International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/217708 Volume 9, Issue 6, November – December (2022)

REVIEW ARTICLE

Trust Management Techniques and their Challenges in Cloud Computing: A Review

Pooja Goyal
Department of Computer Science and Application, MD University, Rohtak (Haryana), India.
poojagoyal895@gmail.com

Sukhvinder Singh Deora
Department of Computer Science and Application, MD University, Rohtak (Haryana), India.
sukhvinder.singh.deora@gmail.com

Received: 13 October 2022 / Revised: 01 December 2022 / Accepted: 10 December 2022 / Published: 30 December 2022

Abstract – Cloud computing is a way to handle tasks like development, production, and maintenance done on the web. This domain is evolving. It uses a pay-per-use system like an electric bill and can be used to run virtual machines. Customers are rapidly adopting and shifting the companies that provide such services due to the presence of numerous service providers. It is also customizable as per users' requirements but poses several security risks. It is dynamic and can be updated to meet the needs of both the client and the service provider. It is a significant feature of such distributed computing platforms. However, this undermines trust and credibility and generates security, protection, individuality, and authenticity problems. Consequently, selecting an appropriate service provider is the most critical test in the cloud environment. The Trust system is an essential part of how QoS and feedback ratings are judged to evaluate the service. Even so, the executive's plan for observing and evaluating QoS still needs to get past several tests. This paper examines the current impediments to trust in the existing trust framework. This report includes a systematic review of various high-quality articles published on trust management between 2010 and July 2022. To do this, some strategies for managing trust are put into four groups: SLA, suggestion, feedback, and prediction. This article also compares the pros and cons, evaluation methods, tools, and simulation settings of different management models.

Index Terms – False Rating, Subjectivity, Cloud Environment, Service Level Agreement, Reputation System, Quality of Service (QoS).

1. INTRODUCTION

In the current scenario, cloud computing serves as the frontal cortex of web design. Still, dispersed processing isn't perfect because it's constantly changing, hard to understand, not clear, and open to anyone. When it comes to what happens to their data once it has been uploaded to the cloud, customers have a dubious point of view. Before making any decisions, they think about who will have access to their data and how it will be kept, documented, shared, and used. Aside from that, the order of their data is not supported [1]. Customers experience a sense of vulnerability in this way when using cloud organizations.

Furthermore, any cloud organization's assurance depends on the QoS and limits set by expert centers. But the main problem is that clients need help measuring QoS for sure since the cloud's capabilities are constantly changing. Furthermore, the needs of customers shift depending on the requirements they have. Also, feedback from real customers is the most reliable way to figure out how cloud-based businesses are doing. However, this information is affected by a malicious component. Trust is used between a buyer and a provider to manage this fundamental obstacle.

Distributed registration gives you access to a pool of high-quality cloud-based resources (association, operating system, application, storage, server) at a lower price [1]. It operates based on compensation that can be accessed from any location, device, or time. SLAs include all information about the congruence of the represented QoS (quality of service) between clients and service providers.

Distributed registering is the delayed result of the expansion of the infinite accumulation of virtualization, the organization of structured design, autonomic, and utility processing [2] development organization that helps their enrolment operations [3,4,5]. Trust is a common understanding between two substances that need to talk with each other for business purposes.

The trustworthiness is classified as theoretical or objective [6]. Through help-level agreements, target trust is assessed among administered and surveyed organizations. So, when the expert association helps out according to the plan, it builds more trust. Analysis evaluations presented by various assistance purchasers are associated with unique trust. It depends upon the consumer's data and organizational tendencies during their coordinated effort [7]. When a client gives an expert association unique information, that client's trust in the expert association grows. Trust is passionate and depends on the feedback provider's knowledge and skill set [8]. Objective trust connects allotted and surveyed organizations through a high-level plan [9].

Hence, the trust of the expert association increases when it offers different kinds of services, as shown by the course of action. The concept of trust is linked to analysis evaluations presented by various assistance buyers. It depends upon the client's data and organizational tendencies during their association. Suppose a purchaser trusts an expert center with extraordinary information and the trust increases. In any case, trust is theoretical and depends on the understanding and willingness of purchasers. But simultaneously, some aggravating hardships are accessible in this system.

The best way to solve this problem is to create a complete cloud trust scheme that creates a safe environment for controlled, cost-effective cloud investments. Even though cloud trust evaluation is an essential part of trust management, many research articles don't look at it systematically. The main goal of this study is to look at the existing trust models, highlight the most critical problems with managing trust in the modern world, and then suggest a way to confirm trust in the use of cloud services.

The following is a concise summary of this paper:

- Providing the fundamental taxonomy and concept of trust, Cloud Computing.
- Providing an overview of the process for evaluating trust in cloud environments.
- Systematically discuss cloud trust models' processes and highlight their essential characteristics.
- Emphasizing the concerns and suggestions for establishing cloud computing system trust.

The remaining sections of the paper are organized as follows. The second section outlines the present scenario of cloud computing, its features, and its challenges. The third section provides an overview of trust with its semantics and terminology in the context of the cloud and discusses the issues of trust management. The fourth section provides an overview of several trust cloud models in the literature. Section five presents a comparative analysis of various trust computation techniques with their models. Section 6 is the discussion part. Section 7 concludes the paper.

2. CLOUD COMPUTING

Cloud computing is a conventional term that applies to getting administrations facilitated on the internet [10]. Cloud computing works on a per-utilized model, like water and power charges that are charged according to utilization. It is the reason why associations show their thoughtfulness regarding this innovation.

As per the American National Institute of Standards and Technology [11], "distributed computing is a model for qualifying on-demand network access to a common pool of adaptable figuring assets that can be immediately provisioned and conveyed with ostensible administration exertion on specialist organization affiliation." The functioning standards of distributed computing are virtualization and SOA (service-situated architecture), which uphold the multi-tenure idea where a few administrations (framework, programming) are shared by a huge arrangement of shoppers on different host stages with heterogeneous execution.

Among the fundamental elements are clients and server providers. Another different element is

Cloud Re-Seller: -They offer different types of assistance for the sake of the service supplier.

Cloud Auditors: They offered a declaration dependent on execution appraisal, security percentage, and data framework activity.

Cloud Carriers: They give availability (telecom, organization) to other cloud elements to guarantee better help provisioning.

2.1. Service Delivery Model

Cloud computing can be described as the sum of three essential help models as shown in Figure 1.

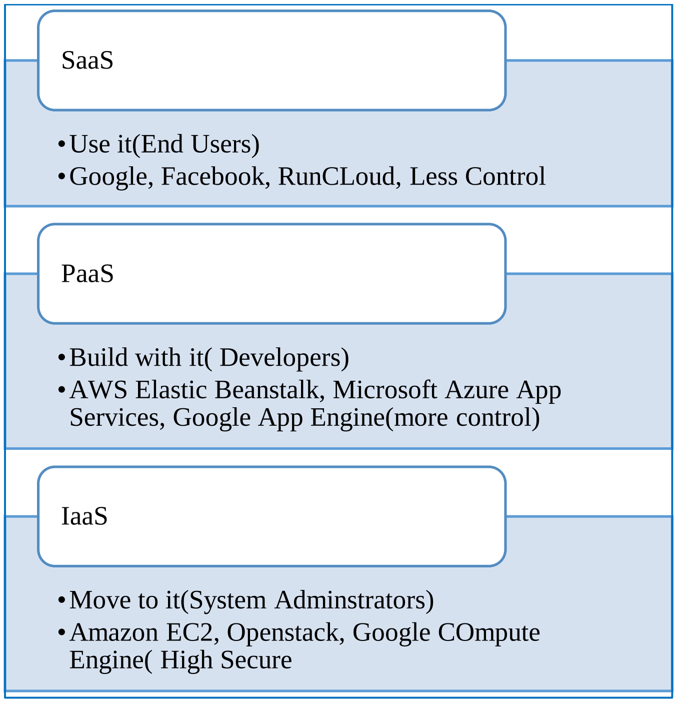
SaaS
•Use it(End Users)
•Google, Facebook, RunCLoud, Less Control
PaaS
•Build with it(Developers)
•AWS Elastic Beanstalk, Microsoft Azure App Services, Google App Engine(more control)
IaaS
•Move to it(System Adminstrators)
•Amazon EC2, Openstack, Google COmpute Engine(High Secure

Figure 1 Classification of Service Delivery Model

IaaS (Infrastructure as a Service) manages hardware assets such as inventory, machines, and networks. The virtualization strategy is employed to provide these actual assets so that cloud users can flexibly modify their systems according to their needs. Amazon, Google Compute Engine, EC2, and Microsoft Azure VM serve as models.

PaaS (Platform as a Service) refers to the stage as a support for its client. It incorporates framework assets just as it incorporates a working framework, data set, and program executable environment. It helps designers create, test, and run their applications—Google Application Engine, Amazon, Versatile Beanstalk, and Windows Azure processes.

SaaS (Software as a Service) assists with running programming. Customers utilize the provided cloud-based application in this scenario. Additionally, a web browser is required to access the application. Customers can oversee infrastructures such as networks, working frameworks, and stockpiling. Microsoft Office 365, Salesforce, Google Apps, OnLive, and AppExchange constitute the model.

2.2. Cloud Building Deployment Model

Cloud computing, sometimes referred to as a two-crossed-edged weapon, and provides comparable structure and management of the resources for clients and attackers to employ to their advantage. Consequently, when the wrong users have the same administrative privileges as cloud customers, they may do various destructive actions on customer data and deceive numerous honest consumers [12]. When they find ways to deal with bugs, they can make more attacks, write the right code, change a buyer's personal information, or use a customer's data.

The concept of distributed registration emerged in 1950 with the success of integrating waiter PCs accessible via unstable or static clients. From now until the foreseeable future, proper processing has been developed for both old and dynamic customers, programs, and organizations [13,14]. Distributed processing gives us a format with information about how different experts work together. Figure 2 represents the various deployment models of cloud computing.

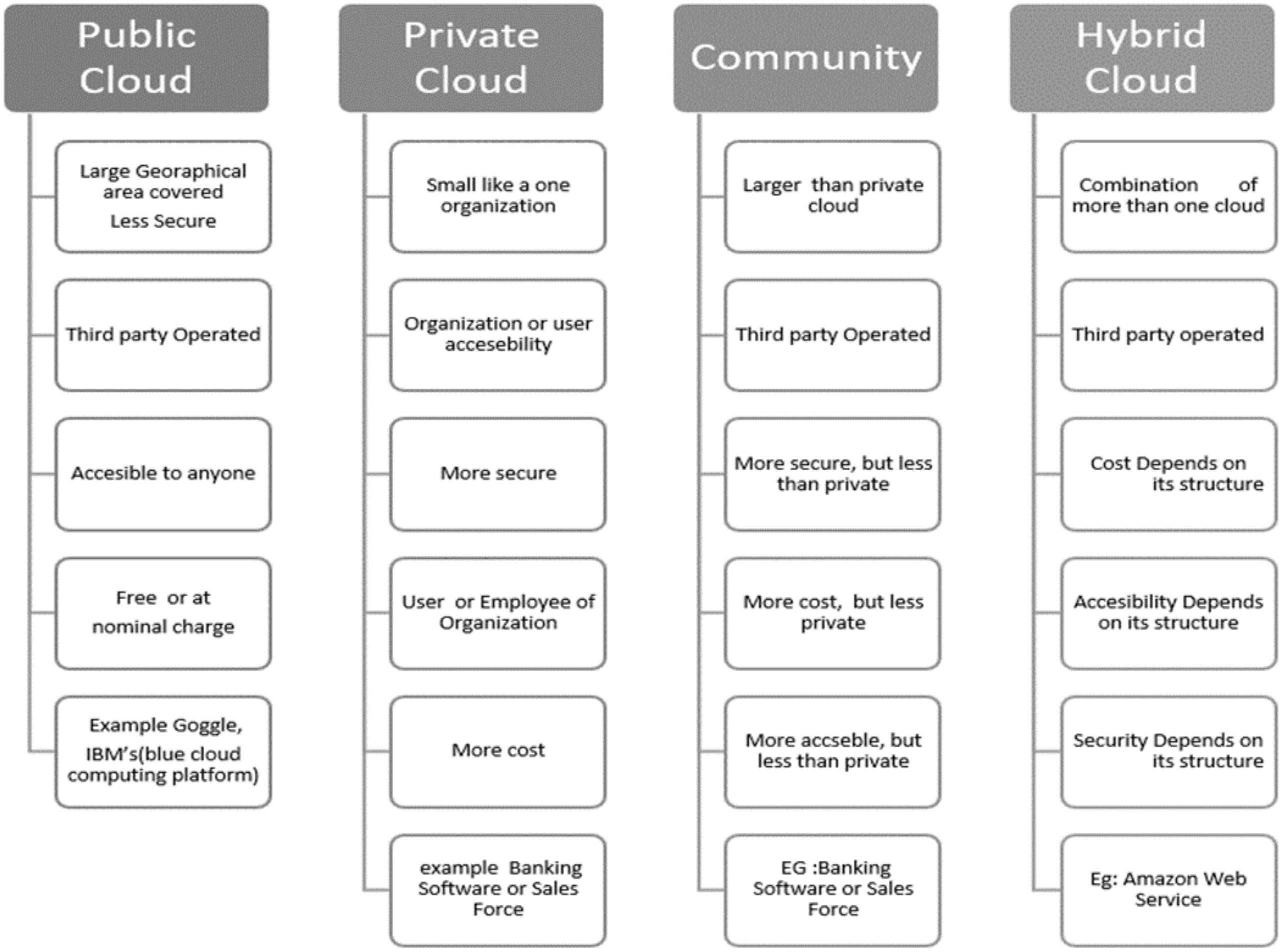
Public Cloud
Large Georaphical area covered
Less Secure
Third party Operated
Accesible to anyone
Free or at nominal charge
Example Goggle, IBM's(blue cloud computing platform)
Private Cloud
Small like a one organization
Organization or user accesebility
More secure
User or Employee of Organization
More cost
example Banking Software or Sales Force
Community
Larger than private cloud
Third party Operated
More secure, but less than private
More cost, but less private
More accseble, but less than private
EG :Banking Software or Sales Force
Hybrid Cloud
Combination of more than one cloud
Third party operated
Cost Depends on its structure
Accesibility Depends on its structure
Security Depends on its structure
Eg: Amazon Web Service

Figure 2 Classification of Types of Clouds

2.3. Security Issues Related to Cloud Computing

a) In a cloud environment, the service provider makes multiple copies of their data instead of giving customers full control over their data and stores it in different places to make the data more consistent and easier to find. It creates a dangerous situation with attackers [15].

(b) The cloud's accessibility depends on the web's increasing risk of browser vulnerabilities and capabilities. [16].

(c)Another issue is inadequate information deletion. There needs to be a way to must be a way to ensure the vendor can't get back the information d [17].

(d) The security system for a cloud climate is as old as the traditional IT climate. So, these systems are adequate for the cloud climate.

(e) The nature of the cloud is dynamic and murky. Subsequently, they can't handle unapproved access to buyers' information [18].

3. TRUST MANAGEMENT SYSTEM

In 1996, M. Burst introduced the concept of confidence (Matt Blaze. et.al 1999). In popular usage, trust is defined as an agreement between two entities, one of which serves the position of trustee and the other of which is the trustor. In the trust model, both parties exchange knowledge and resources to attain their respective goals. Trust is loose, like human conduct, and can't be portrayed and assessed quantitatively. "Trust depends on interpretation." Trust is a position that substantially distinguishes three perspectives: assumption, risk, and belief [18]. Similarly, the essential characteristic of trust is that it is difficult to attain and easy to lose. In addition, it is appropriate to note that the judgment is dynamic, as it can increase or decrease the value based on the trustee's continuous experience with various sources. There are several methods for measuring trust and esteem. Even though the processes would be distinct, the logic behind all equipment is the same and is known as the "Trust Model." TMS aims to improve the degree of confidence between consumers and service providers.

3.1. Aspects of Trust Assessment in Cloud Computing

The primary requirement is to understand the factors influencing cloud trust to establish faith in the cloud environment by avoiding conflicts in cloud trust management. Trust factors (TFs) are the variables that are examined while measuring cloud trust.

Security - Procedures, including encryption, make it difficult for an unauthorized individual to access sensitive data.

Privacy - The preservation of sensitive information from exposure or leaking.

Accountability - The duty of a person or organization to be responsible and answerable for the delivery of agreed services.

Auditability - The relative ease with which a framework or domain may be inspected.

3.2. Trust Management Techniques

The protocol, mechanism, and methods used for estimating the degree of trust are known as trust models. The analysis and identification of the trust model are based on its mechanism. The trust model is divided into four parts (as represented in Figure 3 with their domain):

3.2.1. Agreement-Based Trust Model (Policy Based)

In this approach, the cloud service provider and the cloud users construct and accept a mutual contract that declares the expectations and conditions of both the trustor and the trustee. This contract outlines the terms of the relationship between the two parties and consumers and specifies its security level and various QoS requirements for the required services. This contract is referred to as an SLA or service policy. The working principle of this type of trust model is the exchange of agreements between the cloud consumer and the service provider. Therefore, dynamic modification and monitoring of these contracts are vital for establishing confidence in a cloud environment.

3.2.2. Based on SLA (Service Level Agreement)

In the SLA model, the consumers specify various quality parameters for evaluating trust value. The concept of penalties and rewards with strict clauses controls the CSP and CU. An agreement containing predefined policies and conditions is known as an SLA agreement.

3.2.3. Based on Services Policies

In the service policy-based model, various policies are created by the service provider to provide the resources to the consumers.

There are two ways to check the completion level of services.

Entities' credibility, constituting security, availability, and response time, is measured in quantity or quality.

Feedback Credibility can be measured by a cloud server or by consumer experience.

Let ‘x’ be a CU with a set of policies Px, Cx is a set of Credentials of CU with a Tx set of thresholds, and Rx is the evaluated assessment.

Let ‘y’ be a CSP with a set of policies Py, Cy be a set of Credentials of CSP with Ty set of thresholds, and Ry is the evaluated assessment. (Referred to equation:1)

A trust relationship is maintained between CSP and CU if both satisfy the trust threshold.

$Tr(x,y)= \{ 1, Ry>= Tx \text{ and } Rx>= Ty , \text{ otherwise } 0 \}$ (1)

3.2.4. Recommendation-Based Trust Model

It is also known as the reference model. This mechanism is used when the consumer knows at least one source of trusted feedback. In this model, three agents play a significant role: the trustor, trustee, or recommender, who gives ratings or feedback to the trustee. But this model does not work accurately as authentic, historical, and direct, and the suggested proof is not accessible.

For instance, no recommenders are present when a new CSP joins the system. The main component of this model is a service registry module used for registering CSPs on the cloud. This model is based on feedback and opinions provided by other known cloud users. This model is based on subjective trust assessment.

Let cloud user be ‘x’ and ‘y’ be a trusted known so cloud user ‘x’ recommends CU ‘y’ to 'z' CSP. (define in eq. 2)

$Tr(y,z)/Tr(x,z)) =\{ 1, \text{ if } Tr(x,z) =1, \text{ otherwise } 0 \}.$ (2)

3.2.5. Reputation-Based Trust Model

It is also known as the "feedback model." This model is based on feedback provided by historical cloud users or service providers, depending on the perspective from which the system is designed. Based on the providers' perception, the provided feedback is either positive or negative.

The perception of the feedback provider can be situation-specific or person-specific. The vital difference between reputation and recommendation is in the scenario of the reputation model where the trusted entity (CSP or CU) doesn't know the source of the feedback provider as there is no confidence in a relationship between entities.

Let ‘x’ be a cloud user with Tx trust threshold value. ‘y’ be a CSP with trusted relation with other CU $Tr(y)=\{t1,t2,t3,.....tn\}$ (other CU) and feedback provided by these users are $Tf(y)=\{ f1,f2,f3....fn\}$ (as represent in eq. 3)

$Rep(y) = Tr (x, y) = 1, \text{ if } Rep(y) \geq Tx ,$

$\text{Otherwise } 0$ (3)

3.2.6. Prediction-Based Model

This model is used when ther This model is used when there is no record of the historical interactions between cloud service providers ands based on similar interests and capabilities of CU.

Let ‘x’ be any CU with Tx trust threshold value and $Ix=\{i1,i2,i3.....in\}$ denotes the ‘x’ CU capabilities.

Let ‘y’ be any CU with Ty trust threshold value and $Iy=\{i1,i2,i3.....sm\}$ denotes the ‘y’ CU capabilities.(define in eq 4)

$= sim(Ix, Iy)$(using Cosine amplitude in fuzzy logic)

$\{Tr (x, y) = 1,$

$\text{if } sim(Iy,Ix) \geq Tx \text{ or } Ty, \text{ otherwise } 0 \}$ (4)

Multiple methods exist for trust value evaluation, such as game theory, fuzzy theory, Bayesian theorem, graph theory, data science, grey set theory, and probability theory. Still, the central objective is the same as the trust model or management system. The trust mechanism aims to increase confidence between consumers and service providers [18]. Trust management systems have proven useful in numerous decision-making services like grid computing, the web, and utility computing. In the past, the focus of most of the researchers was either on the subjective (recommender, feedback-based) or objective (Agreement based) trust evaluation [19]. The comprehensive summation of both trusts can provide better results because they can complement each other [20].

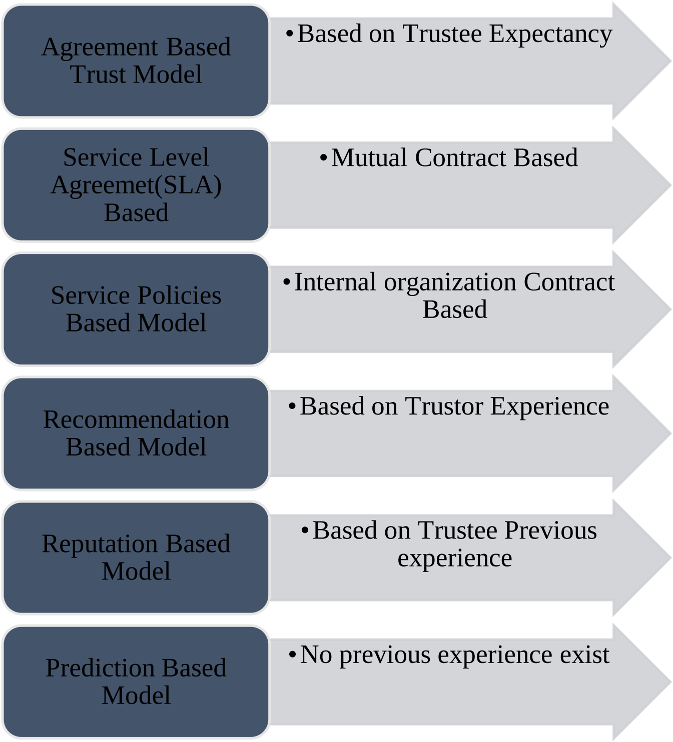
Agreement Based Trust Model
•Based on Trustee Expectancy
Service Level Agreemet(SLA) Based
•Mutual Contract Based
Service Policies Based Model
•Internal organization Contract Based
Recommendation Based Model
•Based on Trustor Experience
Reputation Based Model
•Based on Trustee Previous experience
Prediction Based Model
•No previous experience exist

Figure 3 Trust Management

3.3. Challenges of Trust Management System

3.3.1. Transferring Trust between Contexts

The consumer's faith in the expert associations in the cloud environment relies on the scenario, degree of involvement, and client's perspective. This makes it difficult for TMS to conduct an analysis of recurring consumers, who depend on context and experience.

3.3.2. Trust Evaluation

Multiple components exist for assessing the credibility of expert communities' social networks. Despite this, TMS also has a difficult time selecting the optimal model.

3.3.3. Attack Resistance

When the consumer develops confidence in the TMS or cloud organizations. Multiple malicious agents exist in the cloud environment, each of which provides a variety of attacks based on their requirements. Some cloud environment threats include Sybil, whitewashing, playbook, and extension.

3.3.4. Multi-Faceted Trust Computation

There are many QoS restrictions for assessing the consistency of expert relationships. However, certain restrictions are evaluated emotionally, while others are evaluated quantitatively. Similarly, the addition of equitable and dynamic limitations is an uncomfortable process.

3.3.5. Customization and Aggregation

In general, there are two techniques for managing and storing targeted and appropriate trust. Each framework has its own favorable and unfavorable results, just as the unified system depends on the approved principles. On the contrary, the distributed technique relies on course-corrected rating confidence. So, it's hard for the model of trust to figure out what kind of equipment is used to measure the trust condition. In addition, the amount of customization at which the trust model may be maintained is a crucial challenge.

4. RELATED WORK

The following table depicts the various trust management techniques present in multiple papers. The works [21-25] describe the assessment feedback approach, highlighting its flaws and weaknesses. The publications [26] employ the comprehensive approach methodology. The approach of recommendation and reputation is used in the article [27]. The article [28] implements the integrated approach for estimating trust value. The paper [29] uses the Combining Weights and Gray Correlation Analysis technique. The paper [30] used the Recommendation and SLA techniques. The paper [31] uses the TOPSIS technique. The article [32] uses the ELECTRE (multi-criteria decision-making approach method and the article [33] uses the MOSS technique. The article [34] developed the trust model using graph with behaviour theory. The paper [35] uses Improved CoCoSo Method. The paper [36] employs the TRUSS method. The article [37] employs Pythagorean Fuzzy TOPSIS. The paper [38] uses the Improved TOPSIS technique. The proposed work in article [39] estimate the trust value using service policy and service level agreement. The paper [40] uses the Behaviour Graph technique. Table 1 gives a summary of various trust models present in the previous research articles.

Table 1 Description of Various Trust Models in the Cloud Environment

REF.	Techniques/ Approaches	Shortcomings	Description
[21]	Feedback	Another element like the protection of input suppliers is overlooked.	Work on the dependability of criticism. Dependability of criticism supplier checks by ID number.
[22]	Feedback	Not consider time and defer factor at the hour of affirmation of dependability of criticism.	Work on the dependability of criticism. Dependability of criticism supplier checks by ID number.
[23]	Feedback Based	Not utilizing the idea of discipline and prize.	A map decrease-based system has been characterized for handling buyer input. A FIS (fluffy derivation framework) is utilized for handling keys for assessing trust esteem.
[24]	Feedback	Doesn't involve the idea of differentiating the malicious feedback.	In this paper, we examined the trust assessment best-in-class components that are utilized in the cloud climate up to this point. Likewise, we broke down and looked at them regarding uprightness, security, unwavering quality, trustworthiness, security, dynamicity, secrecy, versatility, and giving an idea for some future exploration.
[25]	Feedback based	Not define a mechanism for how	Here credentials and reputation are used for trust

		to control unfair ratings.	quantification. For interaction with the service provider, select 'n' neighbor node randomly that communicates with the respective service provider and collects the most recent credentials and reputation value from the neighbor nodes. If no historical details, credentials, and reputation =0.
[26]	Comprehensive approach	The exactness of the outcome ought to be improved by thinking about more QoS.	The administration fulfillment-based trust assessment (SSBTE) model fostered that thinking about Direct, companion, and notoriety for trust assessment. Administration fulfillment unpredictability capability likewise presented as a discipline or prize to refresh assessed trust esteem powerfully propose another technique for trust assessment that in light of savaged and assessment pioneer idea. For recognizable proof, three topological measurements are thought of, input degree, yield degree, and notoriety measure.
[27]	Recommendation+ Reputation	Consolidating more QoS is expected for improved outcomes. Likewise created model experience the ill effects of the classification issue.	Propose another technique for trust assessment that in light of savaged and assessment pioneer idea. For recognizable proof, three topological measurements are thought of, input degree, yield degree, and notoriety measures.
[28]	integrated MCDM methods	Should involve the more precise method	This paper means to plan another cloud administration choice model under the fluffy climate by using the logical progressive system process (AHP) and fluffy procedure for request inclination by likeness to the ideal arrangement (TOPSIS).
[29]	Combining Weights and Gray Correlation Analysis	The CSTEM could be additionally improved by considering more trust dynamic update variables of the cloud administrations assessment	In this paper, a model given consolidating loads and dark relationship examination is proposed. Direct trust, proposal, right off the bat, trust, and notoriety together structure a complete trust, bringing about a more precise in general trust
[30]	Recommendation and SLA.	More QoS factors should be considered.	Consumers choose the source and root of information with different characteristics like security, performance, and Agreement. Compute value in the form of proposition and the operator (AND, OR) that can be used to make the various combination of proposition logic terms (PLA’s).
[31]	TOPSIS(MCDM)	Not considered a time and concede factor at the hour of the insistence of reliability of analysis	In this paper, the factual list arrangement of MTs is created to evaluate the trust worth of MTs in the cloud climate. An assessment technique in view of TOPSIS is proposed to get continuous trust measurement of MTs.
[32]	ELECTRE(MCDM)	Doesn’t able to solve time perceptiveness problem in evaluation	This paper proposes a period-mindful way to deal with foresee the dependability positioning of cloud administrations, with the trade-offs between execution cost and possible dangers in various periods.
[33]	MOSS(MCDM)	The process becomes a bit lengthy and tiresome for the user	To resolve these issues, we propose a clever incorporated approach called Methodology for Optimal Service Selection (MOSS). Greenery comprises five phases including the prequel, evaluation, positioning,

			reconciliation, and union/determination.
[34]	Behaviors Graph(feedback)	Should have more reliability factor	The motivation behind this paper is to propose another technique to assess the trust metric among cloud suppliers. The principal objective is to expand the accuracy and precision of the trust assessment technique in cloud conditions.
[35]	Improved CoCoSo Method	Should involve more MCDM factors	In this review, a superior joined compromise arrangement (CoCoSo) strategy is proposed to recognize the positioning of cloud specialist co-ops.
[36]	TRUSS	Not able to differentiate between genuine and malicious user	This paper proposes a dependable choice system for cloud administration determination, TRUSS, which is an incorporated trust assessment technique through joining objective and emotional trust evaluation.
[37]	Pythagorean Fuzzy TOPSIS	Doesn't involve a multi-user ranking facility	The assessments concerning the cloud options are communicated as Pythagorean fuzzy sets. Pythagorean fluffy sets are an expansion of intuitionistic fluffy sets, in which the amount of enrolment and non-participation degrees might be bigger than one though their square aggregate is all things considered equivalent to 1.
[38]	Improved TOPSIS	Should involve multi-user ranking consideration	This paper presents the plan of a trust assessment structure that utilizes the consistency observing system to decide the reliability of specialist organizations.
[39]	SLA	Doesn't include large-scale feedbacks	This paper proposes a unique cloud administration trust assessment model for understanding (SLA) and protection mindfulness.
[40]	Graph-Based	Should involve more QoS factor	This model estimated the trust level based on QoS and used the concept of node and edge for estimating trust value.

5. COMPARATIVE ANALYSIS OF TRUST COMPUTATION TECHNIQUES

A rating-based process is a simple approach for computing the trust value used in web services. However, this method has not been so far due to simplicity and easy computation techniques. There are multiple approaches to the computation of trust value, like graph theory, belief theory, machine learning, Ant optimization techniques, rating techniques, and fuzzy theory. This section gives a detailed summary of multiple computation techniques used for trust computation.

5.1. Rating-Based Techniques

It is a part of the method for computing trust based on feedback. Client users offer their replies using the Likert scale or a star rating to compute the purpose of computing trust. However, this basic approach to trust computation has the issue of producing ineffective results. Table 2 presents a comparative analysis of the rating-based trust models.

5.2. Fuzzy theory

Fuzzy theory is one of the most appropriate techniques for trust computation in uncertain environments. It deals with an approximate value in place of the exact value. The stages for reasoning using fuzzy rules are as follows:

- Initially, design fuzzy sets and evaluation criteria.
- Then, initialize variables for the fuzzy engine.
- Apply fuzzy rules to retrieve the output and conclude.
- Now, review the outcomes and adjust the fuzzy rules as needed.

5.3. Belief Theory

Bayesian approaches use prior knowledge to estimate service providers' average trust value. It is applicable when the dataset size is minimal. Probability theory is the basis for this model. A provider's trustworthiness is regularly updated and contingent on their prior actions. Table 4 presents a comparative analysis of the belief theory-based trust models.

5.4. Subjective Logic Theory

It is a strategy for managing uncertainty. It functions based on opinions and worldviews. Subjective logic is a kind of belief theory and regression analysis. It incorporates elements of the 'Dempster-Shafer belief theory. Subjective logic can be utilized to address partial ignorance and lack of knowledge. Table 5 presents a comparative analysis of subjective logic-based trust techniques.

5.5. Parameters used by different Trust Models

These parameters, also known as "trust factors," are considered during service evaluation or selection. Multiple quality-of-service parameters are available at the time-of-service selection. Moreover, there is another big problem for cloud users in deciding which parameters they select for assessing cloud services. The number and type of parameters depend on the requirements of the organization. These parameters are quantitative as well as qualitative in nature. There is no globally recognized method or parameter to fathom the quality of a cloud service, the service measurement index (SMI) can be considered an initial step in this procedure. As in the present situation, many service distributors with various services and facilities are present creating conditions of ambiguity and confusion for the consumer [54], SMI proves to be important in such cases for the assessment of the service**.** Table 6 briefly compares the parameters used by different research articles.

Table 2 Rating-Based Trust Model

Ref. No. /Year of Publishing	Environment/Approach	Context	Techniques
[41]/2022	IoT social media/ Hybrid (Prediction+ aggregation)	controlling Malicious ratings	Machine learning
[42]/2018	Trusted Parties/Weighted user rating	Inconsistent recommendation	Sampling Approach
[43]/2022	IoT+ Fog Computing	Accuracy	QoS based
[44]/2019	Online social media/clustering approach	Item suggestion calculation in the books and SRNs films	Collaborative Filtering

Table 3 Presents a Comparative Analysis of the Fuzzy Theory-Based Trust Models

Ref/Year	Tool	Input set	Techniques
[45]/2017	Matlab/Simulation	QoS set	Induced ordered weight averaging operator
[46]/2016	simulation	Finance	Abstraction level for different categories of the requestor
[47]/2016	Matlab	feedback	Fuzzy processing and neural network

Table 4 Belief Theory-Based Trust Model

Ref/Year	Techniques	Context	Characteristics
[48]/2022	semi-ring theory	malicious behaviors and heterogeneous characteristics	Handle on-off attacks, Sybil attacks, whitewashing attacks, malicious access
[49]/2017	Game theory with probability	Identify fake feedback	The feedback evaluation model correctly rectifies malicious user
[50]/2015	Bayesian equation with sliding window	Defeating attacks	Consider both direct and indirect trust

Table 5 Subjective Logic-Based Trust Model

Ref/Year	Context	Tool	Characteristic
[51]/2019	Security & privacy in fog computing	iFogSim simulator	Handle data breaches, data loss, and denial of service (DoS) and establish a secure environment
[52]/2018	Selection of trustworthy service	Simulation	Use SLA, belief theory and reputation
[53]/2018	Enhance system security and network interconnection quality	Cloud sim	Use AHP and Fuzzy logic

Table 6: SMI QoS Parameters Used by Different Trust Models

Ref	Security	Availability	Privacy	Cost	Maintenance	Accuracy
[30]	✓		✓			
[31]	✓			✓		
[32]	✓					
[33]		✓			✓	
[34]		✓			✓	
[35]		✓			✓	
[36]	✓		✓		✓	
[37]			✓		✓	
[38]	✓		✓		✓	
[39]				✓	✓	

[40]					✓	
[41]					✓	
[42]	✓					✓
[43]				✓		✓
[44]						✓
[45]						✓
[46]	✓				✓	✓

6. DISCUSSION

After studying over fifty publications from March 2010 to September 2022 based on various trust management methodologies, it was determined that privacy and security constitute a barrier to the expansion of cloud computing. Other concerns include reputation, interoperability, SLA, virtualization, trust administration, and service quality (QoS). The issues associated with cloud computing and trust management are depicted in Figure 4. It is evident from the graph below that security is the most problematic aspect of trust management. Figure 5 illustrates the number of Scopus-indexed and published papers between March 2010 and September 2022, depending on several trust methodologies. The research related to trust management may be divided into four subcategories.

(a) How to access cloud trust.

(b) How to handle malicious trust ratings.

(c) How to provide a different kind of service according to the predicted trust value.

(d) How to monitor trust values as they change over time and circumstance.

The answer to the above question is using the SMI QoS for estimating the trust level through hybrid MCDM techniques with an event and time-driven approach. One definition of a comprehensive model incorporates one that incorporates both objective and subjective measures of trust. It is a technique that usually consists of all the factors required for an accurate ranking. It is analyzed that demand for a comprehensive trust model has increased its popularity among users since 2019. This method is useful for a more accurate and precise selection procedure to choose a cloud service provider. A complete trust model is necessary to overcome the current obstacles associated with cloud computing which is clearly shown in Figure 5.

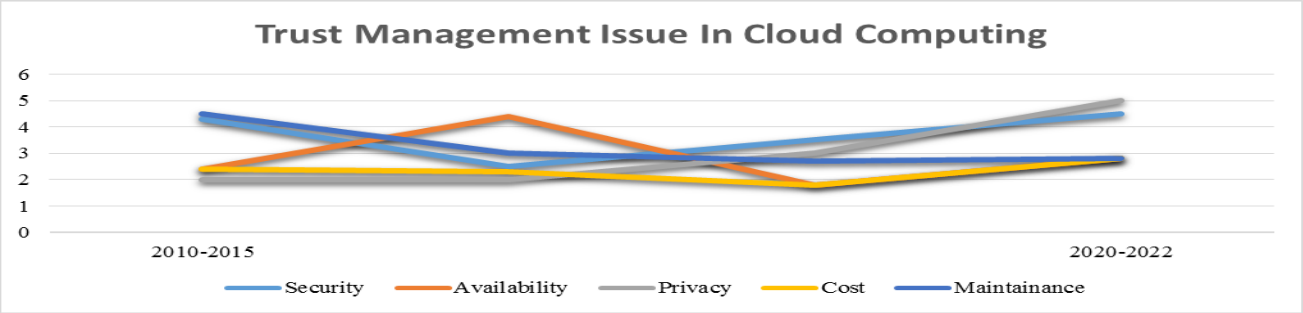

Figure 4 Analysis of Trust Management Issues (Period: 2010-2022)

REVIEW ARTICLE

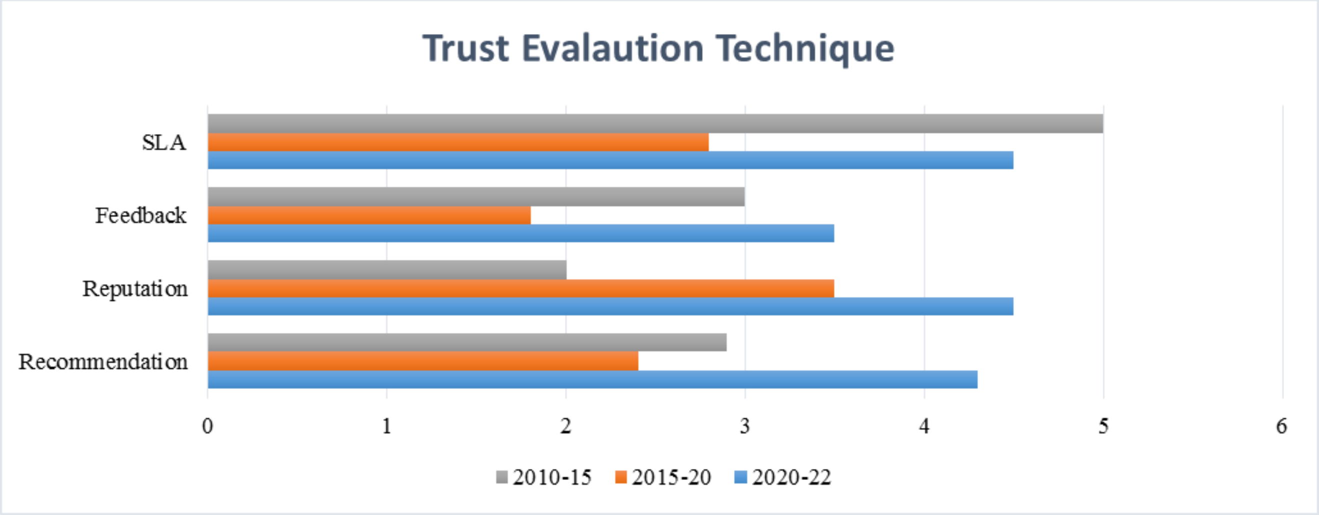

Figure 5 Analysis of Trust Management Evaluation Techniques (Period: 2010-2022)

7. CONCLUSION

Cloud computing is an effective technology, but it requires many concerns to be addressed. Security in the cloud is one such concern. As the cloud environment consists of many different sorts of users, distributors, and brokers, trust management is a crucial characteristic to maintain cloud security. However, poor trust management is inhibiting its expansion. Generally, users of cloud services still have to make decisions based on what cloud service providers say they will have to do. Instead of relying on how service providers actually act, cloud services should use a standard trust management system so that users can fetch and predict right information about the trust. This study analyzed a variety of existing trust management concerns and evaluation methodologies. The study provided an overview of many viewpoints on existing trust management approaches. It offers a comprehensive comparison of the current trust management solutions. In addition, the study discussed trust management challenges in cloud computing that have been the subject of several research publications since decades. It also talks about problems like not being able to trust both the service provider and the customers when exchanging data on the cloud. It opens up interesting questions for further research in this emerging domain.

REFERENCES

[1] P. Varalakshmi, T. Judgi, and D. Balaji, “Trust Management Model Based on Malicious Filtered Feedback in Cloud,” Commun. Comput. Inf. Sci., vol. 804, pp. 178–187, 2018, doi: 10.1007/978-981-10-8603-8_15.

[2] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, “Trust management of services in cloud environments,” ACM Comput. Surv., vol. 46, no. 1, pp. 1–30, 2013, doi: 10.1145/2522968.2522980.

[3] S. Soltani, M. Asadi, D. Gašević, M. Hatala, and E. Bagheri, “Automated planning for feature model configuration based on functional and non-functional requirements,” in Proceedings of the 16th International Software Product Line Conference-Volume 1, pp. 56–65,2012, doi: 10.1145/2362536.2362548

[4] X. Yang, S. Wang, B. Yang, C. Ma, and L. Kang, “A service satisfaction-based trust evaluation model for cloud manufacturing,” Int. J. Comput. Integr. Manuf., vol. 32, no. 6, pp. 533–545, 2019, doi: 10.1080/0951192X.2019.1575982.

[5] E. Kristiani, C. T. Yang, Y. T. Wang, and C. Y. Huang, “Implementation of an edge computing architecture using openstack and kubernetes,” Lect. Notes Electr. Eng., vol. 514, pp. 675–685, 2019, doi: 10.1007/978-981-13-1056-0_66.

[6] G.Aghaee, G. Mehran, and M. Ramin, “A new multi ‐ level trust management framework (MLTM) for solving the invalidity and sparse problems of user feedback ratings in cloud environments,” J. Supercomput., no. 0123456789, 2020, doi: 10.1007/s11227-020-03348-1.

[7] P. Varalakshmi, T. Judgi, and D. Balaji, “Trust Management Model Based on Malicious Filtered Feedback in Cloud,” Commun. Comput. Inf. Sci., vol. 804, pp. 178–187, 2018, doi: 10.1007/978-981-10-8603-8_15.

[8] M. R. Thanka, P. Uma Maheswari, and E. B. Edwin, “An improved efficient: Artificial Bee Colony algorithm for security and QoS aware scheduling in cloud computing environment,” Cluster Comput., vol. 22, no. 5, pp. 10905–10913, 2019.

[9] H. Kurdi, A. Alfaries, A. A. S. Alkharji, M. Addegaither, L. Altoaimy, and S. Hassan, “A lightweight trust management algorithm based on subjective logic for interconnected cloud computing environments,” J. Supercomput., 2018, doi: 10.1007/s11227-018-2669-y.

[10] S. S. Manvi and G. Krishna Shyam, “Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey,” J. Netw. Comput. Appl., vol. 41, no. 1, pp. 424–440, 2014, doi: 10.1016/j.jnca.2013.10.004.

[11] E. Kristiani, C. T. Yang, Y. T. Wang, and C. Y. Huang, “Implementation of an edge computing architecture using openstack and kubernetes,” Lect. Notes Electr. Eng., vol. 514, pp. 675–685, 2019, doi: 10.1007/978-981-13-1056-0_66.

[12] https://en.wikipedia.org/wiki/Cloud_computing

[13] S. S. Manvi and G. Krishna Shyam, “Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey,” J. Netw. Comput. Appl., vol. 41, no. 1, pp. 424–440, 2014, doi: 10.1016/j.jnca.2013.10.004.

[14] Machhi, Sandip, and G. B. Jethava. "Feedback based trust management for cloud environment." In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, pp. 1-5. 2016.

[15] Siani Pearson. Privacy, security and trust in cloud computing. In Privacy and security for cloud computing, pages 3–42. Springer, 2013.

[16] Talal H Noor, Quan Z Sheng, SheraliZeadally, and Jian Yu. Trust management of services in cloud environments: Obstacles and solutions. ACM Computing Surveys (CSUR), 46(1):1–30, 2013.

[17] R Thirukkumaran et al. Survey: Security and trust management in internet of things. In 2018 IEEE global conference on wireless computing and networking (GCWCN), pages 131–134. IEEE, 2018.

[18] J. Huang and M. S. Fox, "An ontology of trust - Formal semantics and transitivity," ACM Int. Conf. Proceeding Ser., no. January, pp. 259–270, 2006, doi: 10.1145/1151454.1151499.

[19] V. K. Damera, A. Nagesh, and M. Nagaratna, "Trust evaluation models for cloud computing," Int. J. Sci. Technol. Res., vol. 9, no. 2, pp. 1964–1971, 2020.

[20] M. Chiregi and N. J. Navimipour, "A new method for trust and reputation evaluation in the cloud environments using the recommendations of opinion leader's entities and removing the effect of troll entities," Comput. Human Behav., vol. 60, pp. 280–292, Jul. 2016, doi: 10.1016/j.chb.2016.02.029.

[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, 2018, doi: 10.1007/s40815-017-0347-5

[22] Q. Duan, "Cloud service performance evaluation: status, challenges, and opportunities – a survey from the system modeling perspective," Digit. Commun. Networks, vol. 3, no. 2, pp. 101–111, 2017, doi: 10.1016/j.dcan.2016.12.002.

[23] M. Tang, X. Dai, J. Liu, and J. Chen, "Towards a trust evaluation middleware for cloud service selection," Futur. Gener. Comput. Syst., vol. 74, pp. 302–312, 2017, doi: 10.1016/j.future.2016.01.009.

[24] M. B. Smithamol and S. Rajeswari, "TMM: Trust Management Middleware for Cloud Service Selection by Prioritization," J. Netw. Syst. Manag., vol. 27, no. 1, pp. 66–92, 2019, doi: 10.1007/s10922-018-9457-0.

[25] W. Fan and H. Perros, "A Reliability-based Trust Management Mechanism for Cloud Services," 2013, doi: 10.1109/TrustCom.2013.194.

[26] S. K. Garg, S. Versteeg, and R. Buyya, "SMICloud : A Framework for Comparing and Ranking Cloud Services," no. Vm, 2011, doi: 10.1109/UCC.2011.36.

[27] N. Yadav and M. S. Goraya, "Two-way Ranking Based Service Mapping in Cloud Environment," Futur. Gener. Comput. Syst., 2017, doi: 10.1016/j.future.2017.11.027.

[28] Y. Wang, J. Wen, X. Wang, B. Tao, and W. Zhou, "A cloud service trust evaluation model based on combining weights and gray correlation analysis," Secur. Commun. Networks, vol. 2019, 2019, doi: 10.1155/2019/2437062.

[29] G. Obulaporam, N. Somu, G. R. ManiIyer Ramani, A. K. Boopathy, and S. S. Vathula Sankaran, "GCRITICPA: A CRITIC and grey relational analysis based service ranking approach for cloud service selection," in International Conference on Intelligent Information Technologies, 2018, pp. 3–16.

[30] N. N. a. C. V. V. a. B. M. A. a. o. Kumbhar, "The Comprehensive Approach for Data Security in Cloud," International Journal of Computer Applications},, vol. 39, 2012.

[31] R. R. Kumar and C. Kumar, "A multi criteria decision making method for cloud service selection and ranking," Int. J. Ambient Comput. Intell., vol. 9, no. 3, pp. 1–14, 2018.

[32] M. Jouini and L. B. A. Rabai, "A security framework for secure cloud computing environments," in Cloud security: Concepts, methodologies, tools, and applications, IGI Global, 2019, pp. 249–263., DOI: 10.4018/978-1-5225-8176-5.ch011.

[33] F. Nadeem, "A Unified Framework for User-Preferred Multi-Level Ranking of Cloud Computing Services Based on Usability and Quality of Service Evaluation," IEEE Access, vol. 8, pp. 180054–180066, 2020.

[34] E. Kristiani, C.-T. Yang, Y. T. Wang, and C.-Y. Huang, "Implementation of an edge computing architecture using openstack and kubernetes," in International Conference on Information Science and Applications, 2018, pp. 675–685.

[35] S. R. a. M. M. Sheikh Mahbub Habib, "Towards a trust management systemfor cloud computing," p. 933–939, 2011.

[36] S. Kaushik and C. Gandhi, "Multi-level Trust Agreement in Cloud Environment," 2019 12th Int. Conf. Contemp. Comput. IC3 2019, pp. 1–5, 2019, doi:10.1109/IC3.2019.8844933.

[37] A C. Qu, R. Buyya, A cloud trust evaluation system using hierarchical fuzzy inference system for service selection, in: Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA, no. May, 2014, pp. 850–857. doi:10.1109/AINA.2014.104.

[38] A. K. Jaithunbi, S. Sabena, and L. SaiRamesh, "Trustevaluation of public cloud service providers using genetic algorithm with intelligent rules," Wirel. Pers. Commun., vol. 121, no. 4, pp. 3281–3295, 2021.

[39] M. B. Chhetri, Q. B. Vo, R. Kowalczyk, Policy-based automation of SLA establishment for cloud computing services, in: Proc. - 12th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput. CCGrid 2012, IEEE, 2012, pp. 164–171. doi:10.1109/CCGrid.2012.116.

[40] W. Jiang, G. Wang, M. Z. A. Bhuiyan, and J. Wu, "Understanding graph-based trust evaluation in online social networks: Methodologies and challenges," Acm Comput. Surv., vol. 49, no. 1, pp. 1–35, 2016.

[41] Ali-Eldin, A. M. T. (2022). A hybrid trust computing approach for IoT using social similarity and machine learning. PLoS ONE, 17(7 July) doi:10.1371/journal.pone.0265658.

[42] Ali-Eldin, A. M. T. (2018). Trust prediction in online social rating networks. Ain Shams Engineering Journal, 9(4), 3103-3112. doi:10.1016/j.asej.2018.03.005

[43] Hallappanavar, V. L., & Birje, M. N. (2022). Prediction of quality of service of fog nodes for service recommendation in fog computing based on the trustworthiness of users. Journal of Reliable Intelligent Environments, 8(2), 193-210. doi:10.1007/s40860-021-00149-y.

[44] Sivabalaselvamani, D., Vidhyasree, S., Pavithra, P., Soundarya, G., &Preethika, M. (2019). Books and movies recommendation and rating prediction based on collaborative filtering networks. International Journal of Advanced Science and Technology, 29(5), 705-714.

[45] Selvaraj, A., & Sundararajan, S. (2017). Evidence-based trust evaluation system for cloud services using fuzzy logic. International Journal of Fuzzy Systems, 19(2), 329-337. doi:10.1007/s40815-016-0146-4.

[46] Pandey, S., & Daniel, A. K. (2016). Fuzzy logic-based cloud service trustworthiness model. Paper presented at the Proceedings of 2nd IEEE International Conference on Engineering and Technology, ICE TECH 2016, 73-78. doi:10.1109/ICETECH.2016.7569215.

[47] Wu, Z., & Zhou, Y. (2016). Customized cloud service trustworthiness evaluation and comparison using fuzzy neural networks. Paper presented at the Proceedings - International Computer Software and Applications Conference, 1 433-442. doi:10.1109/COMPSAC.2016.86.

[48] Wang, J., Wang, M., Zhang, Z., & Zhu, H. (2022). Towards A trust evaluation framework against malicious behaviors of industrial IoT. IEEE Internet of Things Journal, 1-1. doi:10.1109/JIOT.2022.3179428.

[49] Siadat, S., Rahmani, A. M., &Navid, H. (2017). Identifying fake feedback in cloud trust management systems using feedback evaluation component and bayesian game model. Journal of Supercomputing, 73(6), 2682-2704. doi:10.1007/s11227-016-1950-1.

[50] D. a. P. V. a. P. A. a. S. A. a. S. S. Grimaldi, "A Feedback-Control Approach for Resource Management in Public Clouds," 2015.

[51] H. Kurdi et al., "A lightweight trust management algorithm based on subjective logic for interconnected cloud computing environments," J. Supercomput., vol. 75, no. 7, pp. 3534–3554, 2019,doi: 10.1007/s11227-018-2669-y.

[52] A. M. Mohammed, E. I. Morsy, and F. A. Omara,"Trust model for cloud service consumers," in 2018 International Conference on Innovative Trends in Computer Engineering (ITCE), 2018, pp. 122–129, doi: 10.1109/ITCE.2018.8316610.

[53] H. Kurdi, A. Alfaries, A. A. S. Alkharji, M. Addegaither, L. Altoaimy,

and S. Hassan, “A lightweight trust management algorithm based on subjective logic for interconnected cloud computing environments,” J. Supercomput., 2018, DOI: 10.1007/s11227-018-2669-y.

[54] P. Varalakshmi, T. Judgi, and D. Balaji, “Trust Management Model Based on Malicious Filtered Feedback in Cloud,” Commun. Comput. Inf. Sci., vol. 804, pp. 178–187, 2018, doi: 10.1007/978-981-10-8603-8_15.

Authors

Ms. Pooja Goyal: MCA, M.Tech,UGC(NET) COMP.SCI, Pursuing Ph. D from MD University Rohtak.

Designation: Research Scholar

Department: DCSA,MDU

Dr. Sukhvinder Singh Deora: He is currently working as an Assistant Professor in the Department of Computer Sciences, at Maharshi Dayanand University, Rohtak, India. He received the MSc (Mathematics) & M.C.A. from Kurukshetra University in 2000 and 2002 respectively. He did his M.Phil. in Computer Science and completed his Ph.D. in 2015. He is a Reviewer of many SCIS-listed prestigious International and Indian Journals. He is also a member of the Editorial Board of some Journals. To his credit are many prominent papers in the area of data security, big data analytics, and issues related to Cloud Computing, general privacy and Computer Science education. He has also been editor of a few Proceedings at the National Level Seminars/Conferences. With an exposure of 19 years in education and 1.5 years in IT industry, his thrust areas also include Testing, Java technologies, and Database design issues. His current contributions are in areas including Big Data Analytics, Network Security, Theoretical Computer Sciences, and applications of Fuzzy Logic. He is an active member of professional societies like ACM, the Computer Society of India (CSI,) and the Indian Society of Information Theory and Applications (ISITA).

How to cite this article:

Pooja Goyal, Sukhvinder Singh Deora, “Trust Management Techniques and their Challenges in Cloud Computing: A Review”, International Journal of Computer Networks and Applications (IJCNA), 9(6), PP: 761-774, 2022, DOI: 10.22247/ijcna/2022/217708.