I. Teixido-Torrelles, and J. Rius-Torrento, ''CART, a decision SLA model for SaaS providers to keep QoS regarding availability and performance,'' *IEEE Access*, vol. 7, pp. 38195–38204, 2019.

[6] X. Zheng, L. D. Xu, and S. Chai, ''QoS recommendation in cloud services,'' *IEEE Access*, vol. 5, pp. 5171–5177, 2017.

[7] M. Tang, X. Dai, J. Liu, and J. Chen, ''Towards a trust evaluation middleware for cloud service selection,'' *Future Gener. Comput. Syst.*, vol. 74, pp. 302–312, Sep. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X1600011X

[8] P. Lou, L. Yuan, J. Hu, J. Yan, and J. Fu, "A comprehensive assessment approach to evaluate the trustworthiness of manufacturing services in cloud manufacturing environment," *IEEE Access*, vol. 6, pp. 30819–30828, 2018.
[9] L. Sun, H. Dong, F. K. Hussain, O. K. Hussain, and E. Chang, "Cloud service selection: State-of-the-art and future research directions," *J. Netw. Comput. Appl.*, vol. 45, pp. 134–150, Oct. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S108480451400160X
[10] H. Hassan, A. El-Desoky, and A. Ibrahim, "An economic model for cloud service composition based on user's preferences," in *Proc. 13th Int. Comput. Eng. Conf. (ICENCO)*, Dec. 2017, pp. 195–201.
[11] J. Xiahou, F. Lin, Q. Huang, and W. Zeng, "Multi-datacenter cloud storage service selection strategy based on AHP and backward cloud generator model," *Neural Comput. Appl.*, vol. 29, no. 1, pp. 71–85, Jul. 2016, doi: 10.1007/s00521-016-2364-y.
[12] S. S. Yau, J. Huang, and Y. Yin, "Improving the trustworthiness of service qos information in service-based systems," in *Autonomic Trusted Computer*, B. Xie, J. Branke, S. M. Sadjadi, D. Zhang, and X. Zhou, Eds. Berlin, Germany: Springer, 2010, pp. 208–218.
[13] Z. Noorian, M. Fleming, and S. Marsh, "Preference-oriented QoS-based service discovery with dynamic trust and reputation management," in *Proc. 27th Annu. ACM Symp. Appl. Comput. (SAC)*, New York, NY, USA, 2012, pp. 2014–2021, doi: 10.1145/2245276.2232111.
[14] Q. He, J. Yan, H. Jin, and Y. Yang, "Servicetrust: Supporting reputation-oriented service selection," in *Service-Oriented Computer*, L. Baresi, C.-H. Chi, and J. Suzuki, Eds. Berlin, Germany: Springer, 2009, pp. 269–284.
[15] S. Pearson, *Privacy, Security and Trust in Cloud Computing*. London, U.K.: Springer, 2013, pp. 3–42.
[16] Z. Zheng, X. Wu, Y. Zhang, M. R. Lyu, and J. Wang, "QoS ranking prediction for cloud services," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 6, pp. 1213–1222, Jun. 2013.
[17] T. H. Noor, Q. Z. Sheng, A. H. H. Ngu, A. Alfazi, and J. Law, "Cloud armor: A platform for credibility-based trust management of cloud services," in *Proc. 22nd ACM Int. Conf. Conf. Inf. Knowl. Manage. (CIKM)*, New York, NY, USA, 2013, pp. 2509–2512, doi: 10.1145/2505515.2508204.
[18] T. H. Noor, Q. Z. Sheng, L. Yao, S. Dustdar, and A. H. H. Ngu, "CloudArmor: Supporting reputation-based trust management for cloud services," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 367–380, Feb. 2016.
[19] S. Wang, L. Sun, Q. Sun, J. Wei, and F. Yang, "Reputation measurement of cloud services based on unstable feedback ratings," *Int. J. Web Grid Services*, vol. 11, no. 4, p. 362, 2015, doi: 10.1504/IJWGS.2015.072805.
[20] R. Nagarajan, S. Selvamuthukumaran, and R. Thirunavukarasu, "A fuzzy logic based trust evaluation model for the selection of cloud services," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2017, pp. 1–5.
[21] R. Nagarajan, R. Thirunavukarasu, and S. Shanmugam, "A fuzzy-based intelligent cloud broker with MapReduce framework to evaluate the trust level of cloud services using customer feedback," *Int. J. Fuzzy Syst.*, vol. 20, no. 1, pp. 339–347, Jun. 2017, doi: 10.1007/s40815-017-0347-5.
[22] V. Viji Rajendran and S. Swamynathan, "Hybrid model for dynamic evaluation of trust in cloud services," *Wireless Netw.*, vol. 22, no. 6, pp. 1807–1818, Sep. 2015, doi: 10.1007/s11276-015-1069-y.
[23] S.-G. Deng, L.-T. Huang, J. Wu, and Z.-H. Wu, "Trust-based personalized service recommendation: A network perspective," *J. Comput. Sci. Technol.*, vol. 29, no. 1, pp. 69–80, Jan. 2014, doi: 10.1007/s11390-014-1412-2.
[24] S. Ding, S. Yang, Y. Zhang, C. Liang, and C. Xia, "Combining QoS prediction and customer satisfaction estimation to solve cloud service trustworthiness evaluation problems," *Knowl.-Based Syst.*, vol. 56, pp. 216–225, Jan. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0950705113003729
[25] L. F. Bilecki and A. Fiorese, "A trust reputation architecture for cloud computing environment," in *Proc. IEEE/ACS 14th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Oct. 2017, pp. 614–621.
[26] M. Macías and J. Guitart, "Analysis of a trust model for SLA negotiation and enforcement in cloud markets," *Future Gener. Comput. Syst.*, vol. 55, pp. 460–472, Feb. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X15000667
[27] P. Manuel, "A trust model of cloud computing based on quality of service," *Ann. Operations Res.*, vol. 233, no. 1, pp. 281–292, Apr. 2013, doi: 10.1007/s10479-013-1380-x.
[28] P. D. Manuel, S. T. Selvi, M. I. A.-E. Barr, M. Ibrahim, and A.-E. Barr, "A novel trust management system for cloud computing-iaas providers," *J. Combinat. Math. Combinat. Comput.*, vol. 79, pp. 3–22, Nov. 2013.
[29] Y. Wang, J. Wen, W. Zhou, B. Tao, Q. Wu, and Z. Tao, "A cloud service selection method based on trust and user preference clustering," *IEEE Access*, vol. 7, pp. 110279–110292, 2019.
[30] H. T. El Kassabi, M. A. Serhani, R. Dssouli, and B. Benatallah, "A multi-dimensional trust model for processing big data over competing clouds," *IEEE Access*, vol. 6, pp. 39989–40007, 2018.
[31] "IEEE region 10 conference on computer and communication systems (1990: Hong Kong) and IEEE Hong Kong section," in *Proc. IEEE TENCON Conf.* Hong Kong: The Section, 1990, pp. 1–780. [Online]. Available: http://books.google.com/books?id=WCJOAQAAIAAJ
[32] P. Gupta, M. K. Goyal, P. Kumar, and A. Aggarwal, "Trust and reliability based scheduling algorithm for cloud iaas," in *Proc. 3rd Int. Conf. Trends Inf., Telecommun. Comput.*, V. V. Das, Ed. New York, NY: Springer, 2013, pp. 603–607.
[33] A. Singh and K. Chatterjee, "A multi-dimensional trust and reputation calculation model for cloud computing environments," in *Proc. ISEA Asia Secur. Privacy (ISEASP)*, Jan. 2017, pp. 1–8.
[34] K. G. Jöreskog, "Structural analysis of covariance and correlation matrices," *Psychometrika*, vol. 43, no. 4, pp. 443–477, Dec. 1978, doi: 10.1007/BF02293808.
[35] N. Rajganesh and T. Ramkumar, "A review on broker based cloud service model," *J. Comput. Inf. Technol.*, vol. 24, no. 3, pp. 283–292, Oct. 2016.
[36] R. Nagarajan and R. Thirunavukarasu, "A review on intelligent cloud broker for effective service provisioning in cloud," in *Proc. 2nd Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, Jun. 2018, pp. 519–524.
[37] Z. Zheng, Y. Zhang, and M. R. Lyu, "Investigating QoS of real-world Web services," *IEEE Trans. Services Comput.*, vol. 7, no. 1, pp. 32–39, Jan. 2014.
[38] H. J. Syed, A. Gani, R. W. Ahmad, M. K. Khan, and A. I. A. Ahmed, "Cloud monitoring: A review, taxonomy, and open research issues," *J. Netw. Comput. Appl.*, vol. 98, pp. 11–26, Nov. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804517302783
[39] P. S. Anjana, P. Badiwal, R. Wankar, S. Kallakuri, and C. R. Rao, "Cloud service provider evaluation system using fuzzy rough set technique," in *Proc. IEEE Int. Conf. Service-Oriented Syst. Eng. (SOSE)*, Apr. 2019, p. 187.
[40] *Amazon Cloudwatch*. Accessed: Jan. 20, 2020. [Online]. Available: http://http://aws.amazon.com
[41] *Private Cloud Monitoring Systems (Pcmons)*. Accessed: Jan. 20, 2020. [Online]. Available: https://github.com/pedrovitti/pcmons
[42] *Cloud harmony*. Accessed: Jan. 20, 2020. [Online]. Available: http://cloudharmony.com
[43] *Cloud Monitoring Tools*. Accessed: Jan. 20, 2020. https://www.opsview.com/solutions/cloud-monitoring-tools
[44] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. F. De Rose, and R. Buyya, "CloudSim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," *Softw., Pract. Exper.*, vol. 41, no. 1, pp. 23–50, Aug. 2010, doi: 10.1002/spe.995.
[45] *Cloudsim: A Framework for Modeling and Simulation of Cloud Computing Infrastructures and Services*. Accessed: Jan. 20, 2020. [Online]. Available: http://www.cloudbus.org/cloudsim/
[46] *Cloud Service Measurement Index Consortium (CSMIC), SMI Framework*. Accessed: Jan. 20, 2020. [Online]. Available: http://csmic.org
[47] S. K. Garg, S. Versteeg, and R. Buyya, "A framework for ranking of cloud computing services," *Future Gener. Comput. Syst.*, vol. 29, no. 4, pp. 1012–1023, Jun. 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X12001422

HALA HASSAN received the B.Sc. degree from Mansoura University, Egypt. She is currently a Teaching Assistant with the Computer Engineering and Control Systems Department, Faculty of Engineering, Mansoura University. Her research interests include cloud computing, software development, and database administration.



ALI IBRAHIM EL-DESOUKY received the M.A. and Ph.D. degrees from the University of Glasgow, USA. He is currently a Full Professor with the Computer Engineering and Control Systems Department, Faculty of Engineering, Mansoura University, Egypt. He is also a Visiting part-time Professor with the MET Academy. He teaches in American and Mansoura universities and has taken over many positions of leadership and supervision of many scientific papers. He has published hundreds of articles in well-known international journals.

ABDELHAMEED IBRAHIM received the bachelor's and master's degrees in engineering from the Computer Engineering and Control Systems Department, in 2001 and 2005, respectively, and the Ph.D. degree in engineering from the Faculty of Engineering, Chiba University, Japan, in 2011. He was with the Faculty of Engineering, Mansoura University, from 2001 to 2007. He is currently an Assistant Professor of computer engineering with the Faculty of Engineering, Mansoura University, Egypt. His research interests include computer vision, pattern recognition, optimization, cloud computing, and virtual machine migration. He serves as a Reviewer for *Journal of Electronic Imaging, Optical Engineering*, IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, IEEE ACCESS, *Computer Standards and Interfaces, Journal of Healthcare Engineering, IET Image Processing, Multimedia Tools and Applications*, and other respected journals.

EL-SAYED M. EL-KENAWY (Member, IEEE) is currently an Assistant Professor with the Delta Higher Institute for Engineering and Technology (DHIET), Mansoura, Egypt. Inspiring and motivating students by providing a thorough understanding of a variety of computer concepts. He has pioneered and launched independent research programs. He is interested in computer science and machine learning field. Adept at explaining sometimes complex concepts in an easy-to-understand manner.

REHAM ARNOUS received the M.S. and Ph.D. degrees from the Department of Computer Engineering and Control Systems, Faculty of Engineering, Mansoura University, Mansoura, Egypt, in 2008 and 2018, respectively. She is currently a Lecturer with the Delta Higher Institute for Engineering and Technology (DHIET), Mansoura. She has published in the field of resource management in cognitive radio networks. Her research interests include cognitive radio, wireless networking, and applied artificial intelligence. She serves as a Reviewer for *EURASIP Journal on Wireless Communications and Networking*.