The Journal of Supercomputing
https://doi.org/10.1007/s11227-021-03775-8

A novel cloud management framework for trust establishment and evaluation in a federated cloud environment

Rabia Latif[1] · **Syeda Hadia Afzaal**[2] · **Seemab Latif**[2]

Accepted: 25 March 2021
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract

Cloud Computing is being utilized by large-scale organizations for data storage and management. It provides advantages like reducing the cost of information technology services by shared computing resources and more data storage space, in addition to on-demand and easy pay-per-use service mechanism. Different Cloud Service Providers (CSPs) form cloud federation to share their resources. In a cloud environment, it is essential to make sure that the customer's data is fully secured, and standard privacy laws are applied to form a trusted relationship among CSPs and customers. Therefore, the focus of this research is to identify the issues for establishment of a trusted environment and evaluation of trusted levels between customers and their CSP. In this paper, a Federated Cloud Trust Management Framework (FCTMF) is proposed that resolves the trust issues and motivates the cloud providers to successfully participate in cloud federation. The proposed framework evaluates the level of trust based on Service Level Agreement (SLA) parameters, also considering customers and participating CSPs' feedback. The results and comparison exhibit that the proposed framework is more accurate and feasible in terms of calculating level of trust.

Keywords Cloud computing · Cloud federation · Trust evaluation framework · Cloud trusted model

✉ Rabia Latif
rlatif@psu.edu.sa

Syeda Hadia Afzaal
shadia.phdismcs@student.nust.edu.pk

Seemab Latif
seemab.latif@seecs.edu.pk

[1] College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia

[2] National University of Sciences and Technology (NUST), Islamabad, Pakistan

Published online: 09 April 2021

1 Introduction

Cloud Computing introduces many advantages like reducing the cost of IT services by shared computing resources and more storage space. In cloud computing many challenges such as trust establishment, data protection from unauthorized access, data recovery and backup availability when in need and data management capabilities exist. Trust in a cloud environment is a very important term. A trusted model is basically a protocol or management method that includes factors like trust establishment, trust renewal and trust withdrawal [29].

Cloud federation has proved to be an advantage for a CSP, whether small or large scale, to conveniently share its provided services to gain profits and expand its business. In a cloud federated environment, when a CSP has not enough resources it can use resources of other CSPs on-payment that are ready to share their unused capacity of available resources [18]. The main challenge associated with cloud federation, due to which CSPs or customers hesitate to participate, is the low level of trust between the cloud providers. In cloud federation, service requests from customers or CSPs are redirected from one CSP to another because of exceeding demand and load of services. Due to this, the sensitive data items or even the complete virtual machine is migrated from one CSP to another CSP platform.

Now, to make sure that the customer data are fully secured and standard privacy laws are applied, it is essential to form a trusted relationship and estimate the level of trust between the participating CSPs who want to make a reliable federation for their customer's satisfaction [24].

Therefore, the focus of this research is to identify the issues of establishment of trusted environments and evaluation of level of trust between CSPs as it has become a need of time to participate in cloud federation for the best utilization of computing resources. In this research, we put forward a trust evaluation framework that can resolve this issue and can help CSPs to successfully participate in a trusted cloud federation and utilize the best of their resources.

Rest of the paper is arranged as follows: review of the existing techniques and methods used to evaluate trust in cloud environments along with their limitations is presented in Sect. 2. Section 3 elucidates the proposed FCTMF along with its key components and implementation technique. Design and architecture of the proposed framework is also discussed in this section. In Sect. 4, implementation mechanism of the proposed framework and the results are discussed along with the comparative analysis. Finally, the paper concludes in Sect. 5 along with the future directions.

2 Literature review

2.1 Cloud computing trust models

The core idea behind any trust evaluation model is based on control and subjective trust to make secure and reliable transactions between customers and business organizations by building the online trust.

Nowadays, an important domain where trusted models play a vital role is in distributed computing that includes mobile networking, wireless communication, ad-hoc network setup, peer-to-peer networking and grid computing [6]. All these areas are highly vulnerable to security breach due to lack of trust between different nodes that are sharing important information for various purposes.

In cloud computing, trust is considered to be the challenging issue faced by different cloud consumers and cloud providers. The situation becomes critical when consumer's data are distributed across various geographical locations and becomes invisible to the data owner. In this regard, different cloud-based trusted models have been proposed that help to establish trust between clouds.

In [15], Ma et al. have considered trust in cloud environments as a self-organizing system. Using a bionic mechanism, a dynamic trust evaluation method with family attribute is proposed. When an ant colony algorithm is used to optimize search, it is easy to fall into local optimum, which can lead to abnormal results of trust evaluation in the initial stage of trust evaluation.

S.Kaushik et al. [13] have proposed a hierarchical level trusted model. Authors have used the Artificial Bee Colony (ABC) algorithm for searching various CSP for the same service and find the best among them having high calculated trust value or recommendation by other customers in their feedback. The proposed work shows higher accuracy in trust formation, success rate and prevention of any malicious attack.

Wang et al. [28] proposed a dynamic level-based cloud service trust evaluation model in which cloud services levels represent service capabilities in accordance with individual preferences. For direct trust calculation, customer preferences and attenuation factors are considered. Feedback data are assigned different weights for evaluation of reputation. For cloud customer security, a data protection method based on a normal cloud model for data privacy and protection is proposed. A trust update mechanism is also resented for direct trust calculation. The experimental results show that the proposed model provides higher customer satisfaction and success rate than other existing methods. However, the proposed model needs to be optimized using customer feedback to improve requester service selection accuracy.

Bendiab et al. [5] proposed a dynamic trusted model based on Fuzzy Cognitive Maps (FCM). Authors represent the relationships among trust and its manipulating factors in the context of Federated Identity Management (FIM). This approach allows the creation of federations on the basis of resulting trust value which can make service provisioning by CSP and customer communication easier and more flexible. Thus, FIM systems will be more scalable and flexible to successfully deploy in real cloud environments.

Ghafoorian et al. [9] proposed a novel direct trust computation model. Authors addressed the requirements for the accuracy of an indirect access control trusted model for secure data storage in the cloud environments. Authors also addressed the possible security threats of a trust-based system in the proposed indirect trusted model and architecture. Limitation of this model is that customer, roles and Administrator Identity Management are not considered.

Aarthy et al. [1] proposed a model that detects the inefficient cloud service brokers by assessing the customer's feedback through a Trusted Third Party (TTP) for securing the reputation of a CSP. The presented model uses several techniques such as Trust aware service brokering, Resource matching, Feedback aggregation and Adaptive trust evaluation. The experimental results show that the proposed model is relatively better when compared with the other models. To increase the trust, recommendation and reputation-based techniques can be added.

Challangidad et al. [6] proposed a multi-dimensional dynamic trust evaluation scheme to determine the trustworthiness of customers and CSPs through the perspectives of various cloud entities. Trustworthiness is obtained through desired Quality of Service requirements and CSPs to choose desired and legal customers. The results in the paper illustrate the proposed scheme is dynamic and steady in distinguishing trustworthy and untrustworthy CSPs and customers.

Tan et al. [25] proposed SLA trusted model based on behavior evaluation. In this scheme, the provider is selected based on two aspects: (a) the transaction history between the customers and CSPs, (b) The level of trust of that CSP before the service starts. In the service procedure, upon the attainment of SLA parameters, the trust value is updated dynamically using iterative methods. At the same time, the trust value becomes more reasonable using the time factor. This research only focuses on SLA parameters for trust calculation and ignores other important aspects.

Kanwal et al. [12] proposed a trust calculation model that eases the CSPs to weigh the level of trust and enable them to share resources in a trusted and reliable federated Cloud environment. The calculated trust values are swapped between home and foreign CSPs. Limitation of this research is that it only includes the trust of individual CSP and parameters taken for trust calculation are limited.

In [23], Singh et al., proposed a trusted technique to calculate trust values of CSPs. The framework calculates final trust value which is based on consumer's self trust on CSP, friends' trust on CSP and third party's trust on CSP.

It can be concluded from the studied literature that the existing models have some strengths as well as weaknesses. Most of the existing work only considers a few parameters for trust level calculation, which is not acceptable as it directly impacts the privacy of customer data and reputation of cloud providers. So, there is a need to propose a model that could overcome the flaws of the existing schemes and consider other important parameters that lead to a better trust value in order to evaluate trust between CSPs in a federated environment.

3 Proposed federated cloud trust management framework (FCTMF)

We propose a FCTMF for evaluation and establishment of trust in a federated cloud environment. The proposed framework mainly includes three mechanisms for trust calculation, SLA parameters, feedback from customers and feedback from participating clouds. The objective of the proposed framework is to evaluate the level of trust and establishment of a trusted relationship between CSPs. This helps to facilitate them to provide a reliable and secure trust calculation technique in federated cloud environments.

In the presented model, trust is taken as an arithmetic value which lies between 0 and 1 [11]. This value is used to define the range of trust first (between 1 and 0) and then the level of trust (high, medium and low) of a targeted CSP accordingly. The

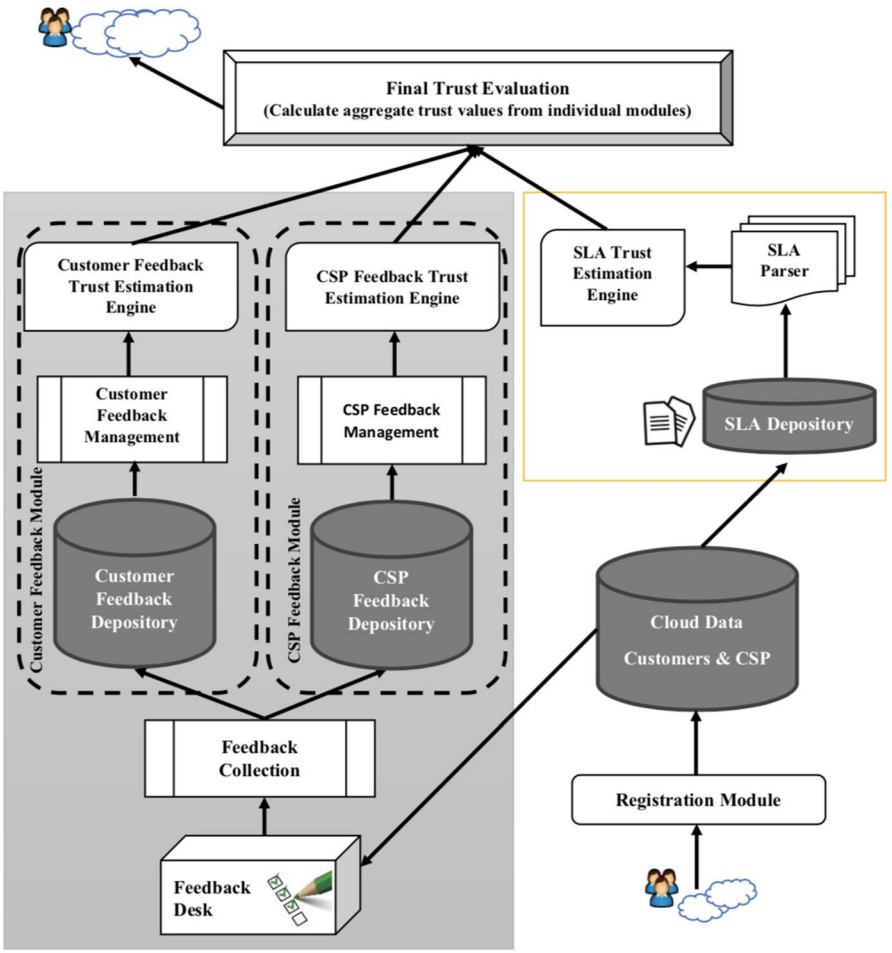

Fig. 1 Proposed federated cloud trust management framework

final trust value is evaluated by aggregating scores from individual proposed mechanisms that gives the overall level of trustworthiness of the targeted CSP.

3.1 Workflow of proposed FCTMF

The complete workflow of the proposed Federated Cloud Trust Management framework is shown in Fig. 1.

The workflow begins when the CSP that wants to participate in federation and its primary customers register for the trust evaluation framework through the Registration Module (RM) shown in Fig. 1. They are then asked to submit the required authorizations that include basic data of the registering customers, SLAs of CSP and CSP basic information about their certain parameters that will be discussed in sections below. The SLAs of registered CSPs that are collected by the SLA module (SM). These are first submitted to the SLA depository where all the data are stored. The SLAs are then sent to the SLA parser where the SLAs are examined according to the set parameters that are defined in the security and privacy domains (discussed in section 3.2.2). The extracted parameters are then evaluated, and the trust score is calculated in the SLA trust evaluation engine as shown Fig. 1.

Then the trust evaluation process starts at the feedback module. The information is first sent to the feedback desk where it differentiates between the feedback request form customer or CSP. The Feedback collection Module asks for feedback from CSP and customers individually. If the feedback is from the customer then the process shifts to the Customer Feedback Module (CFM) and if it's from a CSP then it shifts to feedback from CSP feedback module(CSP-FM).

Next, if the feedback is from the customer then the information goes to the customer Feedback Depository. The customer feedback module collects the feedback in form of a questionnaire. The questionnaire contains different types of questions regarding security and privacy features from the customer aspect. Then the final trust score is evaluated in the customer feedback trust estimation engine.

Similarly, if the feedback is from CSP then the information goes to the CSP feedback module. The information regarding CSP is submitted to the CSP Feedback Depository. Then the CSP feedback management presents a questionnaire for the participating CSP that contains standard attributes of a CSP and level of concern regarding it. The Cloud Service Provider feedback module submits the collected feedback about CSP's to the CSP feedback trust estimation engine of the feedback. It estimates the trust score based on registered CSP feedback.

Finally, The feedback module and SLA module calculates their respective trust scores based on feedback and SLA mechanisms, respectively. All of the calculated trust scores from each are then passed to the Final Trust Evaluation Module(FTEM). The FTEM aggregates the complete trust score that indicates the CSP's trust level.

3.2 Components of proposed FCTMF

The architecture of the proposed FCTMF includes RM, CFM, CSP-FM, SM and FTEM. The core functionality of each module is discussed below.

3.2.1 Registration module (RM)

The RM of the proposed FCTMF is accountable for registration of customers and CSPs who want to participate in the trusted cloud federation. The RM collects the SLA documents of the participating CSP's. These SLA documents are collected only once at the time of registration for establishment of a trusted cloud federation. These collected SLA's are then used by the SLA Management Module for calculation of final SLA-based trust score. The RM also initiates the Feedback Module for the collection of feedback from customers and CSP's to calculate the final feedback-based scores.

3.2.2 Service level agreement module (SM)

The SLA refers to a document that explains the services that are to be agreed upon, parameters that define the level of service, the assurance of guarantees provided regarding the quality of service. It also includes the compensation in case of any violation [25].

The proposed SM mainly includes three main components as shown in Fig. 2. The details of each component are discussed below:

- *SLA depository* It collects the SLAs from the registered CSP and stores them in the depository. These SLAs are then passed onto the SLA parser for further evaluation.
- *SLA parser* After storing, SLAs are parsed using SLA parser. This module searches for the compulsory standard parameters in SLA that must be provided by the CSP to increase its level of trust.
- *SLA trust estimation engine* In this component, the extracted security and privacy parameters from SLA parser are passed on to the SLA-based trust estimation engine for final calculation of SLA-based trust score. The parameters for trust estimation

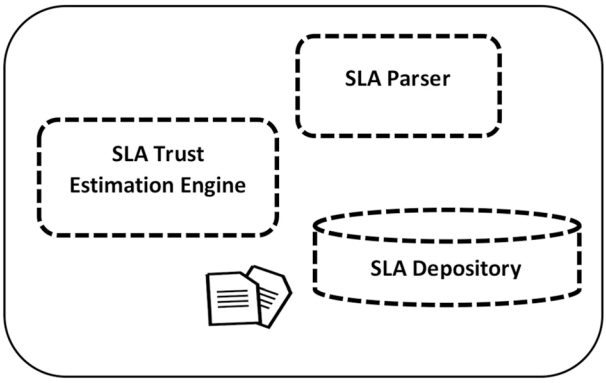

Fig. 2 Components of SLA module

Table 1 SLA trust estimation scaling

Scale	Value	Description
Critical	0.9	A critical scale applies to vulnerabilities that will interrupt the system completely and a complete system compromise will occur along with easy exploitation
Medium	0.8	A medium scale applies to vulnerabilities that will not interrupt system as a whole but have a huge impact on security concerns of system
Low	0.7	This scale applies to vulnerabilities that depend on unlikely situations in order to interrupt the system. These situations include a flawed or unlikely configuration of the system be in place

include confidentiality, Authentication, Access Control, Integrity, Backup, Availability, Encrypted Storage and SLA updates [17]. The scaling is depicted in Table 1.

The SLA-based trust score S_{SLA} is calculated using Eq. 1.

$$S_{SLA} = \frac{\sum_{i=0}^{n}(L_i * SP_i) + (m * \tau)}{|Np|} \tag{1}$$

where N_p is total number of parameters that are taken as standard features of security and privacy concerns. L_i represents the level assigned to each parameter accordingly. SP_i is the i^{th} security parameter that is taken, m is the margin of error [7] and is calculated using Eq. 2. τ defines the threshold for evaluation of trust which is calculated using Eq. 3.

$$m = \frac{N_l}{(N_p + N_l)} \tag{2}$$

N_l represents the total no. of levels defined for scaling purposes.

$$\tau = \frac{1}{N_l} \tag{3}$$

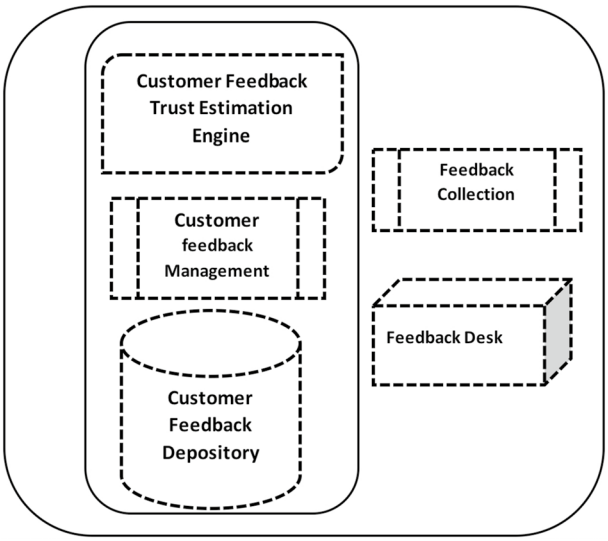

Fig. 3 Components of customer feedback module (CFM)

3.2.3 Customer feedback module (CFM)

Feedback allows the customer to estimate different parameters in a systematic way [3]. Suppose a CSP's customer can give his opinion about the security and privacy concerns of that CSP through submitting feedback. This proves to be a very successful methodology as by analyzing the feedback CSP can possibly overcome its weakness it can increase its customers and strengthen economically. In the proposed FCTMF, Feedback Module is broadly divided into CFM and CSP Feedback Module. CFM collects all the responses from the registered customers. Figure 3 shows the CFM and its components and are discussed below.

- *Feedback desk* Feedback desk directs the customer/ CSP about the type of feedback to be filled in. If the feedback is from the customer, it directs it to the CFM and if it's from CSP shifts the control to CSP-FM.
- *Feedback collection* The task of Feedback collection Module is to collect the feedback regarding security and privacy parameters available by the targeted CSP. For the customer feedback, the process is to collect it in the form of a provided questionnaire which is filled by the registered customers. This questionnaire contains 30 questions to be answered according to the individual experience.
- *Customer feedback depository* The function of CFM is to collect the submitted feedback from the customer by the Feedback collection Module. This module also stores the basic information of the customers.
- *Customer feedback management* This module provides database management services of the stored data of the customer feedback [8]. Collected feedback is then passed on to the customer feedback estimation engine for trust evaluation.
- *Customer feedback trust estimation engine* It collects the feedback of the registered customers from the customer feedback management module and calculates the final trust score of this module. Mathematical logic is applied [11] for the calculation of final customer feedback-based trust score. The trust score is calculated based on different options provided by the module and the respective customer responses, using Eq. 4. Here Pr is the positive response calculated using Eq. 5, Nr is calculated using Eq. 6, it represents the negative response and Ur relates to uncertain response given by the customer for the targeted CSP and is calculated using Eq. 7. Total trust score of individual customers is T^{C}_{csp} which is calculated using Eq. 4, whereas N represents the total number of customers giving responses about the targeted CSP. Individual trust score by the customer is calculated using Eq. 8.

$$T^{C}_{csp} = (Pr, Nr, Ur, m, \tau) \tag{4}$$

$$Pr = \frac{positive\_response}{collected\_response + N_s} \tag{5}$$

$$Nr = \frac{negative\_response}{collected\_response + N_s} \tag{6}$$

$$Ur = \frac{uncertain\_response}{collected\_response + N_s} \tag{7}$$

$$T_{csp}^{C1}, T_{csp}^{C2}, T_{csp}^{C3}, \ldots, T_{csp}^{CN} \tag{8}$$

Here m represents the margin of error and is calculated using Eq. 9, and τ is the threshold value calculated using Eq. 10.

$$m = \frac{N_s}{collected\_response + N_s} \tag{9}$$

$$\tau = \frac{1}{N_s} \tag{10}$$

where N_s defines the total number of scales defined for a customer to give responses. After calculating the individual customer trust score on a CSP from Eq. 4, the overall trust score of a CSP is calculated by combining all the responses from all the customers this is shown by the Eqs. 11, 12, 13, 14 and 15, respectively.

$$T_{csp}^{C1} + T_{csp}^{C2} = (Pr_{new}, Nr_{new}, Ur_{new}, m_{new}, b_{new}) \tag{11}$$

$$Pr_{new} = \frac{(Pr_{csp}^{C1} + m_{csp}^{C2}) + (Pr_{csp}^{C2} * m_{csp}^{C1})}{m_{csp}^{C1} + m_{csp}^{C2} - m_{csp}^{C1} * m_{csp}^{C2}} \tag{12}$$

$$Nr_{new} = \frac{(Nr_{csp}^{C1} + m_{csp}^{C2}) + (Nr_{csp}^{C2} * m_{csp}^{C1})}{m_{csp}^{C1} + m_{csp}^{C2} - m_{csp}^{C1} * m_{csp}^{C2}} \tag{13}$$

$$Ur_{new} = \frac{(Ur_{csp}^{C1} + m_{csp}^{C2}) + (Ur_{csp}^{C2} * m_{csp}^{C1})}{m_{csp}^{C1} + m_{csp}^{C2} - m_{csp}^{C1} * m_{csp}^{C2}} \tag{14}$$

$$m_{new} = \frac{m_{csp}^{C1} * m_{csp}^{C2}}{m_{csp}^{C1} + m_{csp}^{C2} - m_{csp}^{C1} * m_{csp}^{C2}} \tag{15}$$

Trust score given by the individual customer is combined with the trust score provided by other customers. This operation is executed iteratively until the final trust score is achieved. The expected score of trust of a CSP by the individual customer is calculated using Eq. 16.

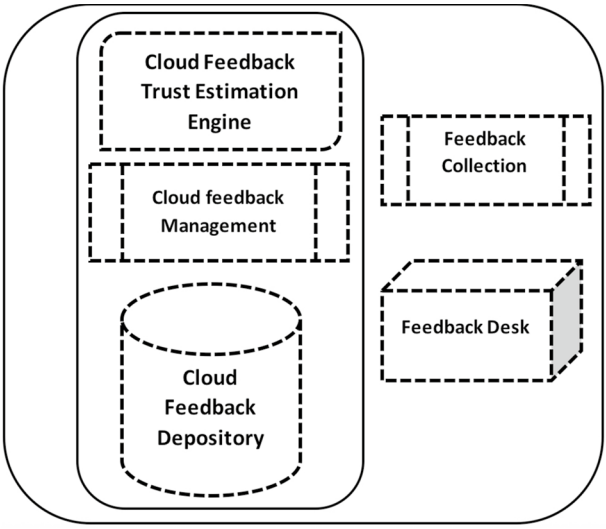

Fig. 4 Components of CSP feedback module

$$S_e = Pr_i + m_i * \tau_i \tag{16}$$

where Pr_i is the positive response of a customer, and m_i and τ_i are the margin of error and threshold values, respectively.

3.2.4 CSP feedback module (CSP-FM)

Figure 4 shows the cloud feedback module and its components. It collects all the responses from all the registered CSPs. It includes the following components:

- *Feedback desk* Feedback desk directs the customer/ CSP about the type of feedback to be filled in. If the feedback is from the customer, it directs it to the CFM and if it's from CSP, it shifts the control to CSP-FM.
- *Feedback collection* The task of Feedback collection Module is to collect the feedback about available parameters of security and privacy of a CSP. For the CCSP-FM, the feedback is collected by concerned CSP's about the individual targeted CSP in the form of a questionnaire. It includes different standard attributes about that CSP and the registered CSPs rate it according to their level of concern regarding each attribute. These are then categorized into three levels high, moderate and low that are marked according to the targeted CSP performance.
- *Cloud feedback depository* The function of this component is to collect the submitted feedback and store it.
- *Cloud feedback management* This module performs the management of the storage of the cloud feedback at the backend database. All the feedback that is col-

lected is then passed on to the cloud feedback estimation engine for the final trust evaluation score.

– *Cloud feedback trust estimation engine* It collects the feedback from Cloud Feedback Management Module and calculates the final trust score. Mathematical logic is applied [26] for the calculation of final Cloud-based feedback trust score. The feedback is based on responses of several registered peer clouds that are using the services of the targeted cloud. Every peer CSP gave an opinion about the respective CSP that includes certain standard features defined in the provided questionnaire. Against these standard features peers have to give responses.

The total score of the defined feature marked by all participating peers T_f is evaluated by using Eq. 17.

$$T_f = \sum_{i}^{T_{peer}} \frac{(W_i * peer_i)}{peer_i} \tag{17}$$

where W_i is the weight given by module according to a specific criteria, T_{peer} represents the total number of peers participating in evaluation of trust, $peer_i$ represents the individual score given by peer CSPs participating in evaluating trust. Total Trust score for Cloud Feedback Estimation Engine S_{CLOUD} is calculated using Eq. 18:

$$S_{CLOUD} = \left[\frac{\sum_{i=0}^{F_T} T_f)}{|T_{peer}|} \right] * (m * \tau) \tag{18}$$

where F_T is the total number of features defined in the questionnaire and total number of levels defined for giving response is N_l. Similarly, margin of error m and threshold value τ is calculated using Eqs. 19 and 20, respectively.

$$m = \frac{N_l}{T_{peer} + N_l} \tag{19}$$

$$\tau = \frac{1}{N_l} \tag{20}$$

Table 2 Defined range of trust

Final trust score	Trust range	Trust level
$0.0 < T_{SCORE} < 0.2$	ROT 1	Low
$0.2 < T_{SCORE} < 0.4$	ROT 2	Medium
$0.4 < T_{SCORE} < 0.6$	ROT 3	Medium
$0.6 < T_{SCORE} < 0.8$	ROT 4	High
$0.8 < T_{SCORE} < 1.0$	ROT 5	High

3.2.5 Final trust evaluation module

This module is responsible for the collection of the evaluated trust scores from all the proposed FCTMF modules (SM,CFM, CSP-FM) [20]. It combines these trust values and calculates an aggregated final trust score T_{SCORE} of the targeted CSP by using Eq. 21:

$$T_{SCORE} = \frac{S_{SLA} + S_c + S_{CLOUD}}{3} \tag{21}$$

where S_{SLA}, S_c and S_{CLOUD} represent trust scores from SLA trust estimation engine, customer trust estimation engine and cloud trust estimation engine, respectively. The range of the calculated trust is determined by using Table 2. This will help in determining the trustworthiness of the targeted CSP.

4 Implementation and results

4.1 Experimental setup

The proposed FCTMF is implemented in Java J2EE Eclipse. For complete database storage, MySQL is used. For the experimental setup, three cloud setup is formed on Linux machines using open source cloud OpenStack. FCTMF is deployed on one cloud, and two other participating CSPs are deployed on the other two cloud setups. All the participating clouds are communicating using Security Assertion Markup Language (SAML) version 2.0 protocol [10].

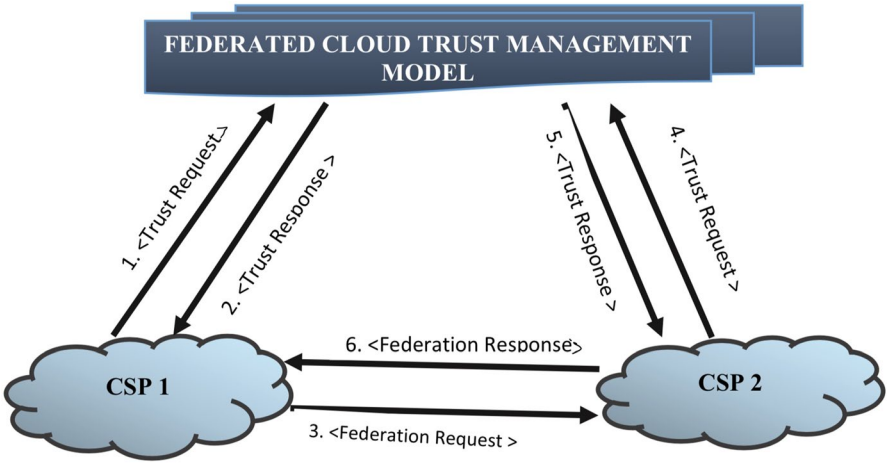

Fig. 5 Workflow for establishment of trusted federation

4.2 Implementation

The two participating CSPs need to establish a trusted environment between them so they could build a trusted federation to share their available resources to get maximum benefit. The presented protocol is based on Trust Score (TS), Level of Trust (LOT) and Range of Trust (ROT) to establish federation. Figure 5 shows the series of operations that are performed during federation establishment between two CSPs. The procedure for the proposed FCTMF is presented in the following steps:

- *Step 1* The mechanism starts when a CSP who wants to establish a trusted federation sends a Trust Request to the FCTMF and requests for the trust attributes of the targeted CSP. For the above scenario, CSP1 is the Trust Requestor.
- *Step 2* The FCTMF authenticates the request from CSP1, and the function moves to the proposed modules namely SLA extraction, Feedback from customers and feedback from peer CSPs for evaluation of trust attributes. The requested trust score for CSP2 is calculated. After evaluating the trust attributes, FCTMF sends a Trust Response containing the Trust Statement for CSP2. The < *Subject* > of this statement is CSP2 whereas FCTMF is the Issuer of the assertion. The FCTMF is the Trust Responder.
- *Step 3* Then the Trust Request is extracted by CSP1, and all the trust attributed are read from it. Then it compares the provided trust score with the predefined trust threshold value. If the value of trust attributes that are provided is greater than the predefined threshold value then a Federation Request is forwarded to the targeted CSP2 from CSP1. On the other hand, if the Trust Score is lower than the value of predefined threshold then CSP1 pursues for another CSP to establish trusted federation.
- *Step 4* Another operation is performed before sending a response for the Federation Request. The targeted CSP2 also calculates the trustworthiness of CSP1. For this, CSP2 generates a Trust Request for the trust attributes of CSP1 and forwards it to the proposed FCTMF. Thus CSP2 becomes a Trust Requestor for CSP1.
- *Step 5* Then the FCTMF receives the request from CSP2 and confirms this request. The FCTMF calculates the trust score, LOT and ROT for CSP1.

  Trust Evaluation Framework then prompts the SAML < *TrustResponse* > that holds the CSP1 Trust statement (includes Trust Score value, SLA, ROT and LOT of CSP1). Here the FCTMF renders as a Trust Responder. Then all the encrypted assertions are forwarded to CSP2. Here FCTMF is the < *Issuer* > of the assertion and the < *Subject* > of this response is CSP1.
- *Step 6* The last step begins when CSP2 extracts the trust attributes after verifying the assertion and compares the values with its own pre-defined threshold values for trust. If this value of CSP1 is copacetic then CSP2 prompts an acceptance response for federation request. In case of low trust value, a corresponding rejection message is generated.

Table 3 Trust value calculation using SLA parameters

Parameters included	Parameters presence	Value assign	$(L_i * SP_i)$	Final SLA trust value
Confidentiality	SLA contains confidentiality	0.9	(1*0.9)	
Integrity	Does not contain integrity	0.8	(0*0.8) + (1*0.9)	$S_{SLA} =$
Authentication	SLA contains authentication	0.7	(1*0.7) + (0*0.8) + (1*0.9)	$\frac{\sum_{i=0}^{n}(L_i * SP_i)+(m*\tau)}{\lvert Np\rvert}$
Access control	SLA includes access control	0.9	(1*0.7) + (0*0.8) + (1*0.9) + (1*0.9)	= ((1*0.7) + (0*0.8) + (1*0.9) + (1*0.9) + (1*0.9) + (0*0.8) + (1*0.9) + (0*0.7)) * (0.2 *0.33) /(8)
Data backup and recovery	SLA contains data backup and recovery	0.9	(1*0.7) + (0*0.8) + (1*0.9) + (1*0.9) + (1*0.9)	= 0.545
Encrypted storage	Does not contain encrypted storage	0.8	(1*0.7) + (0*0.8) + (1*0.9) + (1*0.9) + (1*0.9) + (0*0.8)	
Availability	SLA contains availability	0.9	(1*0.7) + (0*0.8) + (1*0.9) + (1*0.9) + (1*0.9) + (0*0.8) + (1*0.9)	
SLA updates	Does not contain SLA updates	0.7	(1*0.7) + (0*0.8) + (1*0.9) + (1*0.9) + (1*0.9) + (0*0.8) + (1*0.9) + (0*0.7)	

Table 4 Customer feedback-based trust module results

No.	Feedback			Trust vector	Trust acore	
	+ive	−ive	Unsure	$T^{C}_{csp} = (p_f, n_f, U_f, m, \tau)$	Cumulative	Final
C 1	15	5	10	T^{C1}_{csp} = (0.454, 0.151, 0.303 ,0.090 ,0.333)	–	–
C 2	15	13	2	T^{C2}_{csp}=(0.454, 0.393, 0.060, 0.090, 0.333)	$T^{C1}_{csp} + T^{C2}_{csp} = (p_{f_n ew}, n_{f_n ew}, U_{f_n ew}, m, \tau_n ew)$ (0.476, 0.285, 0.190, 0.047, 0.333)	S_{u_1}= 0.492
C 3	7	10	13	T^{C3}_{csp} =(0.393, 0.303, 0.212, 0.090, 0.333)	Resultant + T^{C3}_{csp} (0.462, 0.301, 0.204, 0.032, 0.333)	S_{u_2} = 0.473
C 4	19	2	9	T^{C4}_{csp}=(0.575, 0.060, 0.272, 0.090, 0.333)	Resultant + T^{C4}_{csp} (0.504, 0.243, 0.227, 0.0243, 0.333)	S_{u_3} = 0.512
C 5	3	17	10	T^{C5}_{csp}=(0.303, 0.515, 0.090, 0.090, 0.333)	Resultant + T^{C5}_{csp} (0.470, 0.307, 0.202, 0.019, 0.333)	S_{u_4} = 0.477
C 6	10	15	5	T^{C6}_{csp} = (0.303, 0.454, 0.151, 0.090, 0.333)	Resultant + T^{C6}_{csp} (0.448, 0.338, 0.196, 0.016, 0.333)=	S_{u_5}= 0.453

Table 5 Cloud feedback-based trust module results

Standard attributes	Score by peer			Score of individual attribute	Final trust score
	1	2	3	$T_f = \sum_i^{T_peer} \frac{(W_i * peer_i)}{peer_i}$	
Scalability	0.4	0.2	0.6	0.6	
Availability of data centre zones	0.4	0.4	0.4	0.6	$S_{CLOUD} =$
Data retention	0.2	0.4	0.2	0.4	$\left[\frac{\sum_{i=0}^{F_T} T_f}{\lvert T_{peer}\rvert}\right]$
Premium support	0.6	0.4	0.6	0.4	$* (m * \tau)$
Features stability (security, computing, performance)	0.2	0.2	0.2	0.2	$= 0.565$
Rating (reviews, opinion)	0.6	0.6	0.4	0.2	

Table 6 Final trust score evaluation and results

SM,CFM, CSP-FM trust scores	
$S_{SLA} = \frac{\sum_{i=0}^{n}(L_i * SP_i)+(m*\tau)}{\lvert Np\rvert}$ $= 0.56135$	$T_{SCORE} = \frac{S_{SLA}+S_u+S_{CLOUD}}{3}$
$S_u = p_{fi} + m_i * \tau_i = 0.453$	$T_{SCORE} = \frac{0.561+0.453+0.565}{3}$
$S_{CLOUD} = \left[\frac{\sum_{i=0}^{F_T} T_f}{\lvert T_{peer}\rvert}\right] * (m * \tau)$ $= 0.565$	$T_{SCORE} = 0.5263$

4.3 Results and discussion

The results fabricated by using the above policies implemented in SAML for the proposed FCTMF are discussed in this section.

Table 3 shows results for trust score obtained from SLA-based mechanism. For this, we identified eight parameters for trust assurance. The SLA parser module does not find Integrity, encrypted data and proper SLA updates. The weights allocated by the model are applied to these extracted parameters as high (0.9) moderate (0.8) or low (0.7). Then the final SLA score $S_{SLA}$is calculated and shown in last column of the Table 3.

Table 4 shows the results for CFM for trust evaluation of the targeted CSP. We consider six registered customers for customer-based feedback module. The process begins when the customers submitted their feedback through a questionnaire provided by the Feedback collection Module. This questionnaire consists of thirty questions about the targeted CSP. Third, fourth and fifth columns of Table 4 represent the positive, negative and uncertain feedback responses submitted by the customers. Then the combined cumulative trust score is calculated by adding the resultant of the first two individual trust scores provided with the next customer trust score and so on. These customer feedback are denoted as S_{c1}, S_{c2}, S_{c3} andS_{c4}. Finally, S_{c5} is the final trust score as it represents the feedback-based trust value

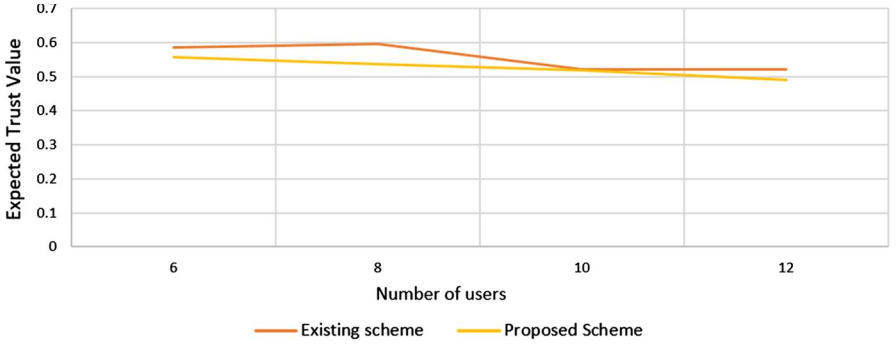

Fig. 6 Comparison of existing model [12] and our proposed framework with respect to increase in the number of customers

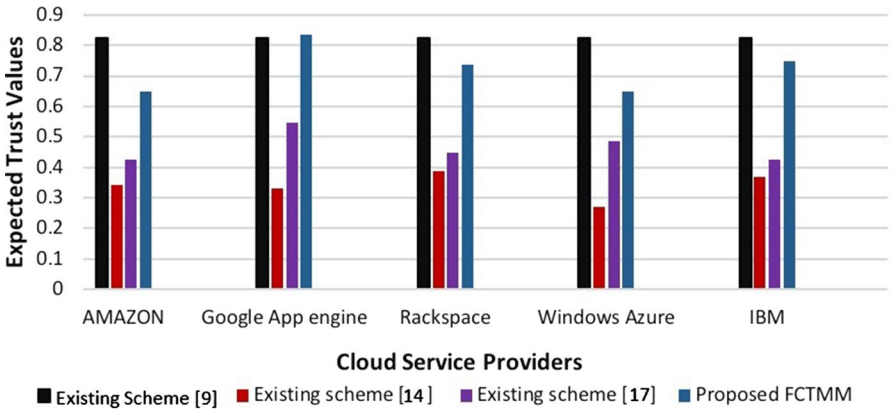

Fig. 7 SLA-based comparison using existing and proposed schemes between different CSPs

for the CFM. This value also depends on the number of customers providing their feedback.

Table 5 shows the results for CSP-FM for the evaluation of individual CSP. We took six essential parameters for measuring trust value that is shown in column 1. The registered CSP submitted their feedback through a questionnaire provided by the feedback collection module. This questionnaire consists of six parameters about the targeted CSP. The 2nd, 3rd and 4th columns reflect the score that participating CSP (who are already using that targeted CSP services) have submitted. The final value for CSP-FM is calculated according to the formula shown in Table 5. The final value for CSP-FM S_{CLOUD} is calculated in the last column. Final trust score T_{SCORE} is calculated by adding the resultant trust scores from the three mechanisms used as shown in the Table 6.

The range of trust is determined by using Table 2. This will help in determining the CSPs trust score which will help in possible decision making for making a cloud federation.

4.4 Comparative analysis

In Fig. 6, proposed FCTMF is compared with the existing scheme [12] that uses customer feedback to calculate trust score. Trust score is calculated with respect to increase in the number of customers. The comparison shows that the proposed FCTMF shows better results than the existing scheme [12]. As with increase in the number of customers feedback the trust score becomes high or low. So with the increase in customer feedback more evident results are produced because the opinion of more customers will all together be true about a CSP reputation. The trust level of the targeted CSP becomes more reliable as more customers provide their feedback.

In Fig. 7 comparative analysis is performed among different CSPs for SLA-based trust calculation scores. For analysis, we select 5 known CSPs and their SLA, considering our selected SLA parameters for calculating SLA-based trust score. These parameters are Authentication, Integrity, Confidentiality, Access Control, Backup, Availability, Encrypted Storage and SLA updates. These are the key parameters that contribute to building a trusted cloud federated environment for the participating CSPs. From Fig. 7, it can be seen that our proposed FCTMF provides better results than the other because it considers all the parameters defined for a good trusted relationship. Other schemes do not consider these factors altogether for the CSP trust score. As from [12], it can be seen that using this scheme the Trust score becomes constant. This indicates false trust value as constant line means no change in value with the increase in customer feedback.

4.5 Robustness of proposed FCTMF

The reliability and improved methodology of the proposed FCTMF can be proved by performing a quantitative analysis of the proposed framework with other existing schemes. In Table 7, it can be seen that our proposed framework is compared with other state of the art research prototypes with respect to the modules considered to calculate trust scores. It is evident that our framework includes more perspectives for trust score calculation. Table 8 shows the qualitative analysis on SLA parameters for SLA trust calculation values. In this table, it is clearly seen that more accurate and precise parameters are chosen for trust calculation. Thus, when our proposed framework is compared with other state of the art research, it produces better results.

5 Conclusion and future work

In a cloud environment to make sure that the customer data is fully secured and standard privacy laws are applied, it is essential to form a trusted relationship and estimate the level of trust between the participating CSPs who want to make a reliable federation.

Table 7 Qualitative analysis based on different modules

Year	Authors	Paper name	Parameters		
			SLA	Customer Feedback	Cloud Feedback
2021	R. Latif, H. Afzaal and S. Latif	Proposed framework	✓	✓	✓
2018	A. M. Mohammed, E. I. Morsy and F. A. Omara [16]	A trust model for cloud service consumers	X	✓	X
2016	Z.tan, Y. Niu and G.Yang [25]	A novel trust model based on SLA and behavior	✓	X	X
2014	A. Kanwal, R. Masood, and M. A. Shibli [12]	Evaluation and establishment of trust in cloud federation	✓	✓	X
2014	N. Agheli, B. Hosseini and A. Shojaee [2]	A trust evaluation model for selecting service provider in cloud environment	X	✓	X
2013	Z. Raghebi and M. R. Hashemi [19]	A new trust evaluation method based on reliability of customer feedback for cloud computing	X	✓	X
2013	S. Wang, J. Wei, L. Sun, Q. Sun and F. Yang [27]	Reputation measurement of cloud services based on unstable feedback ratings	X	✓	X
2013	K. Ravindran [21]	QoS auditing for evaluation of SLA in cloud-based distributed services	✓	X	X
2012	Li, X. and Du, J. [14]	Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing	✓	X	X
2010	H. Sato, A. Kanai and S. Tanimoto [22]	A cloud trust model in a security aware cloud	✓	X	X

Table 8 Qualitative analysis based on SLA trust parameters

Paper name	Parameters							
	Confi-dentiality	Integrity	Authentication	Access control	Backup & recovery	Encrypted storage	Availability	SLA updates
Proposed framework	✓	✓	✓	✓	✓	✓	✓	✓
A novel trust model based on SLA and behavior evaluation for clouds [25]	X	✓	X	X	✓	X	✓	X
Evaluation and establishment of trust in cloud federation [12]	✓	✓	✓	✓	X	X	X	X
SLA-based trust model for cloud computing [4]	X	X	X	X	X	X	X	✓

This research identifies the issue of establishment of a trusted environment and evaluation of trust level between CSPs to take participation in cloud federation for the best utilization of computing resources for their customers. It includes comprehensive analysis of existing schemes for evaluation of trust between CSPs in federated environments.

A Federated Cloud Trust Management Framework is proposed to ensure the security of critical and sensitive data of customers and CSPs participating in trusted federated environments. The proposed framework includes three different mechanisms for calculating trust including SLA parameters for trust, feedback from customers and feedback from CSPs. The results show improved trust calculations to form a trusted cloud federation as compared to existing trust calculation techniques.

In real world scenarios, our proposed framework can be used to increase business value for a CSP, as the main purpose of any business is to increase profit while decreasing cost. Any cloud platform has the ability to decrease cost in several ways by forming a trusted federation and resource sharing. Due to economic hardships, cloud service businesses begin to downsize. In this case, federated cloud platforms can serve as a tool to not only decrease costs but simultaneously increase profit, build better business relations and remain current on technological advances.

The future directions may include trust calculation based on the in-depth architectural analysis of CSPs including study on CSP IaaS platform, analysis of existing protocols and use of several protocols for trust validation. Recommendation and reputational-based analysis of individual CSP can also be performed to extend this work. As with time, the level of trust of a CSP can increase or decrease so our proposed methodology can further be enhanced to calculate the trust score attractively and update the trust value.

Acknowledgements This work was supported by the Artificial Intelligence Data Analytics Lab (AIDA) CCIS, Prince Sultan University, Riyadh, Saudi Arabia. Authors are thankful for the support.

References

1. Aarthy DK, Aarthi M, Farhath KA, Lakshana S, Lavanya V (2017) Reputation-based trust management in cloud using a trusted third party. In: 2017 Third International Conference on Science Technology Engineering Management (ICONSTEM), pp 220–225
2. Agheli N, Hosseini B, Shojaee A (2014) A trust evaluation model for selecting service provider in cloud environment. In: 2014 4th International Conference on Computer and Knowledge Engineering (ICCKE), pp 251–255
3. Akinola AT, Adigun MO (2016) Feedback-based service selection in ad-hoc mobile cloud computing. In: 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE), pp 172–177
4. Alhamad M, Dillon T, Chang E (2010) Sla-based trust model for cloud computing. In: 2010 13th International Conference on Network-Based Information Systems (pp 321–324). IEEE
5. Bendiab K, Shiaeles S, Boucherkha S (2018) A new dynamic trust model for "on cloud" federated identity management. In: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp 1–5
6. Challagidad PS, Birje MN (2019) Determination of trustworthiness of cloud service provider and cloud customer. In: 2019 5th International Conference on Advanced Computing Communication Systems (ICACCS), pp 839–843

7. Chen L, Zhang H (2019) Statistical margin error bounds for l1-norm support vector machines. Neurocomputing 339:210–216
8. Ding D, Li Y, Ai L, Luo S (2012) An adaptive resource scheduling mechanism based on user behavior feedback in cloud computing. In: 2012 13th International Conference on Parallel and Distributed Computing, Applications and Technologies, pp 543–547
9. Ghafoorian M, Abbasinezhad-Mood D, Shakeri H (2019) A thorough trust and reputation based rbac model for secure data storage in the cloud. IEEE Trans Parallel Distrib Syst 30(4):778–788
10. Hughes J, Maler E (2005) Security assertion markup language (saml) v2. 0, technical overview
11. Jøsang A, McAnally D (2005) Multiplication and comultiplication of beliefs. Int J Approx Reason 38(1):19–51
12. Kanwal A, Masood R, Shibli MA (2014) Evaluation and establishment of trust in cloud federation. In: Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication. Association for Computing Machinery
13. Kaushik S, Gandhi C (2019) Multi-level trust agreement in cloud environment. In: 2019 Twelfth International Conference on Contemporary Computing (IC3), pp 1–5
14. Li X, Junping D (2013) Adaptive and attribute-based trust model for service-level agreement guarantee in cloud computing. IET Inf Secur 7(1):39–50
15. Ma S, Shuai X, Zhou Z, Qiao K (2018) Bionic mechanism based dynamic trust evaluation method in cloud environment. In: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), pp 136–141
16. Mohammed AM, Morsy EI, Omara FA (2018) Trust model for cloud service consumers. In: 2018 International Conference on Innovative Trends in Computer Engineering (ITCE), pp 122–129
17. Patel P, Ranabahu A, Sheth A(2009) Service level agreement in cloud computing
18. Prajapati A. G, Sharma S. J, Badgujar V. S (2018) All about cloud: A systematic survey. In: *2018 International Conference on Smart City and Emerging Technology (ICSCET)*, pp 1–6
19. Raghebi Z, Hashemi MR (2013) A new trust evaluation method based on reliability of customer feedback for cloud computing. In: 2013 10th International ISC Conference on Information Security and Cryptology (ISCISC), pp 1–6
20. Rajendran VV, Swamynathan S (2016) Parameters for comparing cloud service providers: a comprehensive analysis. In: 2016 International Conference on Communication and Electronics Systems (ICCES), pp 1–5
21. Ravindran K (2013) Qos auditing for evaluation of sla in cloud-based distributed services. In: *2013 IEEE Ninth World Congress on Services*, pp 247–254
22. Sato H, Kanai A, Tanimoto S (2010) A cloud trust model in a security aware cloud. In: 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet, pp 121–124
23. Singh S, Chand D (2014) Trust evaluation in cloud based on friends and third party's recommendations. In: 2014 Recent Advances in Engineering and Computational Sciences (RAECS), pp 1–6
24. Sun PJ (2019) Research on the tradeoff between privacy and trust in cloud computing. IEEE Access 7:10428–10441
25. Tan Z, Niu Y, Liu Y, Yang G (2016) A novel trust model based on sla and behavior evaluation for clouds. In: 2016 14th Annual Conference on Privacy, Security and Trust (PST), pp 581–587
26. Rehman Z, Hussain OK, Parvin S, Hussain FK (2012) A framework for user feedback based cloud service monitoring. In: 2012 Sixth International Conference on Complex, Intelligent, and Software Intensive Systems
27. Wang S, Wei J, Sun L, Sun Q, Yang F (2013) Reputation measurement of cloud services based on unstable feedback ratings. In: 2013 International Conference on Parallel and Distributed Systems, pp 474–479
28. Wang Y, Wen J, Zhou W, Luo F (2018) A novel dynamic cloud service trust evaluation model in cloud computing. In: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)
29. Yan Z, Holtmanns S (2008) Trust modeling and management? From social trust to digital trust. Computer Security. Privacy and Politics, Current Issues, Challenges and Solutions, pp 290–323

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.