Examining the Empirical Relationship Between Quality of Service (QoS) and Trust Mechanisms of Cloud Services

Pooja Goyal* and Sukhvinder Singh Deora

Department of Computer Science and Application, MD University, Rohtak, Haryana, India
E-mail: poojagoyal895@gmail.com; sukhvinder.singh.deora@gmail.com
**Corresponding Author*

Received 18 March 2023; Accepted 25 September 2024

Abstract

Service selection has emerged as a prominent challenge due to the flourishing demand for computing services and the dynamic nature of its resources. The increasing demand for cloud services makes it challenging to choose a provider offering equal services and facilities at costs that match those of competing providers. Apart from educating customers in the process of choosing cloud services, trust mechanisms include user reviews, reputation systems, and certifications assist to boost consumers' confidence in cloud services. The service measurement index (SMI) offers a disciplined framework combining both functional and non-functional quality of service indicators concurrently, therefore easing decision-making. The main emphasis of the research is on the fundamental elements influencing the choice of cloud services in the present environment, the identification of extra characteristics of cloud services transcending SMI, and the identification of the most suitable approach for some services. By means of the measurement of customer enjoyment and experience, QoS traits provide some insight on the impact of trust mechanisms on service acceptance. Comparisons of SMI and QoS measurements before and after trust mechanism deployment provide

Journal of Web Engineering, Vol. 23_7, 913–972.
doi: 10.13052/jwe1540-9589.2372

insightful analysis. Empirical research guides these comparisons. This study aims to clarify the interactions among QoS, trust mechanisms, and cloud service adoption as well as highlight the implications these elements have for customers and service providers. Furthermore, presented in this paper is an algorithm using a comprehensive method to trust estimation in order to ascertain the degree of confidence worthiness of certain people.

Keywords: Cloud broker, MCDM, trust estimation, QoS, risk assessment, multi-tenancy, SMI.

1 Introduction

Cloud service selection is super-set of web service selections. Nowadays, information is often stored in the cloud, which refers to a collection of internet-based services provided to users. It enables data and information to be stored and accessed from a remote server instead of private data centers or local hard drives. It also creates a new door for the computing paradigm, enabling virtualized distributed resources as a commodity via an online portal with demand-based pricing [1]. Before the introduction of cloud computing, organizations and individuals had to purchase servers to meet their specific needs. It led to spending a lot of money to decrease the probability of downtime and outages and to include a more significant number of simultaneous visitors [2]. Despite having properties of adaptability and versatility, many consumers still face security issues and challenges in providing appropriate privacy [3], even though service providers adopt the highest security requirement and industry certifications. Choosing the optimal service provider requires a framework to compare various non-functional requirements known as QoS. Based on these non-measurable and varied qualities of service characteristics which include qualitative and quantitative aspects the best cloud service might be selected [4]. Thanks to CSMIC's development, there already is a cloud service rating tool, the service measurement index (SMI) [5, 6]. A successful QoS-based assessment of online cloud services in e-marketplaces depends on a method of service selection that combines quantitative and qualitative QoS aspects with different similarity metrics. Using the SMI and QoS elements will help one better grasp how trust mechanisms affect the acceptance of cloud and online services as they are necessary to provide empirical data. One can systematically measure the QoS using the SMI [7]. Factors of QoS are observable markers of a service's degree of fit for user requirements. Usually it covers security, scalability,

reliability, and availability, among other aspects. Using the architecture of trust systems, the SMI can help to assess the effectiveness of security policies implemented in online and cloud services. Among other things, it may assess the reliability of data protection systems, service availability during security events, and scalability of security measures in reaction to service expansion [8]. Establishing a baseline SMI and then comparing it with changes in trust mechanisms would allow one to objectively evaluate how general quality and performance of online and cloud services are affected. Integrating SMI and QoS measurements will provide a comprehensive empirical study of how trust systems influence the acceptance of cloud and online services. Researchers might use these indicators to evaluate changes in service quality, user experience, and general adoption rates [9, 10] thus better understanding how trust mechanisms help to create confidence and trust among users.

1.1 Problem Statement and Motivation Factor

Reliable evaluation tools are becoming increasingly crucial because the environment of cloud computing is evolving so fast. Modern trust rating systems examine many elements, including performance, reputation, and service availability, using numerical values most of the time. Trust is founded on traits like honesty, reliability, and trustworthiness so these strategies are hard to grasp. Although there is space for improvement, the techniques used to measure confidence in cloud services currently steer customers in the direction of reliable replacement. A fixation with numerical metrics, which ignores the complicated and subjective character of trust [14], is largely responsible for this limitation. Many strategies overlook the natural traits influencing genuine user evaluations. Without a comprehensive trust assessment tool, service level agreement (SLA) fulfilment, user maliciousness detection, and security risk mitigation in the complex and always changing cloud environment are all made more difficult. Establishing trust is critical for the integrity of relationships between consumers and suppliers, as well as the immediate and enduring advantages of cloud services. Current methods of assessing trust are inadequate for fostering connection. Trust requires a more sophisticated and thorough understanding than just quantitative evaluations. This study aims to fill a gap by suggesting a better method that takes into account non-functional factors such as user satisfaction, security concerns, and quality of service (QoS) [16]. It does this by looking at how trust is currently evaluated. Favorable developments for consumers and enterprises: these results indicate approaches to enhance the precision, reliability, and thoroughness of trust

assessment systems [17]. The analysis is based on an examination of over 140 academic articles about cloud trust management and online service selection. Despite the availability of various promising evaluation methodologies, they inadequately address critical issues such as security concerns, motivational factors, and the intricate relationships between service providers and their clients.

1.2 Aims and Objectives

This paper explores the relationship between trust systems, quality of service, and cloud solutions acceptance. It aims to improve consumer trust and satisfaction by integrating quantitative and qualitative elements in a unique methodology for evaluating cloud service providers' dependability. The project seeks to provide consumers and service providers with information so they may make wise choices, therefore strengthening trust and raising standards of quality for services. The objective of this paper is to investigate the influence of trust systems and service quality on cloud service acceptance. The main goal of the research is to find how stricter quality-of-service criteria might boost confidence in cloud services, therefore fostering happier consumers and more general acceptance. Combining several qualitative and quantitative criteria, the study also presents a unique way to assess the reliability of cloud service providers. The ultimate aim is to enable better decisions for customers of service providers as well as for them.

***Main objective*:** The main objective is to investigate, using cloud services, the interaction between trust mechanisms and quality of service (QoS). This process will allow us to investigate the relationship between trust and QoS aspects like reliability, security, and validity of the service. These factors influence a user's choice to continue using cloud technology solutions in both quantitative and qualitative sense.

The second purpose created and made accessible a novel method for undertaking an all-encompassing assessment of cloud service dependability. This approach aims to provide a more complex way of trust assessment by considering a broad spectrum of significant elements, like service quality, security, and user feedback. Applying numerous criteria to every cloud service provider, the algorithm is able to produce a more reliable rating.

Thirdly, we would want to conduct an analysis of the several trust assessment models that are now in use. In order to achieve this goal, we will investigate the various trust mechanisms and tactics that are already in use for cloud computing, taking into account both their advantages and

disadvantages. By highlighting where the present approaches fall short, one may demonstrate how the proposed approach is superior in terms of accuracy and breadth.

Our fourth objective is to provide useful information to customers and cloud service providers. The research aims to provide customers with useful guidance so they may help them to make informed decisions about cloud services. With the ultimate intention of building closer relationships between these parties, it also seeks to teach service providers how to improve their services to better fill trust and quality of service needs.

The remainder of this article is structured as follows: Section 2 briefly overviews cloud computing with its operation and trust management and its methodologies. It also discusses the role-play of the SMI and QoS in cloud computing and trust management. Section 3 articulates the associated paperwork. Section 4 presents the comparative analysis of different trust management techniques. It provides the background related to the context of various trust factors and a summary report of QoS parameters used by earlier researchers. In Section 5, the article concludes with a brief reflection and discussion of forthcoming work.

2 Groundwork

Selecting the appropriate cloud service provider might be difficult as it depends on various elements in the always changing cloud computing sector. Among others, performance, dependability, security, and customer assistance define both quantitative and qualitative elements of the QoS factors used in this selection process. The vast numbers of factors that have to be taken into account makes finishing the process difficult even if there are many assessment methods available. This approach especially ignores the intangible elements of trust – that which consists of credibility, honesty, and dependability. One similarity of more traditional methods is the focus on weighing many indicators for service excellence. This means that the dependability evaluation is not particularly comprehensive and may not fairly depict the intricacy of the interactions across cloud services. Given the complex nature of the cloud ecosystem, where services are continuously improved and new vendors join the market, solving the problem becomes even more difficult. The situation is inherently unknown, hence a trust assessment approach that explores more ground than just numerical ratings is required. Users therefore find it difficult to receive honest perspectives and make wise selections. Moreover, present approaches often ignore the motivational elements that might

affect trust. Given the complexity of trust and its flux in the cloud, a more advanced and all-encompassing approach of trust assessment is essential. This is because the present situation of cloud service evaluation requires such an intervention. An overview of cloud computing, including its advantages and disadvantages, as well as information on the trust management system, its procedures, and the limitations it imposes, is provided in this section.

2.1 Cloud Computing

Cloud computing describes process of storing, managing, along with processing data over a network of distant servers that is frequently accessible online. It provides a means for individuals and businesses to access computing resources that are both scalable and flexible without having to invest in costly hardware and infrastructure. In essence, cloud computing enables users to tap into a vast network of computing power, similar to the way that water vapor accumulates to form clouds in the sky. The services offered by the cloud have a widespread network [18]. It supports many applications, including social media sites like Instagram and Facebook, internet-based mailing platforms such as Yahoo and Gmail, and entertainment sites like Netflix and YouTube, which all require nothing except a web browser [19, 20]. It gives new hikes to IT industry by enabling them to store and access available infrastructure along with application services on a subscription basis instead of using a local server or computer hard drive [21]. The primary goal of cloud computing is to supply on-demand resources to the requester through the internet and intelligent communication channels. Compared to conventional computing methods, it provides tremendous advantages regarding dependability, availability, flexibility, and cost [22, 23]. There are three main categories of services: SaaS, PaaS, and IaaS. These services are also known as Internet-based computing stacks, built on top of one another (Figure 1).

2.2 Trust Management

Trust is an integral part of making decisions and is critical to the growth and acceptance of cloud computing [39]. It works as a facilitator for predicting any entity's future behavior, i.e., either requestor or distributor, as per the perspective of the design model [40, 41]. In the cloud computing context, there are three areas of trust evaluation: trust in the CSP, confidence in the service provided by the CSP, along with trust in cloud technology itself. The most difficult of these categories is trust in the cloud computing environment because of the incentive elements employed to encourage users to adopt the

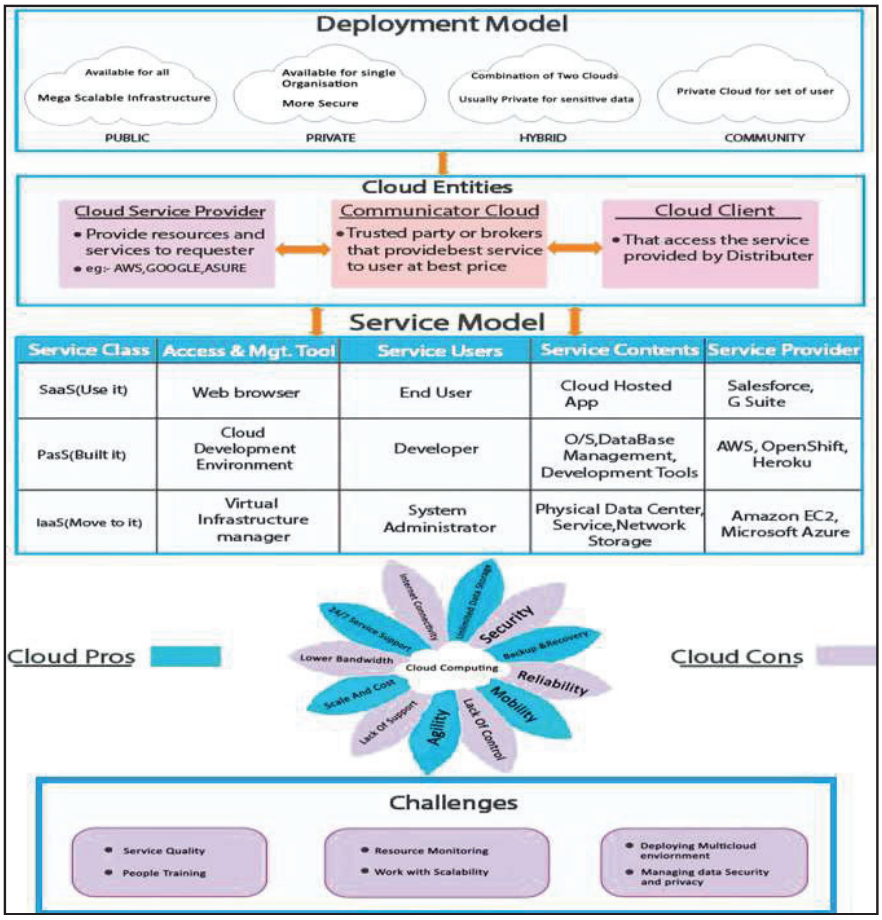

Figure 1 Cloud computing taxonomy [30–38].

service [42, 43]. Now, the question arises, "Why do we require trust in the cloud environment?" The answer is because trust serves as a foundation for security and privacy [44, 45]. The working environment of internet-based computing is non-transparent, dynamic, and complex. Moreover, cloud data storage is scattered across a broad region so that consumers can lose control over the data. For the establishment of healthy trust relations between two partners, various factors have been identified, like the current reputation of the trustee, previous experience or general assumption, and prior knowledge of any known during their past interaction (recommendation) [46]. EENISA recommends developing a trust-based belief system as one of essential factors

for strengthening the security and safety of cloud [47]. According to UC Berkeley, security and trust management systems are considered the top 10 obstacles in the growth and adoption of internet-based computing [48] due to the various hindrances still present in the distributed environment: dependability [49], privacy [50], and security [51, 52].

In cloud computing, trust between requestor and service providers is essential. Various methods are available to help requestors choose trustworthy services, such as SLAs, auditors, measuring, rating, and self-assessment questionnaires [53]. However, most of these methods rely on either requestor feedback or service distributors' technical and functional features. These approaches are often time-consuming along with unmanageable in the cloud environment [54]. We must find a reliable way to select the most suitable service to provide additional support to cloud users. For this, it is essential to have a clear and comprehensive understanding of cloud entities' operations to understand the trust management system employed by them. Figures 2 and 3 visually represent the trust mechanism. These figures illustrate how cloud entities work together to establish along with maintain trust, thereby ensuring the security and reliability of cloud-based services. By studying these figures, one can gain a deeper insight into the intricate workings of the trust management system and appreciate its importance in cloud computing.

2.2.1 Trust mechanism in the cloud

Trust mechanisms are different methods or systems that establish and maintain trust between individuals, organizations, and systems. These mechanisms can be technical, such as authentication and encryption protocols, or social, such as reputation systems and social norms [59–61]. Trust mechanisms are critical in modern society as they enable individuals and organizations to interact and transact with each other securely and reliably. Trust mechanisms address and satisfy the different dimensions of trust (aspects of trust relevant to maintaining trust between entities). For example, authentication and encryption protocols are technical trust mechanisms that address the reliability dimension of trust by ensuring that data is transmitted securely and accurately. Reputation systems and social norms are social trust mechanisms that address trust's honesty and benevolence dimensions by establishing a reputation for individuals and organizations based on their past behavior [62–64]. The many aspects of trust are outlined in further detail in Table 1.

The techniques used to express trust in cloud computing (Figure 2) are:

- Reputation-based trust: This represents a community belief about any particular entity. It is part of the faith model and directly influences the

Table 1 Trust dimensions

Trust Composition	Evaluated Component	QoS: Level of Assurance Social Trust, Reputation
Trust propagation	Describes the storage methodology of composing trust value in the network.	**Centralize:** responsible for work as data storage for all cloud entities. Suffers from storage space issues. **Distribute:** every entity must store and compute trust value. Suffers from attacks like bad-mouthing.
Trust update	Trust value is updated after completion of the transaction for future usage.	**Event-driven:** Trust value updates after the occurrence of any transaction. **Time-driven:** Trust value update after the predefined interval in a regular manner.
Trust formation	Describes the methodology for assigning the weight to various trust features.	**Single trust:** only single property considered for estimating like QoS. **Multiple trust:** multiple parameters are considered.
Trust aggregation	Describes the process of collecting trust features from other sources.	Bayesian inference [65], belief theory [66, 67], fuzzy logic [68, 69], regression analysis [70], graph theory [71, 72] , grey theory [73, 74], machine learning [75, 76], ant bee colony algorithm [77, 78], probability theory [79], rough set theory [80], MCDM approaches [81–83].

amount of confidence in any entity. Trust is an emotional connection between communicating entities and impacts reputation; it addresses the assessment of one entity towards another. The aggregate reviews of all elements comprise "reputation" [84].

- SLA-based trust: An SLA is a predefined and prior signed mutual agreement between a service provider and a consumer. It works on the concept of authentication. Cloud service consumers verify and evaluate the service at the completion time [85]. Moreover, since their nature is qualitative, an SLA only examines quantitative characteristics for measuring any resource distributor's performance and overlooks essential elements like security, privacy, stability, etc. A cloud client doesn't have comprehensive information on SLA observation and confirmation, so they need a third party or cloud dealer to check the QoS worth of cloud administration.

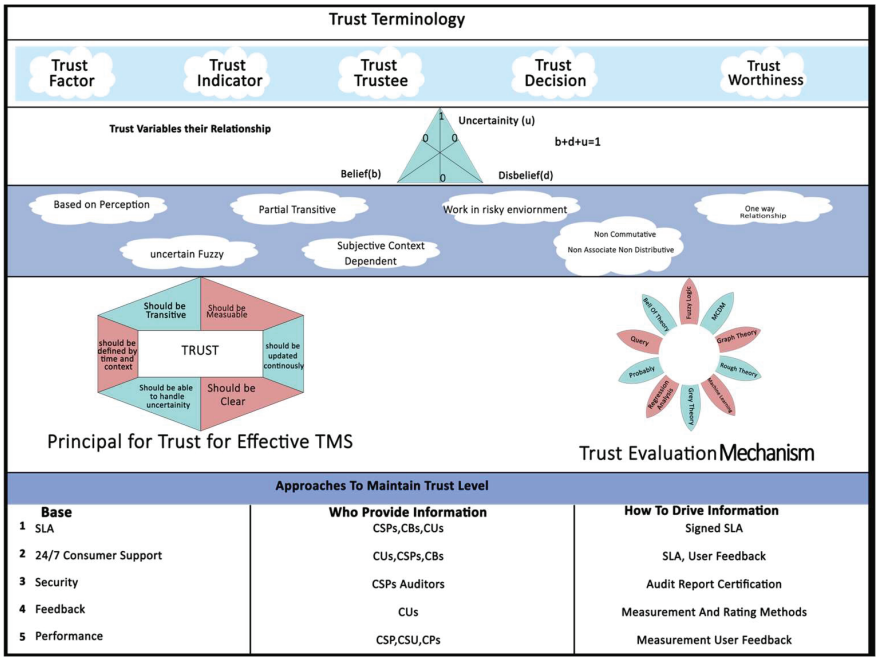

Figure 2 Trust taxonomy [55, 56].

- Self-assessment and revealing information: Cloud transparency and accountability raise the degree of confidence. The CSA created the STAR (security, trust, assurance, and registration) initiative to guarantee the cloud's openness [86]. It allows self-evaluation of security controls in the form of an "CAIQ" or a "CCM". This component's information is provided by the resource distributor, which raises the issue of its authenticity.
- Trust as services (TaaS): The CTA provides a service for monitoring and configuring security facilities of multiple service distributors. It is a cloud-based trust management solution that operates on the idea that "trust = control + visibility" [87]. The essential issue of any TaaS mechanism is deciding and helping in its maintenance in consultation with the service provider.
- Formal certification, standards, and reviews (Figure 3): Formal accreditation and standards are obtained from reputable, independent parties, including audits based on international security standards such as ISO/IEC/27000[27]. The trust parties that partly satisfy cloud clients

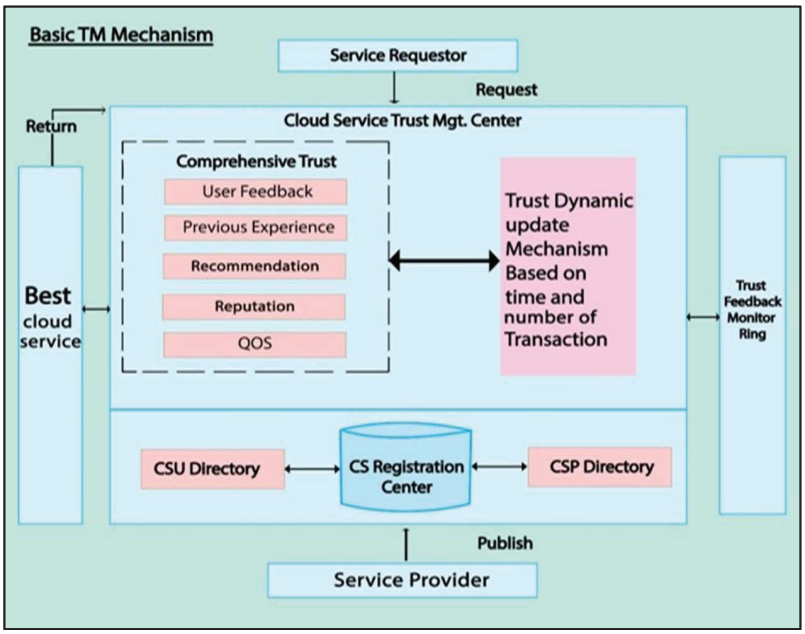

Figure 3 Trust management entities and directories [57, 58].

and distributors don't exist yet. Additionally, formal authorization for autonomous outsider cloud assessors doesn't exist [88].

From Table 2, we conclude that each method represents one aspect of trust while ignoring the other one.

2.2.2 Open issues in the trust management system

- In the cloud environment, the scale of deployment (cloud resources) continues to grow and cloud resources are dynamic, so it isn't straightforward to automate the trust model [90, 92].
- The policy-based technique of trust computation suffers from the issue of accountability [91].
- The characteristic of a distributed environment is auditability. Nevertheless, in the present situation, the leading CSP does not provide total transparency, a tracking capability, and an audit record to access history [89, 93].
- Typically, there is no communication between the requester and the supplier in the cloud environment. The requester lacks adequate information to estimate the provider's service quality [94].

Table 2 The issue with the trust mechanism in the cloud

Trust Strategies	Idea	Constraints
Reputation based	Reflect overall view of the community.	Complexity: too many cloud service requestors and distributors. Reputation is only useful when selecting a service initially, but not thereafter.
TaaS	Through third-party professionals (brokers).	Trusted authority maintains a trust level between communicator. The basis of a trust relationship between broker and consumer is not clear.
Formal accreditation, audit,	Through trusted independent authority.	There is no accepted method for evaluating cloud services by third parties. Acceptable procedures for both cloud customers and cloud service providers do not yet exist.
standard	Self-assessment by service distributors.	It may be possible that the wrong information is filed.
Transparency method	Re-evaluate and verify by monitoring and SLA verification.	Not able to deal with invisible attributes like privacy. Cloud users cannot evaluate on their own and require a professional third party.

- The evaluation methodology used the respondent rating as a component of the trust model that might lead to security concerns [94].
- Trust estimation is challenging due to aggregating subjective and objective parameters [95].
- When calculating trustworthiness, both quantitative and qualitative information from numerous sources must be considered. In addition, these roots have distinct properties, such as information acquired via SLA and audit reports [96].
- A single service provider may deliver various services requiring specialized knowledge. A computational model should express the context in which a service provider has built trust. Multiple viewpoints on cloud computing may relate to distinct service delivery methods. Therefore, understanding the context of service provider and requester is a complicated procedure for internet-based computing.
- Diverse attacks have been evaluated against trust and feedback-based frameworks. When establishing a model built on trust, these types of attacks should be a point of concern.
- The outcome of the trust model is represented by abstract techniques like master scoring and averaging procedures, which make models emotional

and require logic and flexibility. Since trust evidence is inaccessible to all participants and cannot be tracked, the results of trust evaluations are not convincing and cannot be relied upon [96].

2.3 Quality of Service (QoS)

Cloud computing gives opportunities to the IT industry by offering infrastructure and application services online through virtualization and subscription. Several service providers provide the same service with similar characteristics at a comparable rate. Due to the enormous heterogeneity in the service selection process, it's tough for the requestor to choose a particular service provider and identify its justification. In a distributed environment, QoS is optimum for selecting service and customer satisfaction [15]. Service mapping is the process of allocating the appropriate service to requesting consumers. It uses the consumer and provider QoS values as input [104]. A service distributor aims to increase overall performance and obtain the desired rewards [110]. Service selection involves several criteria, known as the multi-criteria decision-making (MCDM) approach. It also covers the similarity matrix used for ranking and selecting cloud services and its limitations. Furthermore, it presents information on the context of various trust factors and a summary of the QoS parameters used by previous researchers.

2.3.1 The SMI and QoS

The Camogie Melon University created the Cloud Service Measurement Index Consortium (CSMIC) [111]. The CSMIC has identified various QoS criteria to estimate cloud service trust levels. The service measurement index (SMI) is a hierarchically structured QoS. These are globally accepted, based on ISO [112], as illustrated in Figure 4. It offers the basis for estimating varied CSPs in the form of the distributor's key performance indicators (KPIs) [14, 17]. The SMI inputs QoS and ranks a provider's list using the MCDM. SMI classifies QoS parameters into seven sections. Every classification is additionally separated into at least two credits, as shown in Figure 4. It includes accountability, cost, security, privacy, performance, usability, assurance, and agility [112]. Quantitative metrics are expressed numerically, while qualitative indicators use nominal or ordinal scales. To date, no standard performance indicator or strategy outlines the KPIs for service classification and selection [8]. Researchers have developed a range of methodologies for estimating service quality. This article aims to compare several existing KPIs and determine the most relevant one from both the requestor and distributor perspectives.

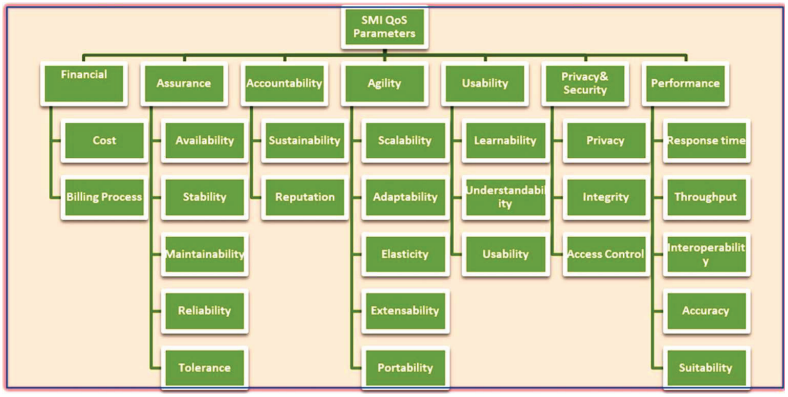

Figure 4 SMI parameters of QoS.

2.3.2 SMI evaluation parameters as per the CSMIC

The cloud service is judged based on the seven key SMI features listed below:

1. **Accountability:** It contributes to establishing a customer's confidence in a cloud service and ensures that customer data is securely managed. It involves auditability, authenticity, sustainability, and reputation. Accountability identifies the cloud service's unique features and plays a crucial part in establishing service trust. A high-level perspective on accountability includes violations abiding by punishment. Aspects of accountability:
   - *Time/goals:* Prevention, detection, evidence, judgment, punishment.
   - *Information:* Identity of participants, violation disclosure, violator identification.
   - *Action:* Centralized vs. decentralized, automatic vs. mediated.
2. **Agility:** The requestor may consume and adjust the need for resources with less expenditure. It incorporates adaptability, flexibility, portability, and elasticity. It specifies the rate of change metric and assesses how thriving service-providing organizations accept the progression and integrate with new capabilities. Agility is achieved by:
   - More rapid time-to-market
   - Automated allotment of resources
   - Faster improvement
   - Adaptive auto-scaling.

3. **Financial**: Cost-effectiveness is one of most imperative aspects of cloud computing. Before migrating to the cloud, the primary concern is whether or not CC is efficient from the perspective of finance. It included the charging process and billing procedure.
4. **Performance:** This group covers the features and methodology of offering resources and services. Through this metric, entities must determine how well their application will perform after accessing cloud resources and whether they meet their predefined objective. It consolidates response time, interoperability, accuracy, and functionality. It tests throughput and latency. Typically, each test checks different aspects of performance, including:
    - *Stress testing:* When resources are put under high load, and checks reliability, stability, and responsiveness.
    - *Load testing:* Analyses how effectively the system functions with numerous users.
    - *Browser testing:* Determines browser–system compatibility.
    - *Latency testing:* Analyses how effectively the system functions with numerous users.
    - *Targeted infrastructure testing:* Checks system issues.
    - *Backup testing:* Verifies a system's ability to allocate additional resources during periods of heavy traffic or consumption peaks. This test can aid in preventing user experience-detracting interruptions.
    - *Capacity testing:* Identifies and benchmarks the cloud system's maximum traffic or load.
    - *Soak testing:* Measures the performance of a system throughout extended periods of high traffic.
5. **Assurance:** These criteria determine whether the SLA-guaranteed traits are met. It integrates availability, tolerance, recoverability, stability, dependability, and usefulness.
6. **Security and privacy:** Security depends on the leaders' access control, data security, data hardship, data integrity, and data location. Balancing privacy and safety is a significant obstacle. This multidimensional measure includes data integrity, privacy, availability, and confidentiality attributes.
7. **Usability:** Represents the quality of interaction between user and their cloud service. Ease of purpose integrates transparency, learnability, present limit, and operability.

2.3.3 QoS model in the cloud environment for service selection

Quantitative and qualitative key performance indicators (KPIs) evaluate cloud services. Hardware and software estimation tools evaluate quantitative KPIs, while qualitative KPIs may be accessed through user experience [44]. This study addresses the shortcomings associated with SMI properties by incorporating additional cloud service selection factors. The proposed research includes 25 cloud service selection factors. Enhancement of a few extra attributes may be acceptable if a subject matter expert suggests it and they play a substantial role in service selection. The valuable metrics and their formulation used in the ranking are as follows:

- **Cost:** Due to the provision of equivalent quality and dimensions, comparing the charges of various providers is a highly tedious task. It comprises the cost of data storage along with security as well as the cost of primary and additional features. It is defined as:

$$C_{cost} = \frac{CCS}{w_1 * p + w_2 * q + w_3 * r + w_4 * s + w_5 * t} \tag{1}$$

where

$CCS =$ Cost of offered cloud service;

$$\sum \text{wi} = 1$$

$p, q, r, s, t$are different KPIs related to the aspects of cost. (2)

- **Billing process:** This includes the compilation of billing information and issuing an invoice. It is a non-quantifiable attribute and reflects how simple and efficient the service's billing procedure is. It includes information about resource type, resource management, resource hierarchy, payment profile, billing account type, charging cycle, and billing contact.
- **Availability:** This indicates the extent of operable time and committed conditions and represents the actual function time of service without interruption. Internet connectivity, security, data backup, storage, and power outages are some of the factors that CSPs supply to guarantee availability. It is defined as:

$$C_{avail} = \frac{TST - TTNA}{TST} \tag{3}$$

where *TST*: Total service time.

TTNA: Total time for which services are not available.
The range of availability is 0–1, where higher values indicate higher availability.

- **Service stability:** This serves as a key to optimal execution. It illustrates the reliability of cloud service performance over time. A service possessing fault tolerance and resiliency features makes it more sustainable. It relies upon three elements: server checking, reproduction, and security. It is described as:

$$C_{stab} = \sum \frac{a/T}{n} \tag{4}$$

where a represents the difference between the actual performance of cloud service and the promised value in the SLA, T = service time, n = number of users
The range of stability is 0–1, where a higher value indicates higher stability.

- **Maintainability:** This is un-measurable and refers to a server's backup system. Usually, a CSP has multiple data centers containing thousands of data servers that require a specified level of preservation. It is essential to reconstruct consumers' data to provide continuous data access and services. It incorporates network replication, data storage, and power supply.
- **Reliability:** This represents the degree to which cloud services operate without failure at a particular time along with condition. It depends on the number of meantime failures promised by the CSP and failures experienced by the client in the past.

$$C_{reliab} = VB * SMTTF \tag{5}$$

$$VB = (1 - \frac{num\ failure}{n})$$

where VB = violation probability, n = number of services, num failure = number of services that experience a failure in a time slot less than promised by the CSP.

$$SMTTF = \frac{\textit{TOTAL TIME BETWEEN FAILURES}}{\textit{TOTAL NUMBER OF FAILURES}} \tag{6}$$

where TOTAL NUMBER OF FAILURES > 0.

- **Fault tolerance:** This refers to how data can be recovered in case of fault or disaster so that the system can continue operating without interruption. Data redundancy is one mechanism to tolerate imperfection.

Clients' prime responsibility is to mention the fault tolerance point in the SLA. It includes the record violation rate, resolution quality, and violation resolution time.

- **Sustainability:** This signifies a cloud service's environmental, social, and economic impact through reusability of computing resources [113]. It indicates how many components of a service may be reused without modification. Aspects of sustainable practice:
  - Economic: risk management, consistent, profitable growth.
  - Environmental: licence compliance, biodiversity management.
  - Social: customer support, human rights, equality opportunity.

$$C_{sustain} = \frac{NCSP}{NCSU} \tag{7}$$

where NCSP is the number of characteristics offered by a service provider and NCSU is the number of characteristics required by the consumer.

- **Reputation:** This signifies the goodwill of an entity in the community, which would result from excellent service or behavior in the past. The basis of reputation consists of objective and subjective trust factors. It is defined as:

$$C_{rep} = \frac{\sum_i rank_i^j}{\sum i} \tag{8}$$

where rank is the rank of *j*th CSP assigned by the *i*th cloud user.

- **Scalability:** Check whether a provider can handle more requests concurrently. Scaling latency refers to the time it takes to assign new resources and instances per consumers' needs. The cloud has two sorts of scalability.
  - Horizontal: when the provider's ability expands by adding additional virtual machines, platforms, and software.
  - Vertical: Raising a service provider's memory, CPU, and network bandwidth.

  It is represented as:

$$C_{scal} = \sum_{i}^{k} \sum_{j}^{n} C_{i,j} \tag{9}$$

where i = cloud service, k = number of services used by clients, j = represents the resource proportion of resources that needs to be increased, where a higher value indicates better scalability.

- **Adaptability:** This represent the ability to change from the current configuration to the new format based on customer demand. It is qualitative. The aspect of adaptability in the environment is divided into three sub-parts:
  - Cloud resource adaptation
  - Adaptation aims
  - Adaptation methodologies.
- **Elasticity:** This indicates the degree to which cloud services scaled during peak times. The description is more abstract and based on the client's experience [114]. It is defined as:

$$C_{elas} = w_1 * E_g = w_2 * E_d, \sum w_i = 1$$

  where $E_g =$ elasticity growth, $E_d =$ elasticity down.
  - $E_g = \frac{1}{a*b}$, a = average response time of CSP from under-provisioning state to an optimal state, b = average amount of resources that need to be optimized or grown.
  - $E_d = \frac{1}{c*d}$, c = average response time of CSP from over-provisioning state to an optimal state, d = average amount of resources that need to be optimized or scaled down.
- **Extensibility/flexibility:** This shows the ability to append additional elements and features to its existing structure of resources. It is also notable for its robust adaptability and discoverability. As it moves between public and private IT environments, the hybrid deployment strategy demands a highly extensible approach. It is defined as:

$$C_{exen} = W_i * VC + W_j * MR$$
$$VC = \frac{AV}{TV}$$
$$MR = \frac{RM}{TM}$$

  where:
  VC represents the number of variation points can be adapted according to cloud computing.
  AV = Adapted variation point.
  TV = Total variation point. *MR* represents how many mismatches can be resolved.
  RM = Resolved mismatch.

TM = Total mismatch.

- **Portability:** This refers to the ability to move the client application from one CSP to another CSP and is generally used in the hybrid cloud model. There are two types of portability:
  - Cloud data portability is moving data from one cloud service to another without re-entering information.
  - Cloud application portability refers to ability to transfer an application one cloud provider to another or between a client's environment and the cloud.
- **Learn ability:** This refers to how consumers learn all the functionality of services offered by the cloud. It depends on understanding, mental cognition, and a Graphical description of the functionality.
- **Understandability:** This represents how easily users can understand the cloud service. It is essential for quality, reusability, maintainability, and reliability.
- **Usability**: This refers to the simplicity of its use or how quickly a user can accept a cloud service. The primary components for measuring the ease of use of any service are operability, learnability, and install ability.

$$\text{Usability}(UT) = \frac{1}{n}\sum_{i=1}^{n} OT - \left(\sum_{i=1}^{n} LT + \sum_{i=1}^{n} IT\right) \tag{10}$$

where:
Operation time (*OT*): effective service delivery time.
Learn time (*LT*): time required for learning the service.
Installation time (*IT*): time required to install the service.

- **Privacy and confidentiality:** Privacy is one of cloud services' most crucial and relevant decision criteria. Customers seek complete protection and confidentiality for their sensitive data, financial information, and geo-location in the cloud. The CSP must coordinate several apps, tools, utilities, and fixes to guarantee privacy. Cloud-based privacy uses homomorphic encryption and anonymization techniques. Due to the diverse physical locations of data centers around the globe, geo-location should be included in the SLA.
- **Access control:** This includes authentication, permission, and auditing. It refers to the capacity to limit access to cloud-based information and helps to reduce risk. It involves a pre-existing trust-based relationship between the supplier and the consumer and a norm of negotiation

to explain the resources, users, and access choices. Authentication is performed through passwords and PINs.

- **Integrity:** This assures that unauthorized users can't share data in the cloud [114]. Techniques used for ensuring data integrity include:
  - Generating hashes.
  - Using trusted third parties.
  - Provable data possession.
  - Proof of retrieval evidence.
- **Response time:** This describes how quickly the service is available for usage and represents the duration between service acceptance and response transmission. It relies on factors such as the average reaction time, the maximum response time, and the system performance failure rate. It is defined as:

$$C_{resp} = T_r - T_0 \tag{11}$$

where T_r represents the time interval of user *i* request for a particular service.

To represent the time interval when service is completed by a particular provider. The average response time for *n* (*n* represents total number of services requested) service are:

$$T_{avg} = \frac{\sum_i^n C_{resp}}{n}. \tag{12}$$

A lower value indicates a better response.

The value of the response should be $C_{resp} > 0$. It is measured in milliseconds.

- **Throughput**: This indicates the total performance of a cloud service and is characterized by the quantity of work executed per unit of time. It depends on variables such as job completion time, the network and disk data transmission rate, the number of tasks, and the correspondence delay between processes.

$$C_{through} = \frac{n}{(Ext_n + ov)} \tag{13}$$

where:

n = number of tasks that were submitted on *m* cloud machine.

Extn = Execution time taken for *n* tasks.

ov = the overhead due to some factors like communication delay.

The range of throughput is 0, 1. Where a higher value indicates higher throughput.

- **Interoperability and compatibility:** Interoperability is the capacity to interact with services provided by the same or a different CSP. It is more qualitative, subjective, and based on client experience. Usability and accessibility are the two primary elements of cloud interoperability.

$$C_{inter} = \frac{NP_{CSP}}{NP_{CSU}} \tag{14}$$

where:
NP_{CSP} = number of platforms offered by the CSP.
NP_{CSU} = number of platforms required by the CSU.
The range of interoperability is 0, 1 where a higher value indicates higher interoperability.

- **Accuracy**: This represents the degree to which the cloud service provider is compromised with the SLA. It is defined as:

$$\sum_{i} F_i/n \tag{15}$$

where F_i is the number of times the CSP fails to satisfy the promised value for user *i* and n = number of previous users.

- **Suitability**: Check whether resources are being allocated to the user according to their expectations. At the time of service selection, the user may pick the cloud service that best fulfills their functional and non-functional needs. There are two instances:
  - If more than one CSP meets both essential and non-essential requirements.
  - If no CSP satisfies their functional and non-functional requirements, only CSPs who meet their functional requirement will be selected.

It is defined as:

$$C_{Suit} = \frac{NE_{CSP}}{NNE_{CSU}} \tag{16}$$

where:
NE_{CSP} = number of essential features offered by the CSP.
NNE_{CSU} = number of non-essential features required by the CSU.

3 Related Work

The SMICloud technique developed by Garg et al. (2011) evaluates and ranks cloud services. They assisted consumers in selecting cloud service providers

based on availability, performance, and affordability. The algorithm evaluated cloud services based on user preferences and service quality to assist in selecting large-scale, multi-tenant cloud solutions [6].

Sarwar and Khan (2013) conducted a comprehensive analysis of confidence in cloud security. They assessed the establishment and preservation of trust between cloud users and providers. Their findings indicate that privacy, integrity, and access control are crucial for dependable cloud services. The research highlighted trust management systems capable of adapting to the dynamic and distributed characteristics of cloud settings [15].

Srivastava and Khan (2018) assessed both the advantages and disadvantages of cloud computing. Their results show that adoption of the cloud depends on trust, privacy, and safety. Examined in the research were scalability, adaptability, data breaches, and user control of cloud services to reduce these hazards while preserving the dependability of cloud systems [18].

Noor et al. underlined in 2016 the challenges of researching cloud trust management. Without clear trust measures and service level agreements (SLAs), it became challenging to keep faith in the absence of trust. In particular, in multi-cloud and federated cloud systems, they suggested open and responsible trust evaluation techniques [21] to increase user confidence in cloud services.

Goyal and Deora evaluated the reliability of systems controlling cloud trust. They examined ideas related to the evaluation and maintenance of trust between cloud users and providers. Their research emphasized the need of trust ratings for the security and dependability of cloud services. They examined decentralized cloud trust management, including the evaluation of trust and detrimental behavior [43].

For fog computing, Afzali et al. (2022) developed a strong trust evaluation method combining social factors, reputation, and quality of service (QoS). Examined were trust qualities to improve choice of secure services. Developed for context-aware trust management in fog computing employing distributed networks [90], this method was inspired by QoS, reputation, and social criteria.

Pourmohseni et al. (2022) developed a computational trust model for the social Internet of Things (SIoT) using interval neutrosophic numbers. Their technique addressed the imprecision and unpredictability in SIoT trust evaluation. Neutroponic logic enhanced trust evaluations, IoT device security, and social collaboration [97].

To build confidence between consumers and suppliers, Monir et al. (2015) looked at trust management systems in cloud computing. They evaluated

openness towards trust, privacy, and data security. Their survey on reputation-based and cryptographic trust evaluation [98] led one to propose study on trust management.

Alhanahnah et al. (2017) classified trust in cloud computing into three categories: establishment, maintenance, and dissolution. Their study demonstrated the influence of service quality, openness, and legal compliance on confidence at every stage. The taxonomy allows cloud service providers to enhance trust management, hence fostering user confidence [99].

Kumar and Goyal (2022) introduced PRTrust for secure service sharing in peer-to-peer federated clouds. Their trust management and risk assessment technology enables cloud customers to make educated choices on trust and risk. PRTrust enhanced the security and dependability of service interactions in decentralized cloud systems when conventional trust mechanisms may be inadequate [100].

Focusing on dynamic and adaptive cloud trust management, Mousa et al. (2021) provide a multi-dimensional trust model for context-aware services computing. Their method evaluates cloud service providers holistically using trust components including context-specific criteria, reputation, and service quality. Intricate cloud service configurations need context-aware trust management [101].

Ray et al. (2018) used game theory to establish reliable cloud federations that ensure profitability and quality for cloud service providers. They optimized resource allocation and trust in cloud federation via game theory. Game theory may assist cloud federations in managing trust and profit distribution [102].

Hussain et al. (2014) conducted a rating of cloud services based on historical quality of service (QoS) data. Their technique enhanced cloud service selection by using historical performance data. Parallel ranking expedited and enhanced cloud service assessments in large, dynamic cloud systems with fluctuating service quality [103].

Lee and Seo (2016) introduced a hybrid multi-criteria decision-making (MCDM) approach for the selection of cloud services. Evaluating cloud services using the balanced scorecard (BSC), fuzzy analytical hierarchy process (AHP), and fuzzy Delphi hybrid approaches including quantitative and qualitative criteria [104] were used to fully assess cloud services.

Srishylam and Umar (2017) suggested a reputation-based method of controlling cloud services known as Cloud Armor. Using reputation ratings helped them build confidence between cloud users and providers. An adaptive

system raised trust by changing reputation ranks in response to user feedback and service effectiveness [105].

Manoharan et al. (2021) retrieved papers from outsourced cloud data by use of a similarity assessment and ranking system based on Euclidean distance. Their techniques helped cloud document retrieval become more accurate and effective. Using similarity assessment, the system ranked documents based on their relevance to user searches thereby enabling extensive data retrieval from cloud storage [106].

Jatoth et al. (2019) build SELCLOUD, a hybrid architecture, to enable the choice of cloud services depending on many criteria. Using several decision-making techniques, they assessed cloud services according to pricing, quality of service, and client preferences. By means of the hybrid approach, cloud services were more precisely and fully evaluated, thereby guiding multi-cloud and federated cloud systems in selecting services [107].

Thanks to Ant Lion optimization, Dewangan et al. (2019) created an autonomous cloud resource management system grounded on service-level agreements (SLAs). Following SLA guidelines, their method maximized the use of cloud resources. Ant Lion optimization's capacity provides efficient and flexible resource management [108] the framework fit dynamic and scalable cloud systems.

Selvaraj and Sundarajan (2017) created an evidence-based fuzzy logic approach to assess trust in cloud services. Using their cloud trust assessment tool to combine user input with service performance enhanced trust management. Particularly under uncertain or incomplete conditions, fuzzy logic increases the range of trust ratings [109].

A comprehensive literature survey is given in Table 3 based on the references provided. Each entry includes the reference number, author(s) and year, objective, methodology, pros, cons, and research gap.

3.1 Significance of this Work

After analyzing previous studies, researchers have utilized various methodologies to assess cloud services. There are multiple approaches to solving the problem of rating cloud services and selecting a reliable service provider. The SMI cloud architecture briefly describes multiple parameters for service selection, but it is not practical for users and providers to consider each parameter during service selection. Therefore, the main question is which QoS is the most appropriate. However, existing techniques have certain

Table 3 Literature survey

Ref	Author/year	Objective	Methodology	Pros	Cons	Research gap
[6]	S. K. Garg, (2011)	To compare and rank cloud services based on multiple criteria.	Developed the Smicloud framework for ranking cloud services based on QoS.	Provides a comprehensive ranking framework for cloud services.	Limited to a few cloud services; does not consider dynamic trust factors.	Expanding the framework to integrate dynamic trust management and reputation mechanisms.
[15]	A. Sarwar and M. N. Khan (2013)	To review trust aspects in cloud computing security.	Literature review and analysis of trust mechanisms in cloud environments.	Provides a clear understanding of trust issues in cloud security.	Does not propose new trust models or algorithms.	Lack of empirical studies and trust model implementations.
[18]	P. Srivastava (2018)	To provide an overview of cloud computing technologies.	Review of key concepts, benefits, and challenges in cloud computing.	Comprehensive overview of cloud computing landscape.	Lacks in-depth focus on trust and security concerns.	No specific focus on trust or security in cloud computing.
[21]	T. H. Noor et al. (2016)	To address the state-of-the-art in managing trust in cloud environments.	Review of current trust management systems in the cloud and their challenges.	Extensive coverage of trust management challenges.	Does not provide solutions for trust management issues.	Lack of real-world applications and solutions for trust management challenges.
[43]	P. Goyal (2016)	To explore the reliability of trust management systems in cloud computing.	Analysis of trust management systems' reliability in cloud services.	Highlights reliability issues in current trust management systems.	Limited in scope; only focuses on specific trust management systems.	Broader exploration of different trust management systems across diverse cloud architectures.
[90]	M. Afzali et al. (2022)	To create a trust evaluation framework for secure service selection in fog computing.	Developed a QoS, reputation, and social criteria-based trust evaluation framework.	Integrates multiple dimensions (QoS, reputation, social criteria).	Focuses only on fog computing; less generalizable to cloud computing.	Expansion of the model to cover broader cloud and hybrid environments.

[97]	Pourmohseni et al. (2022)	To develop a computational trust model for Social IoT based on interval neutrosophic numbers.	Proposed a trust model using interval neutrosophic numbers in social IoT.	Innovatively uses interval neutrosophic numbers for trust evaluation.	Focused only on Social IoT; limited application to cloud services.	Application of the model in cloud environments beyond IoT.
[98]	M. B. Monir et al. (2015)	To survey trust management in cloud computing.	Review and analysis of trust management systems in cloud computing.	Comprehensive review of trust systems in cloud environments.	Does not provide specific model recommendations or improvements.	Research lacks practical trust management system implementation.
[99]	Alhanahnah et al. (2017)	To develop taxonomy of trust factors and trust phases for cloud service providers.	Proposed a taxonomy of trust phases and factors for cloud services.	Provides a structured view of trust factors.	No implementation or validation of the proposed taxonomy.	Real-world validation and implementation of the trust taxonomy.
[100]	R. Kumar l (2022)	To develop a performance-based risk-driven trust model for secured service sharing in peer-to-peer federated cloud.	Proposed the PRTrust model based on performance and risk factors.	Integrates risk management with trust evaluation.	Focused only on peer-to-peer federated clouds.	Application of the PRTrust model in different cloud environments.
[101]	A. Mousa et al. (2021)	To propose a multi-dimensional trust model for context-aware services computing.	Developed a multi-dimensional trust model integrating context-aware computing.	Innovatively integrates context awareness into trust evaluation.	No real-world implementation or performance evaluation.	Validation of the model through implementation and case studies.
[102]	B. K. Ray et al. (2018)	To develop a game theory-based approach for trusted cloud federation formation.	Applied game theory to form trusted cloud federations based on quality and profit assurance.	Uses game theory to assure trust and profitability in cloud federations.	Only focuses on federations; less applicable to individual cloud services.	Exploration of game theory applications in non-federated cloud environments.

(*Continued*)

Table 3 Continued

Ref	Author/year	Objective	Methodology	Pros	Cons	Research gap
[103]	Hussain et al. (2014)	To propose a parallel cloud service selection and ranking model based on QoS history.	Developed a parallel service selection model based on QoS history.	Enhances efficiency by using parallel processing for cloud service selection.	Limited focus on trust and security concerns.	Incorporating trust factors into the parallel service selection process.
[104]	S. Lee (2016)	To propose a hybrid multi-criteria decision-making model for cloud service selection.	Developed a hybrid model using BSC, fuzzy Delphi method, and fuzzy AHP for service selection.	Combines multiple decision-making techniques for robust service selection.	Complexity of the model increases computational requirements.	Simplifying the model without compromising accuracy in cloud service selection.
[105]	R. Srishylam (2017)	To develop Cloud Armor, a reputation-based trust management system for cloud services.	Proposed a reputation-based management system called Cloud Armor for cloud services.	Focuses on reputation-based trust to enhance security.	Limited consideration of dynamic trust aspects.	Expanding the model to integrate dynamic trust and real-time evaluations.
[106]	Manoharan et al. (2021)	To propose a Euclidean distance-based similarity measurement for document search in outsourced cloud data.	Developed a similarity measurement technique for document search in cloud environments.	Efficient similarity measurement using Euclidean distance.	Focused only on document search; does not address broader trust issues.	Application of similarity measurement techniques in broader cloud trust systems.
[107]	C. Jatoth et al. (2019)	To propose a hybrid multi-criteria decision-making model for selecting cloud services.	Developed SELCLOUD, a hybrid model for selecting cloud services based on multiple criteria.	Robust service selection model with multi-criteria decision-making.	Complexity increases computational overhead.	Simplifying the model while retaining accuracy and performance.

[108]	Dewangan et al. (2019)	To propose a SLA-based cloud resource management framework using the Ant Lion optimization algorithm.	Developed a cloud resource management framework based on Ant Lion optimization and SLA.	Efficient SLA management using metaheuristic optimization.	Limited focus on trust management in cloud services.	Incorporating trust factors into SLA-based cloud resource management.
[109]	A. Selvaraj (2017)	To propose an evidence-based trust evaluation system using fuzzy logic for cloud services.	Developed a trust evaluation system using fuzzy logic.	Utilizes fuzzy logic to manage uncertainty in trust evaluations.	Fuzzy logic models may be computationally expensive.	Exploring lightweight trust evaluation methods for cloud services.

drawbacks that hinder the decision-making process and affect its accuracy and consistency.

1. Expanded decision-making standards increase application and computational complexity, hence diminishing performance.
2. Comparing QoS is tricky.
3. Rank inversion is crucial.
4. In cloud service selection, they are incapable of controlling fuzziness and subjectivity.

3.2 Why It's Not Practical for Users and Providers to Consider Each Parameter During Service Selection

There are good reasons why customers and providers struggle to evaluate all cloud service options. Users often have to balance dependability, performance, pricing, security, and other issues, adding to the complexity. This makes it difficult to consider all the factors and may cause confusion and decision fatigue. Customer decision paralysis may result from a large list of needs. This might make prioritizing features based on user demands challenging, leading to procrastination or poor decision-making. Our large data and measurement set may obscure essential details or misread features, adding to the process's complexity. Rushing individuals may not be able to examine all the aspects, resulting in subpar outcomes. Another challenge for suppliers is clearly presenting all the key aspects of their services without overwhelming users or hiding their core features.

- **Complexity Overload:** Complexity overload makes it difficult for users to evaluate several factors at once – that is, cost, reliability, security, and performance.
- **Providers:** For providers, clearly and succinctly stressing all of these elements might be challenging.
- **Decision paralysis:** Some consumers may find it challenging to prioritize the features depending on the large number of criteria, therefore causing uncertainty.
- **Information overload:** Reliable comparisons and assessments of services might be challenging given the abundance of data and metrics at hand.
- **Time and effort:** Users who have time-sensitive decision-making requirements might not be able to provide enough focus to properly evaluating every criterion.

3.3 How Does Our Approach Address These Issues?

We use powerful algorithms to integrate several components to create a consistent trust score, simplifying assessment. These concerns are addressed. One statistic simplifies evaluation with a solid, clear standard. Users may avoid choice fatigue by making better, faster judgements based on a single trust score rather than several variables. Our method helps suppliers since the trust score enables them immediately describe their product's dependability and quality without much elaboration. This tailored assessment technique streamlines decision-making by focusing clients on service quality and trust. Our solution simplifies and clarifies the decision-making process for consumers and cloud service providers, making it easier to choose the right service.

- **Simplified trust estimation:** The new approach aggregates numerous components into a single trust score, hence simplifying trust estimate. This all-inclusive and simply understandable dependability scale simplifies the assessment process.
- **Enhanced decision-making:** Users can more rapidly and with less mental effort make better decisions when the information is simplified around a single trust score instead of several factors.
- **Effective communication:** Service providers may show the dependability and high quality of their products by means of the trust score, therefore sparing consumers pointless information.
- **Focused evaluation:** The system helps consumers avoid losing themselves in pointless minutiae by guiding them to focus on the most important elements of trust and service quality.

4 Research Methodology

To investigate, and for a better understanding of the trust management and cloud services offered by various providers, this segment addresses the identification of critical elements in deciding the SMI QoS for selecting the best-suited cloud service and service providers. This discussion helps to conclude the essential elements through positioning-based feedback from cloud users. It finalizes the critical aspect of QoS that was already present, or that should be added for building trust-based solutions. To improve the study approach in cloud computing and trust management, this paper covers the data source, search strategy, search-related questions, and study selection process method. A systematic analysis will assist the researcher in finding

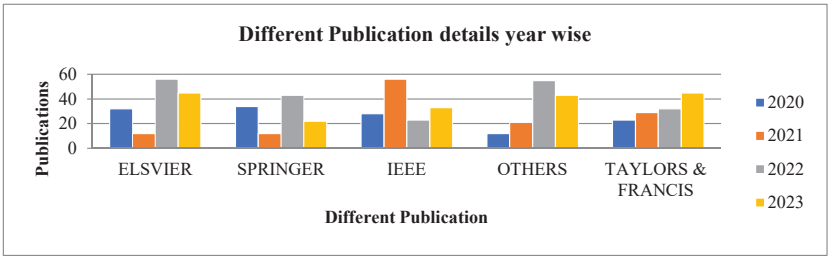

Figure 5 Research articles collected from different publications in the last 4 years.

a solution to the security of the cloud computing problem and the trust management model.

4.1 Data Source

We analyzed more than 200 papers from different platforms like IEEE-Explore Research-Gate, Google-Scholar, Wiley Library, ACM library, Science Direct – Elsevier, Springer, Hindwai, Sagepub, and Taylor & Francis. Figure 5 is a graph displaying the number of papers and platforms. The important contributions from many articles published between 2015 and 2023 on trust management systems, including trust, MCDM, SMI, SLA-based booking, single goal, bi-objective, multi-user evaluation techniques, and QoS boundaries-based booking methods in distributed computing, have been compiled for future use.

4.2 Research Questions and their Motivation

This article has designed and answered ten research questions:

Question 1: What is the obstacle to cloud computing?

Question 2: What is the current state of privacy and security mechanisms for internet-based computing?

Question 3: How can the executive's trust be built in the appropriate environment?

Question 4: What are the methodologies for trust value assessment and loopholes of the current trust methodologies?

Question 5: Which components ought to be viewed in the choice of CS?

Question 6: What is each administration choice plan on reproduction factors, datasets, test systems, and QoS measures?

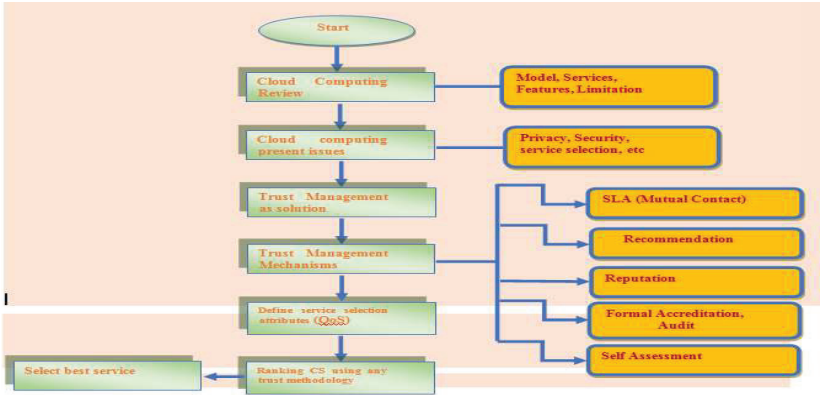

Figure 6 Flowchart of trust management in cloud computing.

Question 7: Did the responsive investigation lead to checking the accomplished results?

Question 8: Which SMI criteria are most significant when selecting a cloud service?

Question 9: How do you evaluate the non-measurable SMI attributes?

Question 10: Which problems and solutions are more appropriate in future research related to cloud service selection and ranking of various service distributors?

Much research has already been done to handle the security and privacy issue, ranking the QoS and improving trust mechanisms [35]. The present study uses the CSMIC-developed framework known as SMI architecture to define the essential QoS for selecting the most favorable cloud service [39]. It helps to solve present research challenges and is beneficial for future research work for ranking the service selection process.

4.3 Review Strategy

Here, a comprehensive methodology is intended to locate unbiased and relevant research papers on security and privacy problems of cloud computing using different trust management strategies and the SMI framework of QoS Figure 6 depicts a whole trust management system's review procedure. It involved a few articles from Springer, Elsevier, Wiley, and IEEE and gathered research papers in light of the watchwords utilized in search rules. The majority of the analyzed articles were discarded based on their names, as

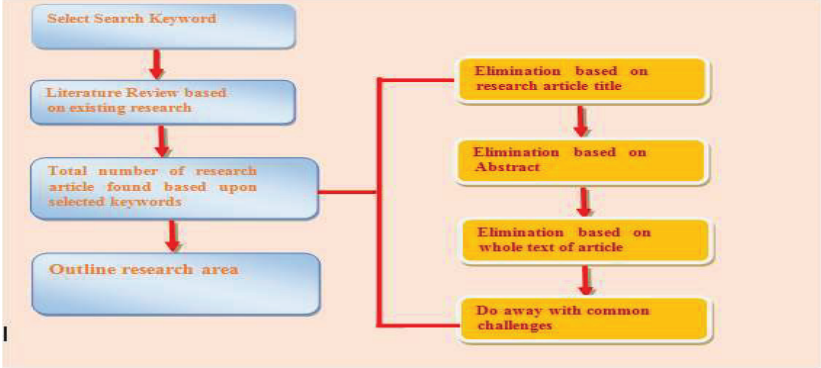

Figure 7 Review technique of article identification in trust management under the cloud environment.

they did not comply with our current research review. Additionally, several articles were excluded due to the absence of an idea and conclusion. The initial number of gathered research and review publications was 150, yet most of the articles were screened out due to failing to meet referenced standards. The remaining papers were evaluated to examine watchwords and acceptance/rejection criteria. In the end, 209 papers were finalized for review of the distributed computing paradigm (Figure 7).

5 Results and Discussion

Trustworthiness in cloud computing is crucial for service selection, and measuring trustworthiness using metrics like SLAs, social interaction recommendations, and reputation can help. A comprehensive comparative analysis of trust management techniques and QoS is provided, focusing on research articles published between 2015 and 2023. The SLA-based approach is essential for protecting against violations but may not be feasible for all cloud services. The recommendation-based approach estimates trust levels using subjective trust, while the reputation/feedback-based approach uses user comments and opinions on QoS and security. A comprehensive approach-based model is needed to establish trust and credibility in a cloud environment. A review of research on trust management models from 2016 to 2023 shows that comprehensive trust management techniques are increasingly explored. For a comprehensive trust model with dynamic updates for user and provider directories, a proposed trust estimate technique initializes directories, gathers and preprocesses data, computes trust scores, changes trust levels, and

produces reports. These trust-building algorithms and trust-management systems help to enhance cloud decision-making, and use trustworthy criteria to evaluate a service or organization. Useful measures include SLA monitoring, recommendations for social engagement, and reputation history. Developing confidence in a good or institution depends on evaluating trustworthiness criteria. Direct trust from service level agreements and indirect trust from reputation and referrals provide a more realistic and predictable confidence level. Algorithm 0 presents a whole trust model with dynamic user and provider directory modifications. Initializing directories, gathering and pre-processing data, computing trust scores, adjusting trust levels, and generating reports are part of it. Algorithm 1 explains how to interact with the service provider directory, assign weights to trust measures, and choose the highest-ranked cloud service provider depending on whole trust ratings.

5.1 Proposed Algorithms for Trust Estimation

Algorithm 0 represents the complete working procedures of the comprehensive trust model with a dynamic update of the trust level in both the user and provider directories.

Algorithm 0

Inputs:

- CSU Directory: Details about cloud service users.
- CSP Directory: The CSP Directory contains information kept by cloud service providers.

Outputs:

- Updated trust levels: Cloud service providers' and users' trust levels, updated to reflect new information and changes.

Algorithm steps:

1. *Initialization*:
    - Initialize directories: Set the default or historical-based trust levels of the CSU and CSP directories first.
    - Define trust parameters: Find and define the measurements that will form the foundation of trust computation.

2. *Data collection*:
    - Collect new data: Note any recent data on performance measures, user ratings, and service use provided by CSPs mentally.
    - Update directories: Add most current information to the CSP and CSU databases.
3. *Preprocessing*:
    - Normalize new data: Standardize the updated data to ensure it is consistent by nature. Standardize the measurements, comments, and ratings before including them into the current data system.
    - Filter relevant information: Filtering among the present directories, find the most relevant information for trust computation.
4. *Trust calculation*:
    - Compute individual trust scores:
        - For CSPs: As a weighted average of user reviews, dependability, security, and KPIs, determine a trust score for each CSP.
        - For CSUs: Users' interactions and comments may be used to calculate a trust score. This helps CSUs evaluate how reliable they are and how they impact the service ecosystem.
    - Adjust for recent feedback: Use fresh data or changes in provider or user activity to dynamically change trust ratings.
5. *Dynamic update*:
    - Update trust levels:
        - For CSPs: Change the trust levels in the CSP directory depending on calculated trust values for CSPs. Point out variations in the dependability and quality of the service.
        - For CSUs: Update the trust level in every user's CSU directory to correspond with their dependability, recent comments, and current interaction record.
        - Recalculate aggregates: One approach to ensure accuracy of aggregate trust levels is frequent recalculating of them.

6. *Output updated trust levels*:
    - Generate reports: Check that, with any pertinent modifications, all CSPs and CSUs have current trust levels corresponding with the latest trust ratings.
    - Disseminate information: Make sure the material is easily available and useable; next, distribute it to customers and suppliers via the appropriate channels using the most current trust levels.
7. *Feedback loop*:
    - Monitor and review: Always keep an eye on how well the trust model is working by reading customer and provider reviews.
    - Adjust parameters: Improve the accuracy and relevance of the trust calculation by adjusting the parameters and weighting based on feedback and observed performance.

Algorithm 1 shows its working procedures.

Algorithm 1. Algorithm for trust evaluation through comprehensive procedure

INPUT: Cloud service user (CSU) directory, cloud service provider directory (CSP).
OUTPUT: Compute the trust level of the cloud service provider.
1: CSU submits the list of required resources with their QoS and Threshold value.

CSUi ← CSUi (id) AND CSUi (transaction history).
QoSi ← List of required QoS with their threshold level.
Qi ← CSUi (trust level).

2: Cloud broker (CB) finds the list of available service providers (CSPs) from the service provider directory as per CSUi and QoSi.

CSPj ← CSPj (ID) AND CSPj (status F/B)
QoSj ← List of offered QoS with their capacity level.

3: if (CSUi AND CSPj) interact in the past then
4: Go to Step 9.
5: else
6: Find the list of recommenders with their past transaction record.

7: Collect the feedback from all the historical users who have transactions with CSPj.
8: end if
9: Obtain direct interaction feedback with time intervals.
10: Assign a weight to direct trust (DT), recommender trust (RT) and reputation trust (RepT) using any weight assignment method. where:

$$\sum W_i = 1 \ (17)$$

11: Define trust evaluation procedure (graph theory, MCDM approach, AI & ML, etc.).
12: Evaluate direct trust (DT), recommender trust value (RT), reputation trust (RepT).
13: Comprehensive trust:

(CT) ← W1 ← DT + W2 ← RT + W3 RepT.

14: if (CTi >= Qi) then
15: Go to Step 20.
16: else
17: Discard CSPj, select another the CSP from CSPs directory.
18: Go to Step 3.
19: end if
20: Prepare a list of CSPs for a cloud service user (CSUi) with their QoSj.
21: Rank the CSPj using any ranked approach (AHP, TOPSIS, CRPA algorithm, etc.).
22: Select the highest ranking CSPj for CSUi.
23: Availed the cloud service from highest ranked CSP.
24: Submit the response using the dynamic update method.
25: Update the list of CSU and CSP in their directory.
26: Stop

Understanding the various techniques for managing trust is crucial to establishing trust. This section provides a comprehensive comparative description of various trust management techniques and QoS. To facilitate a better understanding, Tables 4–7 present brief yet informative descriptions of different research articles published between 2015 and 2023 based on trust strategies.

5.2 Comparative Analysis of Research Articles about to QoS

The SMI framework has a hierarchical QoS structure. It consists of the crucial characteristics in case of selecting a service in cloud environment. It may not

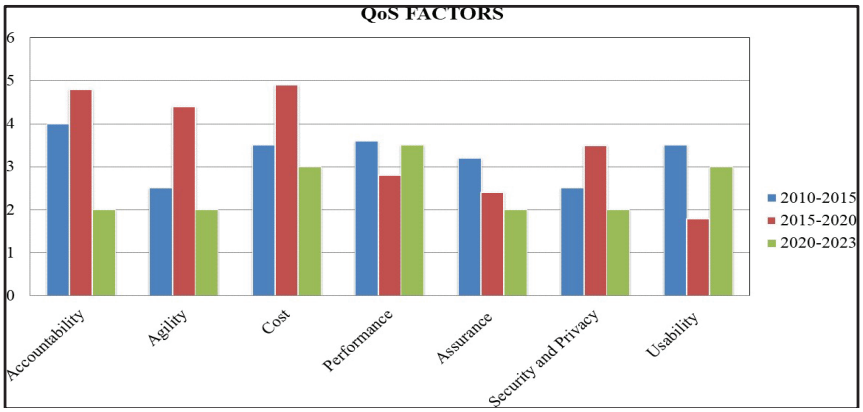

Figure 8 Analysis of various QoS factors according to various research articles during the year 2010–2023.

be feasible for any cloud service to include all the QoS criteria of the SMI for service selection. Figure 8 examines seven essential QoS elements of the SMI framework based on research publications published between 2010 and 2023. The research indicates that fewer papers address security, assurance, and usability. Table 3 highlights the research work of some of the articles with the details of QoS applied to trust management and cloud environments.

5.3 SLA Based Approach

An SLA is an essential contract between communicating entities that can protect from violation. It is an emerging method that is inadequate for new characteristics of cloud computing that are qualitative and can't be measured, like security, understandability, or sustainability. Table 4 provides an overview of different trust frameworks and their methods and data sources created using the SLA technique.

5.4 Recommendation Based Approach

It is a system where preferences are given based on the experiences or recommendations of previous users. Users must have access to recommendation algorithms to locate suitable cloud services. The recommendation-based trust model estimates trust levels using subjective trust. Table 5 briefly describes several recommendation-based trust models, their estimation approach, and their implementation tools.

Table 4 Service level agreement based trust management frameworks

Objective/Ref.	Advantage	Parameters	Year	Technique/Class of Method	Data Source
Fuzzy logic and ANN: trust model for grid and cloud [125]	Fuzzy logic is used to remove uncertainty. ANN is used for forecast trust value.	Reliability response time, fault tolerance, security.	2022	Fuzzy logic & ANN	Dataset of 2000 instances are collected from authenticated sources.
Smart contract and blockchain-based distributed SLA management [126]	Dynamic SLA framework through a smart contract. Specifies how supplied service level might vary over time.	Scalability, cost, flexibility, stability.	2021	Block chain architecture	Two clouds as test beds: AWS10 and ExoGENI11. For each six data centers and three VM types.
Smart contract-based game-theory paradigm for enforcing trustworthy cloud SLA using witnesses. [127]	Witness approach with smart contracts. Witness is rewarded/punished	Four stages of a smart contract are considered: busy, free, confirm, release.	2021	Game theory's Nash equilibrium principle. An unbiased algorithm is used to avoid a collision. For controlling malicious witness auditing mechanism is used.	Ethernum blockchain, "Rinkeby".
Cloud service provider evaluation and selection system based on the streamlined PROMETHEE- II criteria. [128]	For performing the SLO violation.	Cost, reliability, efficiency.	2022	PROMETHEE-II method is used for centralized QoE and QoS.	Case study.
A framework for ensuring cloud service security conformity based on behavior-aware SLAs. [129]	Weight assigned to CSPs using the PROMETHEE-2 method.	Reliability, stability, throughput, availability, security	2020	UPPAAL tool to check performance and security	Case study along with experiment with real cloud service based on the open stack.
Ant Lion optimization algorithm-based SLA-based autonomous cloud resource management framework. [108]	Integration of security constraints with service behavior.	Cost, throughput, availability, SLA violation	2019	Ant Lion optimization algorithm.	Cloud Sim

Table 5 Recommendation based trust management frameworks

Objective/Ref.	Year	Descriptions	Technique/Class of Method	Data Source
Trust-based federated learning strategy to combat cold start issue in recommendation systems: Federated against cold. [130]	2022	Federated learning is used for recommendation system.	Collaborative-filtering approach through ML	Simulations on Movie Lens 1M and Epinions dataset.
Innovative method has been developed to address cold start issue in recommender systems. [131]	2020	Trust score estimated by double deep Q learning scheduling approach.	Machine learning, classification, tree+, random forecast	From social sites.
An item rating-based fidelity homogenous genesis recommendation model.[132]	2022	Social media data used to develop a behavioral profile to categorize people.	Utilizing an autonomous map approach for clustering.	Simulation.
Building trust in a collaborative filtering recommendation system via Blockchain technology.[133]	2021	Machine learning methods for trust estimation.	User-item privacy marmalade technique is used to determine recommender's credibility.	Simulation.
DDTMS stands for Dirichlet-distribution-based trust management system used in the IoT.[134]	2019	Problem of sparse data is tackled by combination of comparable previous case reasoning approach and average filling.	Blockchain.	Simulation.
A methodology for assessing reliability of cloud services using weights and grey correlation analysis [135]	2019	An algorithm for decentralized recommendation systems that relies on collaborative filtering and decentralized matrix completion form.	Binomial distribution and probability distribution	Simulation.

5.5 Reputation/Feedback-based Approach Model

Reputation and feedback are used to build trust. This methodology gathers user comments and opinions based on QoS and security to quantify cloud provider trust. Table 6 briefly describes several feedback-based trust models, their estimation approach, and their data sources with their descriptions.

5.6 Comprehensive Approach-based Model

To gain trust and credibility in a cloud environment, it is essential to thoroughly examine the functional along with the non-functional aspects of cloud-based trust models. It is important to note that no single trust mechanism can provide us with a secure and a reliable trust model. The solution to this challenge is to adopt a hybrid approach, which involves a comprehensive trust model. By leveraging comprehensive trust models, cloud users can make informed decisions and select a cloud service that is both secure and efficient. To help illustrate this point, Table 7 summarizes various comprehensive trust models, along with their estimation methodology and implementation mechanism.

5.7 Summary of Research Work Done in Trust Management Model in 2016–2023 Using a Scopus Indexed Database

Extensive research has been conducted on the Scopus database to determine the publication rate regarding trust management in cloud computing. A sophisticated search query was created by combining the Boolean OR and AND operators with a primary pilot. As a result, three key terms, namely, "trust management," "cloud computing," and "trust strategies," were selected. These key terms cover most of the research efforts invested in SLA, recommendation, and feedback-based trust mechanisms. Further research is necessary to develop comprehensive trust strategies for selecting cloud services. The publication summary of these trust strategies has been summarized in Figure 9. However, comprehensive trust management techniques seem to be the more explored area. From the above data, we concluded that four major factors for trust management evaluation are considered, which are:

- *SLA*: A service level agreement is an agreement between customer and service provider. From the present data, we can analyze that an SLA was a popular choice until 2019, but the preference for this technique has declined over the years.

Table 6 Feedback-based trust management frameworks

Objective/Ref.	Year	Descriptions	Technique/Class of Method	Data Source
Interoperable fog computing trust management system. [136]	2020	Developed system work on provider perspective and consider both QoS and reputation for trust estimation.	Collaborative-filtering approach through ML	Java
An effective fog computing to trust management via use of feedback credibility evaluation. [137]	2022	Checker-based feedback assessment approach for identifying unauthorized users.	Machine learning, classification, tree+, random forecast	Simulation
Improving the quality of service model for evaluating trust in cloud setting. [6]	2020	Accumulated trust value updated after each transaction and calculated by reputation history of provider.	Utilizing an autonomous map approach for clustering.	Cloud Sim Eclipse
Objective logic trust for federated peer-to-peer clouds in smart cities: Trusty Feer. [138]	2018	Service registry, reputation database management, trust calculator. Trust value is computed by multiplying the total of all metric values by a specified weight.	User-item privacy marmalade technique is used to determine the recommender's credibility.	Java
Cloud-based trust management based on a third party's reputation. [139]	2017	Use ID to check credibility of feedback provider.	Blockchain.	Simulation
Message passing perspective on user trust inference in online social networks. [140]	2022	Developed a graphical probabilistic model for online trust inference.	Binomial distribution and probability distribution.	Online social network

Table 7 Comprehensive based trust management frameworks

Objective/Ref.	Year	Descriptions	Technique/Class of Method	Data Source
Working towards trust assessment framework to counteract IIoT malfunctions. [141]	2022	Malicious behavior of node and heterogeneous features of edge network.	Bayesian framework and semi ring theory.	Simulation
A model for trust management in the cloud based on fuzzy rules. [58]	2021	Work in multi-cloud that use both subjective and objective parameters to evaluate trust value.	Fuzzy theory and belief theory.	Simulation Dataset from Epinion
Interval neutrosophic number-based computational trust models for social IoT [97]	2022	To handle uncertainty related to TM interval neutrosophic numbers used.	Neutrosophic sets.	Simulation
A reliable system for assessing reliability of secure service providers in fog computing. [90]	2022	Considered full set of secure service selection criteria. Findings show QoS affects secure service selection by 0.470.	Fuzzy inference system and best worst method	Simulation
Method for evaluating and initially ranking cloud services based on user preferences. [142]	2020	CPRA ranks cloud services based on customer preferences before any transaction takes place.	Aggregation operator.	Dataset: Amazon EC2, Windows Azure, Rackspace, OpenStack and Eucalyptus
An algorithmic structure for cloud service ranking prediction in a fuzzy setting. [117]	2021	Weight calculation of QoS through fuzzy AHP theory. Ranking by TOPSIS.	MCDM approach: Fuzzy AHP and TOPSIS.	Dataset: Amazon EC2, Windows Azure, Rackspace, OpenStack and Eucalyptus

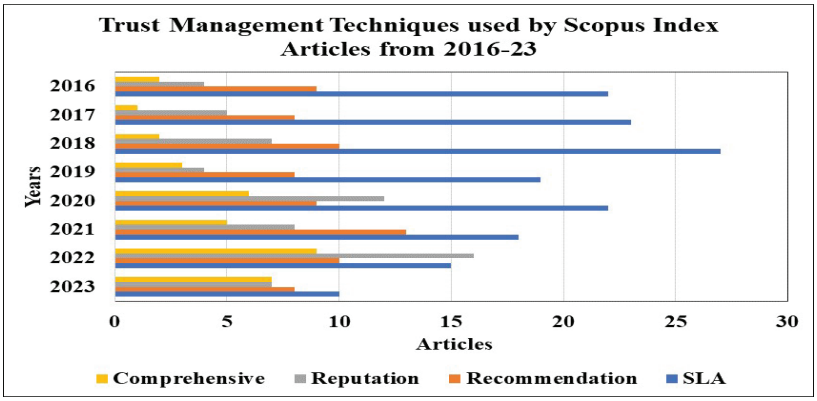

Figure 9 The rate of articles indexed using the Scopus database (2016–2023) for trust management using different trust strategies.

- *Recommendation*: This is a system where preferences are given based on previous users' experiences or recommendations. From the present data, we can see that recommendations have increased in popularity among users since 2019.
- *Reputation*: Ranking of services is determined based on users' evaluations of various tasks. According to current data, reputation has gained popularity among users since 2019.
- *Comprehensive*: This technique often includes all of the elements necessary for an accurate rating. The current stats reveal that reputation has been widespread among users since 2020. This method is preferred as it provides a more accurate and precise selection."

6 Conclusion

Cloud services play a critical role in modern computer systems, and their efficiency depends heavily on the quality of cloud services they utilize. It is, therefore, imperative to carefully choose the appropriate cloud services that meet end-user's requirements and expectations. To make an informed decision, it is necessary to conduct a thorough analysis of various cloud services as per the customer's needs and preferences. This evaluates different trust management techniques, highlighting their key features, advantages, and limitations. Examining the empirical relationship between QoS, trust mechanisms and cloud services is a complex and challenging operation. However, it introduced a trust mechanism where different QoS parameters are considered.

This work provides a dynamic trust mechanism and supported cloud service adoption considering user satisfaction and experience. The report discusses the criteria for selecting cloud services. It proposes additional SMI elements to improve the accuracy of evaluating and rating web and cloud computing services like space management, payment interface, and financial stability. A precise algorithm helps consumers to select a service. Fuzzy logic with interval and qualitative performance data may be employed to build a trust model for future assessment and ranking techniques. The grey theory also rates cloud services based on functional and non-functional KPIs for a better choice making about cloud services.

References

[1] S. Pearson, "Privacy, security and trust in cloud computing," in Privacy and security for cloud computing, Springer, 2013, pp. 3–42.

[2] M. Shameem, R. R. Kumar, C. Kumar, B. Chandra, and A. A. Khan, "Prioritizing challenges of agile process in distributed software development environment using analytic hierarchy process," J. Softw. Evol. Process, vol. 30, no. 11, p. e1979, 2018.

[3] M. Chiregi and N. J. Navimipour, "Cloud computing and trust evaluation: A systematic literature review of the state-of-the-art mechanisms," J. Electr. Syst. Inf. Technol., vol. 5, no. 3, pp. 608–622, 2018.

[4] H. Hassan, A. I. El-Desouky, A. Ibrahim, E.-S. M. El-Kenawy, and R. Arnous, "Enhanced QoS-based model for trust assessment in cloud computing environment," IEEE Access, vol. 8, pp. 43752–43763, 2020.

[5] S. Soltani, M. Asadi, D. Gas¡evic´, M. Hatala, and E. Bagheri, "Automated planning for feature model configu- ration based on functional and non-functional requirements," in Proceedings of the 16th International Software Product Line Conference-Volume 1, 2012, pp. 56–65.

[6] S. K. Garg, S. Versteeg, and R. Buyya, "Smicloud: A framework for comparing and ranking cloud services," in 2011 Fourth IEEE International Conference on Utility and Cloud Computing, 2011, pp. 210–218.

[7] Z. Raghebi and M. R. Hashemi, "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), 2013, pp. 1–6.

[8] R. R. Kumar, S. Mishra, and C. Kumar, "A novel framework for cloud service evaluation and selection using hybrid MCDM methods," Arab. J. Sci. Eng., vol. 43, no. 12, pp. 7015–7030, 2018.

[9] A. Tripathi, I. Pathak, and D. P. Vidyarthi, "Integration of analytic network process with service measurement index framework for cloud service provider selection," Concurr. Comput. Pract. Exp., vol. 29, no. 12, p. e4144, 2017.

[10] S. K. Garg, S. Versteeg, and R. Buyya, "A framework for ranking of cloud computing services," Futur. Gener. Comput. Syst., vol. 29, no. 4, pp. 1012–1023, 2013.

[11] R. K. Tiwari and R. Kumar, "A robust and efficient MCDM-based framework for cloud service selection using modified TOPSIS," Int. J. Cloud Appl. Comput., vol. 11, no. 1, pp. 21–51, 2021.

[12] C. Qu and R. Buyya, "A cloud trust evaluation system using hierarchical fuzzy inference system for service se- lection," in 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, 2014, pp. 850–857.

[13] R. K. L. Ko et al., "TrustCloud: A framework for accountability and trust in cloud computing," in 2011 IEEE World Congress on Services, 2011, pp. 584–588.

[14] J. Huang and D. M. Nicol, "Trust mechanisms for cloud computing," J. Cloud Comput. Adv. Syst. Appl., vol. 2, no. 1, pp. 1–14, 2013.

[15] A. Sarwar and M. N. Khan, "A review of trust aspects in cloud computing security," Int. J. Cloud Comput. Serv. Sci., vol. 2, no. 2, p. 116, 2013.

[16] A. Ezenwoke, O. Daramola, and M. Adigun, "QoS-based ranking and selection of SaaS applications using heterogeneous similarity metrics," J. Cloud Comput., vol. 7, no. 1, pp. 1–12, 2018.

[17] M. Almorsy, J. Grundy, and I. Mu¨ller, "An analysis of the cloud computing security problem," arXiv Prepr. arXiv1609.01107, 2016.

[18] P. Srivastava and R. Khan, "A Review Paper on Cloud Computing," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 8, no. 6, p. 17, 2018, doi: 10.23956/ijarcsse.v8i6.711.

[19] A. Tyagi, "A review paper on cloud computing," Int. J. Eng. Res. & Technol. ISSN, pp. 181–2278, 2017.

[20] A. Rashid and A. Chaturvedi, "Cloud computing characteristics and services: a brief review," Int. J. Comput. Sci. Eng., vol. 7, no. 2, pp. 421–426, 2019.
[21] T. H. Noor, Q. Z. Sheng, Z. Maamar, and S. Zeadally, "Managing trust in the cloud: State of the art and research challenges," Computer (Long. Beach. Calif)., vol. 49, no. 2, pp. 34–45, 2016.
[22] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, "Trust management of services in cloud environments: Obstacles and solutions," ACM Comput. Surv., vol. 46, no. 1, pp. 1–30, 2013.
[23] W. Kim, "Cloud computing: Today and tomorrow.," J. Object Technol., vol. 8, no. 1, pp. 65–72, 2009.
[24] I. M. Khalil, A. Khreishah, and M. Azeem, "Cloud computing security: A survey," Computers, vol. 3, no. 1, pp. 1–35, 2014.
[25] M. K. Muchahari and S. K. Sinha, "A new trust management architecture for cloud computing environment," in 2012 International Symposium on Cloud and Services Computing, 2012, pp. 136–140.
[26] H. P. Borges, J. N. de Souza, J. N. de Souza, B. Schulze, and A. R. Mury, "A process for clouds services procurement based on model and qos," in 2012 IEEE Latin America Conference on Cloud Computing and Communications (LatinCloud), 2012, pp. 37–42.
[27] 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.
[28] R. L. Winkler, J. L. Butler, K. J. Curtis, and D. Egan-Robertson, "Differential privacy and the accuracy of county-level net migration estimates," Popul. Res. Policy Rev., vol. 41, no. 2, pp. 417–435, 2022.
[29] 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.
[30] X. Wu, R. Zhang, B. Zeng, and S. Zhou, "A trust evaluation model for cloud computing," Procedia Comput. Sci., vol. 17, pp. 1170–1177, 2013.
[31] P. Varalakshmi, T. Judgi, and D. Balaji, "Trust management model based on malicious filtered feedback in cloud," in International Conference on Data Science Analytics and Applications, 2017, pp. 178–187.
[32] J. Capachin, "Change on the horizon: The impact of cloud computing on treasury and transaction banking," J. Payments Strateg. & Syst., vol. 4, no. 4, pp. 334–344, 2010.

[33] J. Sidhu and S. Singh, "A novel cloud auditor based trust management framework for cloud computing," Int. J. Grid Util. Comput., vol. 7, no. 3, pp. 219–235, 2016.
[34] M. Chiregi and N. J. Navimipour, "A comprehensive study of the trust evaluation mechanisms in the cloud computing," J. Serv. Sci. Res., vol. 9, no. 1, pp. 1–30, 2017.
[35] S. T. Alshammari, A. Albeshri, and K. Alsubhi, "Building a trust model system to avoid cloud services reputation attacks," Egypt. Informatics J., vol. 22, no. 4, pp. 493–503, 2021.
[36] P. Sun, "Security and privacy protection in cloud computing: Discussions and challenges," J. Netw. Comput. Appl., vol. 160, p. 102642, 2020.
[37] G. Aghaee Ghazvini, M. Mohsenzadeh, R. Nasiri, and A. M. Rahmani, "A new multi-level trust manage- ment framework (MLTM) for solving the invalidity and sparse problems of user feedback ratings in cloud environments," J. Supercomput., vol. 77, no. 3, pp. 2326–2354, 2021.
[38] E. Cayirci and A. S. De Oliveira, "Modelling trust and risk for cloud services," J. Cloud Comput., vol. 7, no. 1, pp. 1–16, 2018.
[39] V. R. Thakare, "Computational trust evaluation algorithm for cloud models using fuzzy logic approach," Int. J. Ad Hoc Ubiquitous Comput., vol. 38, no. 1–3, pp. 127–140, 2021.
[40] S. M. Habib, S. Hauke, S. Ries, and M. Mu¨hlha¨user, "Trust as a facilitator in cloud computing: a survey," J. Cloud Comput. Adv. Syst. Appl., vol. 1, no. 1, pp. 1–18, 2012.
[41] S. S. Deora and others, "A Review: Trust Management Techniques Used for Cloud Computing," Proc. Data Anal. Manag., pp. 117–132, 2022.
[42] A. K. Jaithunbi, S. Sabena, and L. SaiRamesh, "Trust evaluation of public cloud service providers using genetic algorithm with intelligent rules," Wirel. Pers. Commun., vol. 121, no. 4, pp. 3281–3295, 2021.
[43] P. Goyal and S. S. Deora, "Reliability of Trust Management Systems in Cloud Computing".
[44] M. Alazab, G. Manogaran, and C. E. Montenegro-Marin, "Trust management for internet of things using cloud computing and security in smart cities," Cluster Comput., vol. 25, no. 3, pp. 1765–1777, 2022.
[45] S.-K. Chong, J. Abawajy, M. Ahmad, and I. R. A. Hamid, "Enhancing trust management in cloud environment," Procedia-Social Behav. Sci., vol. 129, pp. 314–321, 2014.
[46] D. H. McKnight and N. L. Chervany, "The meanings of trust," 1996.

[47] D. Catteddu, "Cloud Computing: benefits, risks and recommendations for information security," in Iberic Web Application Security Conference, 2009, p. 17.
[48] M. Armbrust et al., "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.
[49] K. Hwang, S. Kulkareni, and Y. Hu, "Cloud security with virtualized defense and reputation-based trust mange- ment," in 2009 Eighth IEEE international conference on dependable, autonomic and secure computing, 2009, pp. 717–722.
[50] G. Garrison, S. Kim, and R. L. Wakefield, "Success factors for deploying cloud computing," Commun. ACM, vol. 55, no. 9, pp. 62–68, 2012.
[51] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, 2010.
[52] M. Soleymani, N. Abapour, E. Taghizadeh, S. Siadat, and R. Karkehabadi, "Fuzzy Rule-Based Trust Management Model for the Security of Cloud Computing," Math. Probl. Eng., vol. 2021, 2021.
[53] M. Nikravan and M. H. Kashani, "A review on trust management in fog/edge computing: Techniques, trends, and challenges," J. Netw. Comput. Appl., p. 103402, 2022.
[54] N. El Ioini, H. R. Barzegar, C. Pahl, and others, "Trust management for service migration in multi-access edge computing environments," Comput. Commun., 2022.
[55] D. Gambetta and others, "Can we trust trust," Trust Mak. Break. Coop. relations, vol. 13, no. 1, pp. 213–237, 2000.
[56] S. Ries, "Extending bayesian trust models regarding context-dependence and user friendly representation," in Proceedings of the 2009 ACM symposium on Applied Computing, 2009, pp. 1294–1301.
[57] S. M. Habib, S. Ries, and M. Muhlhauser, "Cloud computing landscape and research challenges regarding trust and reputation," in 2010 7th International conference on ubiquitous intelligence & computing and 7th international conference on autonomic & trusted computing, 2010, pp. 410–415.
[58] 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.

[59] Liu, Yijia, et al. "A survey on blockchain-based trust management for Internet of Things." IEEE internet of Things Journal 10.7 2023, pp. 5898–5922.

[60] Huber, Brennan, and Farah Kandah. "DECAY: Dynamic Evaluation and Component Analysis for Enhancing Trust Management." In 2024 IEEE International Conference on Consumer Electronics (ICCE), pp. 1-6. IEEE, 2024.

[61] Fotia, Lidia, Fla´via Delicato, and Giancarlo Fortino. "Trust in edge-based internet of things architectures: state of the art and research challenges." ACM Computing Surveys 55.9 (2023), pp. 1–34.

[62] Zeng, H., Dhiman, G., Sharma, A., Sharma, A. Tselykh, A. (2023). An IoT and Blockchain-based approach for the smart water management system in agriculture. Expert Systems, 40(4), e12892.

[63] Shirvani, Mirsaeid Hosseini, and Mohammad Masdari. "A survey study on trust-based security in Internet of Things: Challenges and issues." Internet of Things 21 (2023): 100640.

[64] Joshua, Salaki Reynaldo, et al. "Trust components: An analysis in the development of type 2 diabetic mellitus mobile application." Applied Sciences 13.3 (2023), pp. 1251.

[65] M. Hosseinnezhad, M. A. Azgomi, and M. R. E. Dishabi, "A Probabilistic Trust Model for Cloud Services Using Bayesian Networks," 2021.

[66] A. S. Ali and O. F. Rana, "A belief-based trust model for dynamic service selection," in Economic models and algorithms for distributed systems, Springer, 2009, pp. 9–23.

[67] S. Pal, A. Hill, T. Rabehaja, and M. Hitchens, "A blockchain-based trust management framework with verifiable interactions," Comput. Networks, vol. 200, p. 108506, 2021.

[68] R. Nagarajan, S. Selvamuthukumaran, and R. Thirunavukarasu, "A fuzzy logic based trust evaluation model for the selection of cloud services," in 2017 International Conference on Computer Communication and Informatics (ICCCI), 2017, pp. 1–5.

[69] K. Chandran, V. Shanmugasudaram, and K. Subramani, "Designing a Fuzzy-Logic Based Trust and Reputation Model for Secure Resource Allocation in Cloud Computing.," Int. Arab J. Inf. Technol., vol. 13, no. 1, 2016.

[70] 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.

[71] N. Alhadad, Y. Busnel, P. Serrano-Alvarado, and P. Lamarre, "Graph-Based Trust Model for Evaluating Trust Using Subjective Logic," 2013.

[72] 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.

[73] G. Obulaporam, N. Somu, G. R. ManiIyer Ramani, A. K. Boopathy, and S. S. Vathula Sankaran, "GCRIT- ICPA: 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.

[74] Y. Kuo, T. Yang, and G.-W. Huang, "The use of a grey-based Taguchi method for optimizing multi-response simulation problems," Eng. Optim., vol. 40, no. 6, pp. 517–528, 2008.

[75] I. Benjamin Franklin, M. Paul Arokiadass Jerald, and R. Bhuvaneswari, "Machine Learning-Based Trust Management in Cloud Using Blockchain Technology," SN Comput. Sci., vol. 3, no. 6, pp. 1–11, 2022.

[76] U. Jayasinghe, G. M. Lee, T.-W. Um, and Q. Shi, "Machine learning based trust computational model for IoT services," IEEE Trans. Sustain. Comput., vol. 4, no. 1, pp. 39–52, 2018.

[77] S. S. Sefati and S. Halunga, "A Hybrid Service Selection and Composition for Cloud Computing Using the Adaptive Penalty Function in Genetic and Artificial Bee Colony Algorithm," Sensors, vol. 22, no. 13, p. 4873, 2022.

[78] 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.

[79] L. Huang, Z. Xiong, and G. Wang, "Evaluating Mechanism Trust Model Based on Behavior Result under Cloud Computing.," Int. J. Simulation–Systems, Sci. & Technol., vol. 17, no. 30, 2016.

[80] X. Li and J. Du, "Adaptive and attribute-based trust model for service-level agreement guarantee in cloud computing," IET Inf. Secur., vol. 7, no. 1, pp. 39–50, 2013.

[81] J. Araujo, P. Maciel, E. Andrade, G. Callou, V. Alves, and P. Cunha, "Decision making in cloud environments: an approach based on

multiple-criteria decision analysis and stochastic models," J. Cloud Comput., vol. 7, no. 1, pp. 1–19, 2018.

[82] F. Nawaz, M. R. Asadabadi, N. K. Janjua, O. K. Hussain, E. Chang, and M. Saberi, "An MCDM method for cloud service selection using a Markov chain and the best-worst method," Knowledge-Based Syst., vol. 159, pp. 120–131, 2018.

[83] J. Sidhu and S. Singh, "Design and comparative analysis of MCDM-based multi-dimensional trust evaluation schemes for determining trustworthiness of cloud service providers," J. Grid Comput., vol. 15, no. 2, pp. 197–218, 2017.

[84] C.-W. Hang and M. P. Singh, "Trustworthy service selection and composition," ACM Trans. Auton. Adapt. Syst., vol. 6, no. 1, pp. 1–17, 2011.

[85] E. Zupancic and D. Trcek, "QADE: a novel trust and reputation model for handling false trust values in e-commerce environments with subjectivity consideration," Technol. Econ. Dev. Econ., vol. 23, no. 1, pp. 81–110, 2017.

[86] J. Luna Garcia, R. Langenberg, and N. Suri, "Benchmarking cloud security level agreements using quantitative policy trees," in Proceedings of the 2012 ACM Workshop on Cloud computing security workshop, 2012, pp. 103–112.

[87] M. Tavakolifard, S. J. Knapskog, and P. Herrmann, "Trust transferability among similar contexts," in Pro- ceedings of the 4th ACM symposium on QoS and security for wireless and mobile networks, 2008, pp. 91–97.

[88] A. W. Coviello, H. D. Elias, P. Gelsinger, and R. McAniff, "Proof, not promises: creating the trusted cloud," in ISSE 2011 Securing Electronic Business Processes, Springer, 2012, pp. 9–20.

[89] S. N. V Schweizerische, "Information technology-Security techniques-Information security management systems-Requirements," ISO/IEC Int. Stand. Organ., 2013.

[90] M. Afzali, H. Pourmohammadi, and A. Mohammad Vali Samani, "An efficient framework for trust evaluation of secure service selection in fog computing based on QoS, reputation, and social criteria," Computing, pp. 1–33, 2022.

[91] Y. Wang and J. Vassileva, "A review on trust and reputation for web service selection," in 27th international Conference on distributed computing systems workshops (ICDCSW'07), 2007, p. 25.

[92] L. Ertaul, S. Singhal, and G. Saldamli, "Security Challenges in Cloud Computing.," in Security and Management, 2010, pp. 36–42.
[93] M. D. H. Parekh and R. Sridaran, "An analysis of security challenges in cloud computing," Int. J. Adv. Comput. Sci. Appl., vol. 4, no. 1, 2013.
[94] A. Behl, "Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation," in 2011 World Congress on Information and Communication Technologies, 2011, pp. 217–222.
[95] X. Deng, J. Liu, L. Wang, and Z. Zhao, "A trust evaluation system based on reputation data in mobile edge computing network," Peer-to-Peer Netw. Appl., vol. 13, no. 5, pp. 1744–1755, 2020.
[96] N. Subramanian and A. Jeyaraj, "Recent security challenges in cloud computing," Comput. & Electr. Eng., vol. 71, pp. 28–42, 2018.
[97] S. Pourmohseni, M. Ashtiani, and A. A. Azirani, "A Computational Trust Model for Social IoT based on Interval Neutrosophic Numbers," Inf. Sci. (Ny)., 2022.
[98] M. B. Monir, M. H. AbdelAziz, A. A. AbdelHamid, and E.-S. M. EI-Horbaty, "Trust management in cloud com- puting: a survey," in 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS), 2015, pp. 231–242.
[99] M. Alhanahnah, P. Bertok, and Z. Tari, "Trusting cloud service providers: trust phases and a taxonomy of trust factors," IEEE cloud Comput., vol. 4, no. 1, pp. 44–54, 2017.
[100] R. Kumar and R. Goyal, "Performance based Risk driven Trust (PRTrust): On modeling of secured service sharing in peer-to-peer federated cloud," Comput. Commun., vol. 183, pp. 136–160, 2022.
[101] A. Mousa, J. Bentahar, and O. Alam, "Multi-dimensional trust for context-aware services computing," Expert Syst. Appl., vol. 172, p. 114592, 2021.
[102] B. K. Ray, A. Saha, S. Khatua, and S. Roy, "Quality and profit assured trusted cloud federation formation: Game theory based approach," IEEE Trans. Serv. Comput., vol. 14, no. 3, pp. 805–819, 2018.
[103] O. K. Hussain, F. K. Hussain, and others, "Parallel cloud service selection and ranking based on QoS history," Int. J. Parallel Program., vol. 42, no. 5, pp. 820–852, 2014.
[104] S. Lee and K.-K. Seo, "A hybrid multi-criteria decision-making model for a cloud service selection problem using BSC, fuzzy Delphi method

and fuzzy AHP," Wirel. Pers. Commun., vol. 86, no. 1, pp. 57–75, 2016.

[105] R. Srishylam and M. Umar, "Cloud Armor: A Trusty Supporting Reputation-based Management for Cloud Services," CVR J. Sci. Technol., vol. 12, pp. 104–107, 2017.

[106] S. N. Manoharan and others, "Euclidean Distance Based Similarity Measurement and Ensuing Ranking Scheme for Document Search from Outsourced Cloud Data," Turkish J. Comput. Math. Educ., vol. 12, no. 3, pp. 4386–4395, 2021.

[107] C. Jatoth, G. R. Gangadharan, U. Fiore, and R. Buyya, "SELCLOUD: a hybrid multi-criteria decision-making model for selection of cloud services," Soft Comput., vol. 23, no. 13, pp. 4701–4715, 2019.

[108] B. K. Dewangan, A. Agarwal, M. Venkatadri, and A. Pasricha, "Sla-based autonomic cloud resource manage- ment framework by antlion optimization algorithm," Int. J. Innov. Technol. Explor. Eng.(IJITEE), vol. 8, pp. 119–123, 2019.

[109] A. Selvaraj and S. Sundararajan, "Evidence-based trust evaluation system for cloud services using fuzzy logic," Int. J. Fuzzy Syst., vol. 19, no. 2, pp. 329–337, 2017.

[110] Y. Lu, X. Zheng, L. Li, and L. D. Xu, "Pricing the cloud: a QoS-based auction approach," Enterp. Inf. Syst., vol. 14, no. 3, pp. 334–351, 2020.

[111] N. Yadav and M. S. Goraya, "Two-way ranking based service mapping in cloud environment," Futur. Gener. Comput. Syst., vol. 81, pp. 53–66, 2018.

[112] M. Saleem, M. R. Warsi, S. Islam, A. Anjum, and N. Siddiquii, "Trust Management in the World of Cloud Computing. Past Trends and Some New Directions," Scalable Comput. Pract. Exp., vol. 22, no. 4, pp. 425–444, 2021.

[113] 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.

[114] R. Chalse, A. Selokar, and A. Katara, "A new technique of data integrity for analysis of the cloud computing security," in 2013 5th International Conference and Computational Intelligence and Communication Networks, 2013, pp. 469–473.

[115] L. Sun, J. Ma, Y. Zhang, H. Dong, and F. K. Hussain, "Cloud-FuSeR: Fuzzy ontology and MCDM based cloud service selection," Futur. Gener. Comput. Syst., vol. 57, pp. 42–55, 2016.

[116] J. Sidhu and S. Singh, "Improved topsis method based trust evaluation framework for determining trustwor- thiness of cloud service providers," J. Grid Comput., vol. 15, no. 1, pp. 81–105, 2017.
[117] R. R. Kumar, M. Shameem, and C. Kumar, "A computational framework for ranking prediction of cloud services under fuzzy environment," Enterp. Inf. Syst., vol. 16, no. 1, pp. 167–187, 2022.
[118] 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.
[119] P. Sun, "Research on cloud computing service based on trust access control," Int. J. Eng. Bus. Manag., vol. 12, p. 1847979019897444, 2020.
[120] S. Machhi 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, 2016, pp. 1–5.
[121] M. Chiregi and N. J. Navimipour, "A new method for trust and reputation evaluation in the cloud environments using the recommendations of opinion leaders' entities and removing the effect of troll entities," Comput. Human Behav., vol. 60, pp. 280–292, 2016.
[122] R. Nagarajan, R. Thirunavukarasu, and S. Shanmugam, "A fuzzy-based intelligent cloud broker with MapRe- duce framework to evaluate the trust level of cloud services using customer feedback," Int. J. Fuzzy Syst., vol. 20, no. 1, pp. 339–347, 2018.
[123] 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.
[124] X. Li, C. Yin, and F. Liu, "A trust estimation method of machine tool resources in the cloud environment," J. Stat. Comput. Simul., vol. 87, no. 13, pp. 2572–2580, 2017.
[125] G. M. Kumar, S. Ramachandram, and J. Gyani, "Trust model for cloud and grid environment using fuzzy logic and artificial neural network".
[126] R. B. Uriarte, H. Zhou, K. Kritikos, Z. Shi, Z. Zhao, and R. De Nicola, "Distributed service-level agreement management with smart contracts and blockchain," Concurr. Comput. Pract. Exp., vol. 33, no. 14, p. e5800, 2021.
[127] H. Zhou, X. Ouyang, J. Su, C. de Laat, and Z. Zhao, "Enforcing trustworthy cloud sla with witnesses: A game theory–based model

using smart contracts," Concurr. Comput. Pract. Exp., vol. 33, no. 14, p. e5511, 2021.

[128] W. Hussain and J. M. Merigo´, "Centralised quality of experience and service framework using PROMETHEE- II for cloud provider selection," in Intelligent processing practices and tools for e-commerce data, information, and knowledge, Springer, 2022, pp. 79–94.

[129] X. Liu, C. Xia, T. Wang, L. Zhong, and X. Li, "A behavior-aware SLA-based framework for guaranteeing the security conformance of cloud service," Front. Comput. Sci., vol. 14, no. 6, pp. 1–17, 2020.

[130] O. A. Wahab, G. Rjoub, J. Bentahar, and R. Cohen, "Federated against the cold: A trust-based federated learning approach to counter the cold start problem in recommendation systems," Inf. Sci. (Ny)., vol. 601, pp. 189–206, 2022.

[131] J. Herce-Zelaya, C. Porcel, J. Bernabe´-Moreno, A. Tejeda-Lorente, and E. Herrera-Viedma, "New technique to alleviate the cold start problem in recommender systems using information from social media and random decision forests," Inf. Sci. (Ny)., vol. 536, pp. 156–170, 2020.

[132] I. E. Albert, A. J. Deepa, and A. L. Fred, "Fidelity Homogenous Genesis Recommendation Model for User Trust with Item Ratings," Comput. J., 2022.

[133] Y. Himeur et al., "Blockchain-based recommender systems: Applications, challenges and future opportuni- ties," Comput. Sci. Rev., vol. 43, p. 100439, 2022.

[134] W. Fang, W. Zhang, L. Shan, X. Ji, and G. Jia, "DDTMS: Dirichlet-distribution-based trust management scheme in Internet of Things," Electronics, vol. 8, no. 7, p. 744, 2019.

[135] 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.

[136] E. Alemneh, S.-M. Senouci, P. Brunet, and T. Tegegne, "A two-way trust management system for fog computing," Futur. Gener. Comput. Syst., vol. 106, pp. 206–220, 2020.

[137] R. Yadav and G. Baranwal, "An Efficient Trust Management using Feedback Credibility Evaluation Method in Fog Computing," Simul. Model. Pract. Theory, vol. 120, p. 102610, 2022.

[138] H. Kurdi, B. Alshayban, L. Altoaimy, and S. Alsalamah, "TrustyFeer: A subjective logic trust model for smart city peer-to-peer federated clouds," Wirel. Commun. Mob. Comput., vol. 2018, 2018.

[139] D. K. Aarthy, M. Aarthi, K. A. Farhath, S. Lakshana, and V. Lavanya, "Reputation-based trust management in cloud using a trusted third party," in 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM), 2017, pp. 220–225.
[140] Y. Liu and B. Wang, "User Trust Inference in Online Social Networks: A Message Passing Perspective," Appl. Sci., vol. 12, no. 10, p. 5186, 2022.
[141] J. Wang, M. Wang, Z. Zhang, and H. Zhu, "Towards A Trust Evaluation Framework against Malicious Behaviors of Industrial IoT," IEEE Internet Things J., 2022.
[142] A. Qadir Md and V. Vijayakumar, "Combined preference ranking algorithm for comparing and initial ranking of cloud services," Recent Adv. Electr. & Electron. Eng. (Formerly Recent Patents Electr. & Electron. Eng., vol. 13, no. 2, pp. 260–275, 2020.

Biographies

Pooja Goyal. She is received a BCA degree in Computer Science from Maharshi Dayanand University, Rohtak in 2009, an MCA degree in 2012 and M.Tech in Computer Science and Engineering from the Maharshi Dayanand University, Rohtak in 2017, UGC(Net) in Computer Science in 2017 and pursuing PhD from Maharshi Dayanand University under the guidance of Dr. Sukhvinder Singh Deora.

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). Some short vitae can be included here.