Trust Establishment and Estimation in Cloud Services: A Systematic Literature Review

Kanwal Mahmud[a, b], Muhammad Usman[a, *]

[a]Department of Computer Sciences, Faculty of Natural Sciences, Quaid-I-Azam University, Islamabad, Pakistan

[b]Department of Computer Sciences & Information Technology, University of Poonch, Rawalakot, AJK, Pakistan

*corresponding author email: musman@qau.edu.pk

Abstract

Cloud computing has increasingly attracted a large number of entrepreneurs to deploy innovative web services to expand the horizon of their businesses. The selection of trustworthy services, by considering the adequate QoS parameters, is imperative for the cloud service consumers to fulfill their requirements. Over the years, many studies have been carried out to establish trust between service providers and cloud service consumers. The findings of these studies need to be analyzed in order to explore the essential features and limitations with respect to the essential QoS requirements. Therefore, a systematic literature review has been performed in this study with an aim to identify and classify the existing research on trust establishment and estimation in cloud services. A critical review of the existing literature has been presented along with the identification of potential future research avenues. This study has also highlighted the need of improving the service selection process by employing user preferences based on their particular application domains in the context of utility.

Keywords

Cloud Computing

Cloud Services

Quality of Service (QoS)

Trust Establishment

Trust Estimation

1. Introduction

The recent technological advancements have realized the widespread adoption of cloud computing technology in a number of industries such as entertainment, healthcare, education, e-government, and e-learning to gain functional efficiency and monetary benefits. The service selection decision typically depends on the satisfaction of promised Quality of Service (QoS). The optimum selection of a service (or a set of services) is a challenging task for cloud users (Mehndi *et al*., 2016; Qu *et al*., 2015; Ghosh *et al*., 2015; Jula *et al*., 2014; Singh *et al*., 2016; Sidhu & Singh, 2017; Lu & Yuan, 2018). The pool of services has numerous services with divergent QoS attributes which are provided by multiple service providers. The selection of a service, based on consumer preferences, has emerged as a key research domain (Jula *et al*., 2014; Sun *et al*., 2013; Garg *et al*., 2011).

The service selection process typically relies on security, privacy, and trust values (Sun *et al*., 2011; Dorey *et al*., 2011; Anakath *et al*., 2017). Rezaei *et al*. (2014a) argued that the key barrier to Software as a Service (SaaS) selection in distributed cloud computing is interoperability, that is, the ability of users to connect with other users through heterogeneous cloud environments. The trust establishment between cloud computing entities, that is, service providers and cloud consumers, plays an essential part in cloud computing adoption. Hence, the notion of trust can be viewed as a confidence of a cloud user on cloud service. The trustworthiness of an entity or a service helps the cloud users to make decisions.

Over the years, a number of studies have addressed the cloud service selection problem. These studies are primarily focused on two directions of trust, namely, trust establishment (Ghosh *et al*., 2015; Ko *et al*., 2011; Mehandi *et al*., 2012; Shaikh & Sasikumar, 2015; Chakraborty & Roy, 2012,) and trust estimation (Sun *et al*., 2013; Zheng *et al*., 2013; Zheng *et al*., 2011; Noor *et al*., 2013; Machhi & Jethava, 2016; Lu & Yuan, 2018). These studies have employed statistical methods; multiple-criteria decision analysis techniques; algorithmic solutions; reputation-based trust approaches; and biological techniques for trust establishment in cloud services (Habib *et al*., 2014; Bedi *et al*., 2012; Divakarla & Chandrasekaran, 2016; Liu *et al*., 2012).

A systematic literature review has been performed in this study to critically review the research patterns of recent years. The service trust establishment and estimation techniques have been examined. The identification and classifications of divergent solutions, with their benefits and limitations, highlight the major contributions of this systematic literature review. Another objective of this study is to highlight the trust factors employed in different studies in the literature of cloud computing. This study has also identified a number of potential future research directions. It is imperative to mention that the sole focus of this study is on trust establishment and estimation techniques. The trust management through brokerage, recommendation, and other such aspects of trust have not been considered in this study.

The remaining part of the paper is structured as follows. Section 2 summarizes a brief introduction to

cloud services, deployment models, and cloud-based web services. The literature statistics analysis and research questions are discussed in Section 3. The trustworthiness techniques in cloud computing literature has been critically reviewed and analyzed in Section 4. Section 5 elucidates the future research directions. Section 6 sums up the key findings of this study.

2. Background

2.1 Cloud Computing

Before we review and classify the related literature, some fundamental aspects of cloud computing have been discussed in this section. Buyya *et al*. (2009) predicted the future computing model as fifth utility after water, gas, telephone, and electricity. The computing resources are now available as general utilities, which can be used by consumers by employing pay-per-use model (Chiregi *et al*., 2016). Vaquero *et al*. provided a comprehensive definition of cloud computing, based on 22 descriptions (Vaquero *et al*., 2009). The authors termed cloud as accessible, dynamically reconfigurable, and virtualized resource pool, which offers Service Level Agreement (SLA) guarantees. Fig. 1 illustrates the five fundamental characteristics of cloud computing, services layers, and deployment models on the basis of standard documents provided by National Institute of Standards and Technology (NIST) (Mell *et al*., 2011).

a) *On-demand self-service.* The users can request for service provisioning with pay-per-use pricing model without having human interaction.
b) *Broad network access.* The resources and services can be accessible over the internet and can be accessed from the heterogeneous thin (e.g., software and browsers) or thick (e.g., smartphones, notebooks, and PDAs) client platforms.
c) *Resource pooling.* Cloud computing supports multi-tenant model, where resources are dynamically allocated and reallocated depending on the consumer demands. The users typically remain unaware about the location of the service providers. This helps vendors to dynamically deliver different real or virtual resources.
d) *Rapid elasticity.* The users are able to rapidly increase or decrease the usage of provided resources (e.g., computing, storage, and bandwidth) according to their need.
e) *Measured services.* The cloud-based systems automatically regulate, monitor and optimize the different aspects of services at some level of abstraction for both vendors and consumers.

2.1.1 Cloud Services

Cloud computing facilitates the provisioning of diverse kinds of services which can be grouped by the mode of their delivery. The cloud services are typically grouped into the following three service models:

a) *Software as a Service (SaaS*). SaaS is the provision of sophisticated web-based software applications. SaaS enables consumers to use vendor applications provided through the cloud infrastructure. The

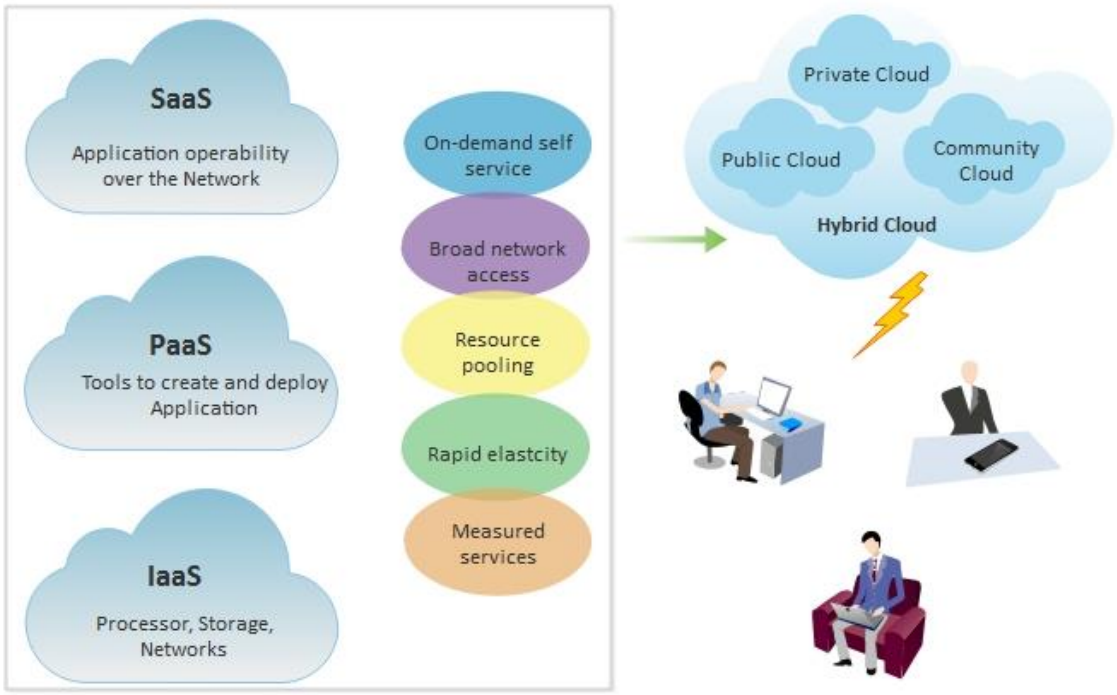


Fig. 1. The cloud computing paradigm

application provision is typically achieved through a thin client (e.g. browser) or an interface for data sending or receiving. The consumer does not need to manage the application provider infrastructure. Thus, has a limited configuration setting authority.

b) *Platform as a Service (PaaS).* PaaS is the provision of configurable development and production environments. This service model allows consumers to develop applications or software using the basic requisites which are provided by the service vendors. The consumers remain unaware of the underlying infrastructure, but they manage the acquired applications and their configuration settings.

c) *Infrastructure as a Service (IaaS).* IaaS is the provision of configurable computing resources (e.g., storage, network) by virtualization. IaaS provides consumer the capability to deploy and run software with only basic infrastructure need. The vendors provide the services for processors, storage, and networking infrastructure.

2.1.2 Deployment Models

The cloud deployment models have been mainly classified into four different types, based on the requirements specified by consumers (Mell *et al*., 2011).

a) *Private cloud:* This deployment model allows the exclusive use of clouds by a single organization. It involves a secure cloud-based environment because of the utilization of corporate firewalls and other associated security measures.

b) *Community cloud:* The community cloud infrastructure facilitates a specific community (a group of

organizations), having similar requirements, to share the cloud computing services. The responsibility of the cloud infrastructure provision can be owned by a third party or a series of community members.

c) *Public cloud:* This approach allows the cloud owner to offer public services on the internet. A public cloud is a publicly accessible cloud environment. The cloud providers are responsible for the establishment and maintenance of public clouds and IT resources required by the clouds.

d) *Hybrid cloud:* A cloud environment with the composition of two or more different cloud deployment models. This type of cloud infrastructure enables businesses to gain advantages of the secure private cloud as well as the cost benefits by having shared data on public clouds.

2.2 Cloud-based Web Services

The cloud services heavily rely on distributed computing, leveraging the benefits of loosely coupled data sharing and complex computations over the large network infrastructure. Web services, with Service Oriented Architecture (SOA), are commonly used technologies for the provision of services over cloud. The web services Application Programming Interfaces (APIs) are used as a bridge to access cloud services (Muchahari & Sinha, 2013). The Web Services Description Language (WSDL) describes the web service functionality. A Universal Description Discovery and Integration (UDDI) platform is provided to register and discover web service applications (Papazoglou, 2007; Heilig & Voß, 2014).

Many cloud service vendors such as Amazon AWS and Microsoft Azure implemented Web service APIs, using SOAP and HTTP protocols, to offer service accessibility to consumers. Moreover, the web services, based on Extensible Markup Language (XML) and Representational State Transfer (REST) architecture, also facilitate the potential ways to implement cloud SaaS.

2.3 Cloud Computing in Industry

Enterprises prefer cloud computing in order to capitalize the service delivery models. The association of the productivity of the supercomputer and the agility of the client/server system is made possible through cloud paradigms. Firms are the main customers of cloud-based services to take the advantage of business-to-business capabilities of cloud computing (Haug *et al*., 2016).

The outsourcing of services by firms can be complete or partial, in the form of renting out the storage space, computing powers, or other services. Lin & Chen (2012) identified that users can capitalize from scalable capacities of cloud computing. The suppliers of the public cloud market include vendors who own and maintain the data center platforms (Marston *et al*., 2011). Among the vendors, Amazon (AWS) is the leading cloud service provider, followed by Google (Google cloud and App Engine), Microsoft Azure and IBM (Smart Cloud) (Haug *et al*., 2016; Sikeridis *et al*., 2017). Sikeridis *et al*. (2017) reported that AWS is holding over 40% share of the cloud service market whereas, Microsoft Azure, Google Cloud Platform, and IBM collectively retain share of 23% of public cloud IaaS and PaaS. The evolving trends

such as trustworthy service delivery, based on pay-per-use and other models, have strong influence on IT services industry. The key reason of cloud adoption is the performance improvements in the production cycles including the repetitive practices of design and test based on the demands of customers, which leads to the high level of customer satisfaction. The key characteristics of cloud computing contributing to the industry are as follows:

Service-oriented perspective: Cloud computing can be observed as the combination of basic service models discussed in Section 2.1.1. IaaS deliver hardware specific resources. Amazon EC2, Google Engine, and Microsoft Azure Virtual Machine are today's typical examples of IaaS. PaaS facilitates with the provision of platform (operating system, databases, execution environment) to create, test and run applications. Google AppEngine and Amazon Elastic Beanstalk are representative implementation of PaaS. The ease of access to published software is provided by SaaS. Google Apps, Onlive, and Salesforce AppExchange are famous demonstration of SaaS. In the wireless area Apple App Store is famous. Amazon for electronic books resources is also a well-known cloud service.

Virtualization and Loose coupling: Multi-tenancy, shared resources pool and virtualization are implemented to make computing resources as VMs by decoupling the binding of IT and hardware infrastructure. A shared virtual pool can be formed to configure the requirements of memory, storage, I/O, and computational ability conferring to the demand of user. Cloud-based ERP solutions, such as SAP Business Bydesign, demonstrate the ability of virtualization and multi-tenancy. Software services are vended in pay-per-use style and being run on terminals such as 3G phones, tablets or laptops.

Ease of Use and on-demand customization: The concerns to user experience are facilitating the ease of use. The emergence of web 2.0 can be seen as extension of user experience (Ram & Vijayaraj, 2011). The web applications and services are becoming like software because of the emerging AJAX technology. On the basis of custom-built templates, cloud can configure cloud services automatically. The ubiquitous accessibility and human interactions with computers also guarantee the usability of cloud.

Several studies have also highlighted the adoption decisions of cloud computing, where adoption criteria remained a focal point (El-Gazzar, 2014; Phaphoom *et al*., 2015; Marston *et al*., 2011; Smith *et al*., 2014; Zhang *et al*., 2010; Hsu *et al*., 2014; Tarhini *et al*., 2017; Safari *et al*., 2015; Gupta *et al*., 2013; Garg & Stiller, 2015; Heilig & Voß, 2014; El-Gazzar *et al*., 2016;). These studies have investigated the importance of benefits of cloud computing in industrial practices. The cost effectiveness (pay-as-you-go model) appeared to be the most influential factor followed by security, privacy and IT resources. The users are granted on-demand self-services wrapping the IT infrastructure, platform and software by ubiquitous terminals (smartphones, tablets) without much waking up to cloud technology. The users' requirements of computing and storage are met dynamically which enable the significant decrease in costs of development and management of IT systems. Fig. 2 represents the comparative analysis of industrial

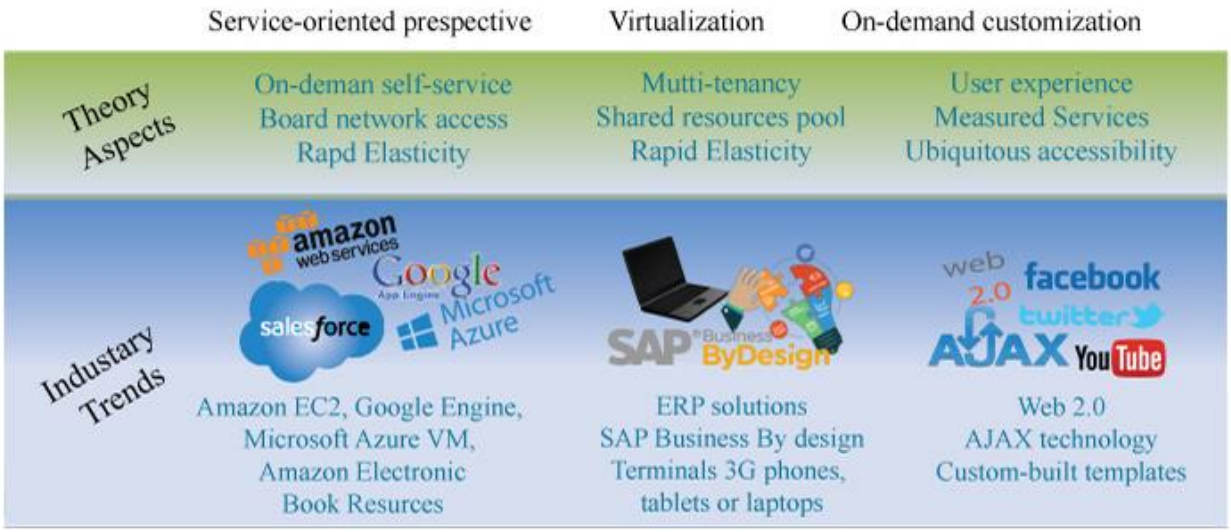


Fig. 2: Industry Trends

trends and theoretical aspects of cloud computing.

2.4 Trust Management

The cloud computing environment offers a cost-efficient indirect communication between the service vendors and consumers for the numerous scalable and shared services. The trust management system enables the stakeholders to present their reliable capabilities with proper supervision (Firdhous *et al*., 2011; Habib *et al*., 2011). In past, the trust management has been discussed mainly in context of reliable and factual feedback ratings (Firdhous *et al*., 2011; Filali & Yagoubi, 2015b, Kumar *et al*., 2016, Machhi *et al*., 2016;) and also as the method to ensure security and privacy requirements (Habib *et al*., 2011; Habib *et al*., 2013; Habib *et al*., 2014; Harbajanka & Saxena, 2016; Anakath *et al*., 2017).

A well-designed trust management system not only facilitates the cloud service providers to offer services in more assured manner, but also enables cloud consumers to select a trustworthy CSP. The accuracy of trust management system, based on feedback ratings, relies on the filtration of suspicious feedbacks. The systems should be adept to purify the feedback parameters from malicious rating values in order to produce reliable trust score. Moreover, for the management of trust, the assurance of data security and privacy in accordance with cloud security alliance is vital. The security is maintained through the means of cryptographic techniques to avoid the malicious access attacks, implementation of SLAs and certificates, and compliance to audit standards.

2.5 Trust Establishment and Evaluation Framework

The comprehensive belief in the system of service providers and the supportive technological infrastructure imitates the concept of trust in cloud paradigm (Sun *et al*., 2011; Dorey & Leite, 2011;

Chakraborty & Roy, 2012). Fig. 3 shows the major conceptual phases of trust in a global cloud structure. The trust establishment techniques are meant to setup the trust and produces a pre-trust value (rooted trust). Due to the dynamic nature of clouds, the trust estimation techniques offer the evaluation of a trust value by employing different trust parameters.

2.6 Service Level Agreements

The relationships between CSPs and the cloud users are realized through quantifiable evidences such as service level agreements (SLAs) and terms of use (Wu *et al*., 2012). The SLAs serve as the starting trust agreement for cloud customers. SLA consists of contracts for Service-level objectives (SLO), restrictions, penalties, time period, etc. The QoS parameters are monitored and guaranteed by SLAs (Chakraborty & Roy, 2012; Serrano *et al*., 2016). Availability, security, privacy, portability, scalability, backup, recovery and performance are some of the significant parameters of SLAs (Wu *et al*. 2012; Sahal *et al*., 2016). The monitoring techniques can be used to trace violations of SLAs.

Two groups of qualities, i.e., measureable and unmeasurable can be recognized in SLAs (Bianco *et al*., 2008; Aljoumah *et al*., 2015, Darwish *et al*., 2015). The measureable SLA qualities can be computed by specified and quantifiable metrics such as the percentage measure for the availability of system. The unmeasurable SLA qualities cannot be calculated automatically by considering a specific perspective (Aljoumah *et al*., 2015). Accuracy, availability, capacity, demand cost, latency, reliable messaging, scalability, provisioning-related time, backup interval, CPU utilization, response time, and throughput are the most important measureable SLAs (Frey *et al*., 2013; Aljoumah *et al*., 2015; Darwish *et al*., 2015; Sahal *et al*., 2016). Unmeasurable SLA qualities include interoperability, modifiability, and security (Aljoumah *et al*., 2015; Darwish *et al*., 2015).

Interoperability relates with the communication of information and functionality according to agreed semantics. Rezaei *et al*. (2014b) analyzed models for the evaluation of interoperability and found that most of the models are focused on standards for technical, semantic, syntactic, and organizational aspects. However, the interoperability evaluation varies significantly. Interoperability can be determined on multiple platforms, interface format, and communication protocols (Kaur & Singh, 2015). Security is the assurance to resist unauthorized access and includes characteristics of non-repudiation, confidentiality, integrity, assurance, and auditing. The use of secure socket layer or cryptographic protocol contributes towards the assessment of security (Kaur & Singh, 2015). Security Assertions Markup Language (SAML) and eXtensible Access Control Markup Language (XACML) are two standards used in web services for security verification. The issues regarding security can be handled by basic security profile to ensure the interoperability of security attributes. Security assurance has been remained an important consideration for estimation of trust of services. Section 4.4.1.1 (b) elucidates the highlights of a few security centered trust models. Modifiability concerns with the specification of how often the interface or implementation

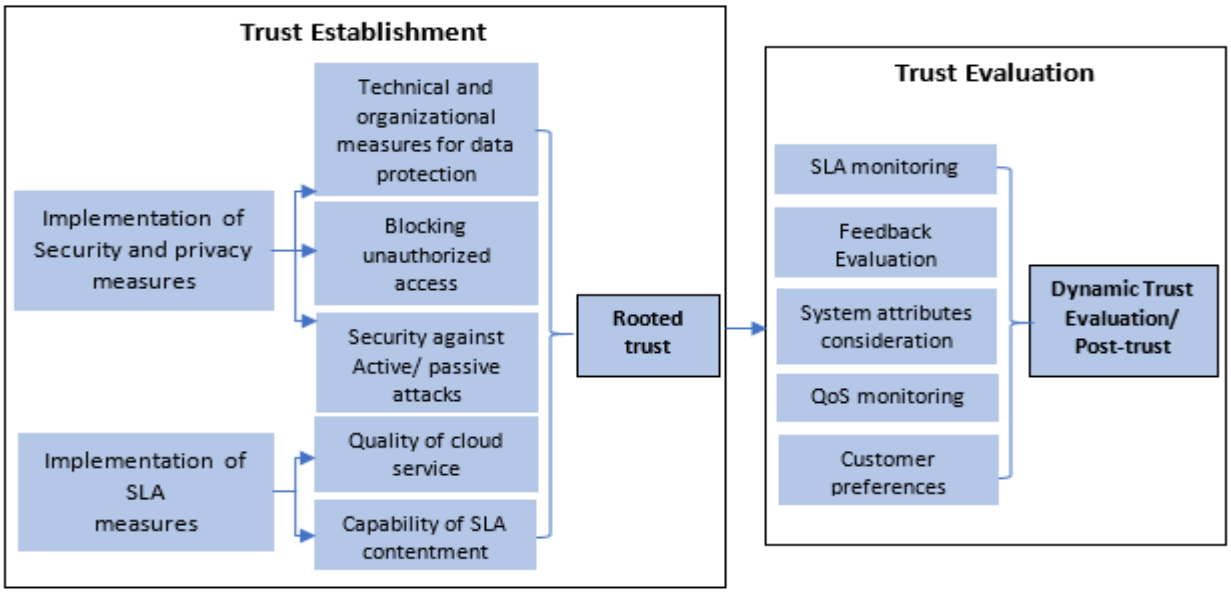


Fig. 3. Trust Establishment and Evaluation Framework

of services changes. Modifiability ensures the facility to modify data, logic, and presentation layers while taking care of the multitenant characteristics of cloud services (Burkon, 2013). However, to the best of our knowledge, the evaluation models for the assessment of modifiability attribute is not extensively studied in the literature.

2.7 Cloud Certifications

Certificates are issued to cloud users and cloud service providers to ensure security, integrity, and compliance to rules and agreements. A number of studies have been carried out to improve the transparency and trust in cloud computing (Anisetti *et al*., 2015; Cimato *et al*., 2013).

Data confidentiality is one of the ongoing challenges of cloud computing. Rocha *et al*. (2011) proposed a solution to address the confidentiality issue by designing a trusted platform module which provides the protection against malicious insider attacks in infrastructure-as-a service implementation of clouds. A framework is designed for the assessment of security and functional characteristics of cloud (Cimato *et al*., 2013). The certification compatible definitions of security attributes are formalized along with the lifecycle stages of certificates. Similarly, a certification approach, aimed at the security properties for different types of cloud services, is introduced by Krotsiani *et al*. (2013). The approach is based on the continuous security assessment on the basis of the operational evidences generated through continuous monitoring. In another study, Anisetti *et al*. (2014) presented a trust model which is based on the multiple signature processes. The model manages dynamic states of the security certificates to establish trustworthiness in the cloud environment. Then, an open source solution, for the management of the infrastructure services, named, as OpenStack is also presented by Anisetti *et al*. (2015). The authors

presented several analysis steps for the certification of security and performance factors along with the results of the process.

The importance of the dynamic certification of cloud has been highlighted to demonstrate the cloud providers' reliability and security to cloud consumers (Lins *et al*., 2016). The dynamic certification demands the monitoring and auditing to be performed automatically, and ensures the transparency in service provider's verification. A formal modeling based hybrid certification model with defined characteristics is proposed by Katopodis *et al*. (2014). The model is based on security monitoring and automatic testing that is intended to enhance the customer reliability and trust.

Cloud service certification knowledge is structured by taxonomy for assessment criteria (Schneider *et al*., 2014). Six dimensions with numerous characteristics are presented as criteria where security, privacy, legal compliance, flexibility, availability, stability, and contract are included in service assurance dimension. A certification-based adaptive assurance method is proposed to enhance the transparent cloud system (Anisetti *et al*., 2017). The scheme has provided a certificate life cycle management mechanism which includes the certificate issue and its adaptation to handle the occurrence of changes during these phases. An abstract property, as a building block of certification, is derived from the shared terminologies (confidentiality, integrity, availability) or regulations, and specifications.

3. Research Methodology

The systematic literature review process typically involves the framing of research questions for a review, the identification of the related work, estimating the quality of services, reviewing the evidence, and incorporating the findings (Khan *et al*., 2003). This study is based on a fine-grained approach to extend key phases into multiple sub-phases. The detailed workflow of the review process employed in this study is depicted in Fig. 4.

3.1 Article selection

The strategy for the selection of articles is based on the two main stages by following the steps shown in Fig. 4. The search, on the basis of keywords and publication years, has been performed in the first stage. The keywords such as cloud trust, cloud trustworthiness, trust in cloud, trust evaluation, and trust cloud services are utilized to retrieve the relevant articles from famous electronic research repositories such as Web of Science, IEEE, Elsevier, and ACM and around 120 articles were retrieved. However, in the second stage, 79 articles for analysis were considered on the basis of the certain screening criteria. The screening criteria involved the identification of QoS, SLAs, and introduction of schemes or techniques for trust estimation and establishment of trust between CSPs and cloud consumers. The screening process then included careful reading of titles, abstracts, and content of the articles for relevance.

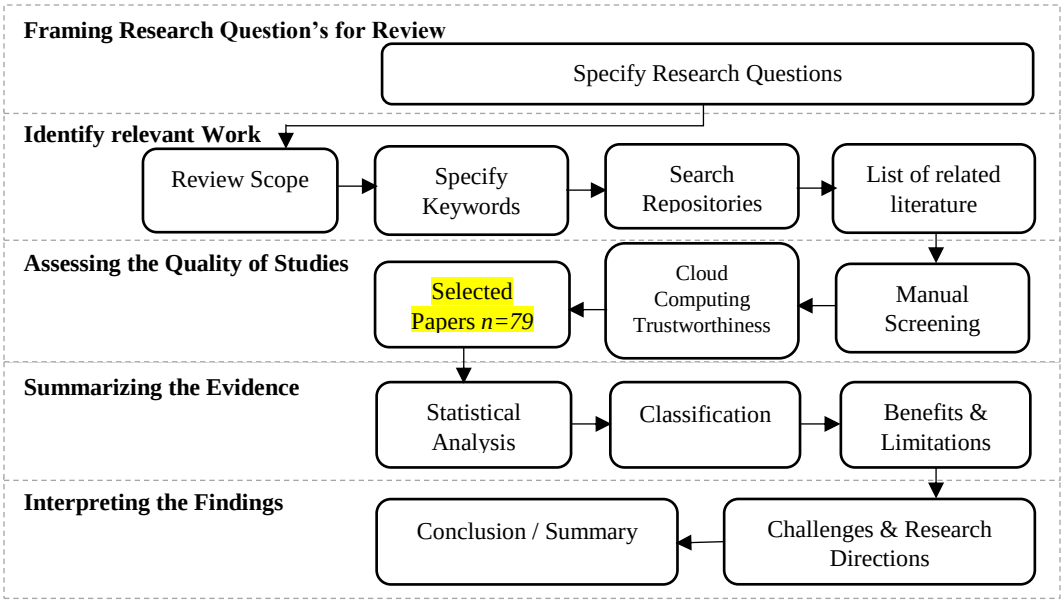


Fig. 4. The workflow of the review process

3.2 Literature Statistics Analysis

The scope of this study, in terms of date, is from 2010 to 2018. A total of 79 research papers have been selected for this study, which appeared in prestigious conferences and journals during the mentioned period. Fig. 5 provides an overview of the broad classification, with number of studies per class. It is pertinent to observe that the algorithmic solutions for the trust estimation have been explored in the least number of studies. On the contrary, the highly focused areas have been the policy-based trust establishment and the trust computation frameworks. These studies seem to be overwhelmed by the user trust estimation fever, based on feedbacks, usage experiences, and statistical approaches. The service usage experience appeared as the most focused parameter. The fuzzy logic, multi-criteria decision making techniques and algorithmic solutions have been other imperative trust estimation techniques.

3.3 Research Questions

This study aims to get the answers of the following research questions:

Q1. How to classify the recent existing trust establishment and estimation techniques?

Q2. What constituent components of the trust are employed in different studies and what is their usage pattern?

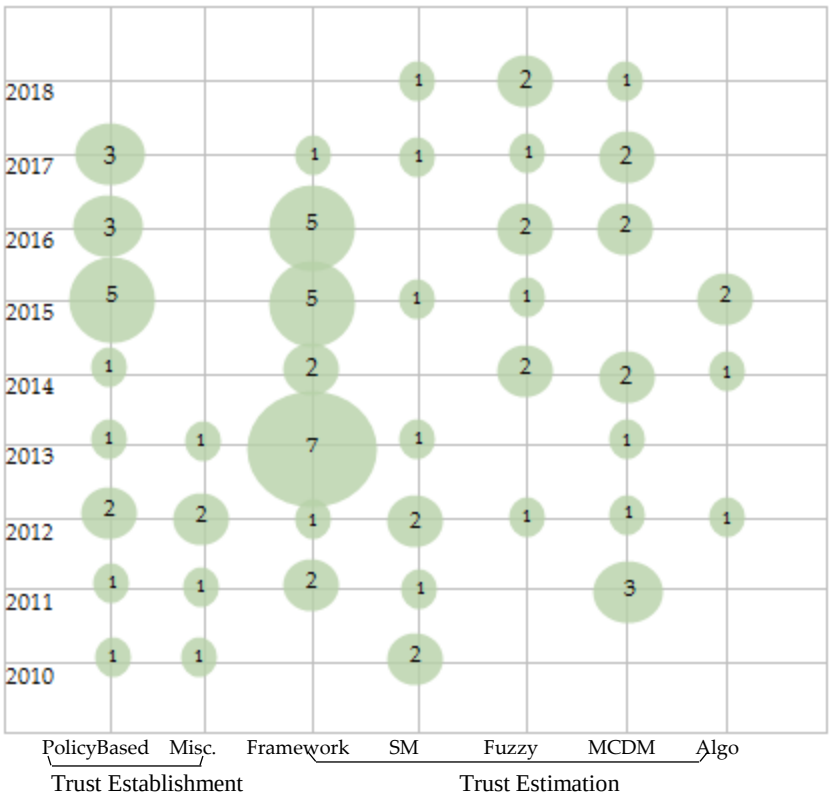
Q3. What are the benefits and limitations of the existing approaches?

Q4. What experiment patterns have been used in the literature?

Q5. What other possible directions can be explored for further research?

4. Trust in Cloud Services

Trust is a term borrowed from the social sciences discipline, where it is defined as the belief of an individual on another in a collaborative environment (Abrams, 1995; Grabner-Kräuter, 2009; Grabner-



Misc.; Miscellaneous Schemes, SM; Statistical Methods, MCDM; Multi-Criteria Decision Making, Algo; Algorithm

Fig. 5. Literature Statistics

Kräuter & Bitter, 2015). In the social perspective, the trust is a human notion, but the concept of the trustworthiness appears to be more imperative in a distributed computing environment such as cloud computing. The acceptance of cloud services is highly affected because of the non-transparent and distributed multi-tenant cloud environment. Therefore, the trust establishment is inevitable in cloud computing.

In a number of studies in the existing literature, the trust has been referred as a general term of privacy and security (Khan & Malluhi, 2010; Sun *et al*., 2011; Dorey *et al*., 2011; Abbadi & Martin, 2011). The consumers of cloud services usually feel the loss of the control over data which they store on the cloud. Furthermore, the trustworthiness of the cloud providers is also a hurdle in the widespread adoption of cloud computing (Khan & Malluhi, 2010; Sun *et al*., 2011; Abbadi & Martin, 2011; Huang & Nicol, 2013). The cloud trust management techniques mainly depend on the user expectations of QoS, Service Level Agreements (SLAs), and audits and compliance. Fig. 6 (the left side) shows the typical workflow of consuming n number of services offered by cloud service providers. Fig. 6 (the right side) highlights that the trust evaluation and management typically relies on the security assurances, QoS monitoring, SLAs, audits, and compliances. The selection of Cloud Service Provider (CSP) is one of the

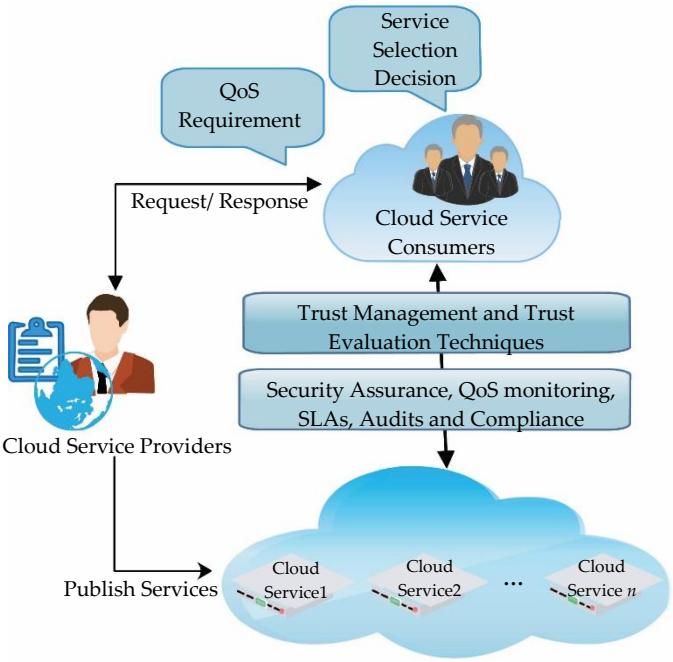


Fig. 6. Trust in cloud computing.

most challenging issues because of the context sensitive nature of the trust. The cloud environment enables communicating entities to initiate transactions without establishing the direct communication among service providers and consumers. A trust management system, in cloud computing, manages trust relationships between distributed entities. The standardization bodies, challenges in the establishment of trust, and review of the related literature have been presented in Sections 4.1, 4.2, and 4.3, respectively.

4.1 Evolution of Trust

The notion of trust is widely realized in real-world applications with the adoption of distributed systems (Abrams, 1995). During early 2000s, the trustworthiness studies considered ratings as the measure of conformance to trust (Rahman & Hailes, 2000; Cahill *et al*., 2003; Carbone *et al*., 2003). Trust has also been used as an imperative decision making factor in web-based applications. Thereafter, the definition of trust points towards the subjective likelihood by which a group is expected to accomplish assigned tasks with the notion of relative security (Josang *et al*., 2007). The trust computation has also been examined in the reputation evaluation of Grid environments (Eymann *et al*., 2008). Manuel *et al*., (2009) evaluated trust as the measure of reliability, security, capability, and availability in the milieu of the distributed environment. The requirements of data integrity, identification management and security and privacy, ultimately took the form of trust management (Khan and Malluhi, 2010). The basic definition of the trust management was set as the establishment of the belief and assurance on the resource or service providers in the distributed systems. Fig. 7 illustrates the paradigm shift during the pre-selected era of this study.

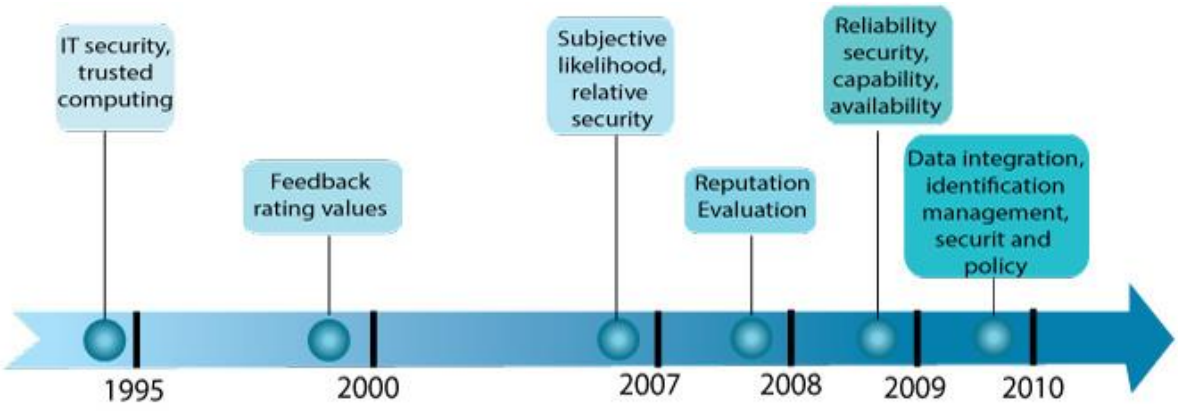


Fig. 7. Evolution of Trust in Cloud Computing in pre-selected era of this study

4.2 Standardization bodies

The monitoring of QoS attributes and the verification of SLAs are essential for the factual trust evaluation of cloud services because of their dynamic nature (Selvaraj & Sundararajan, 2017). The most of the QoS parameters such as related to security and privacy aspects remain invisible for the end users to be monitored by themselves. The provision of transparency is enhanced through the introduction of Security, Trust and Assurance Registry (STAR) and Cloud Trust Protocol (CTP) by Cloud Security Alliance (CSA) (Habib *et al*., 2014; Shaikh & Sasikumar, 2015; Selvaraj & Sundararajan, 2017). STAR is a free registry program with public access which helps the CSPs to put out their security assessments in Consensus Assessments Initiative Questionnaire (CAIQ) or a Cloud Controls Matrix (CCM). CTP is a request-response functionality that facilitates cloud users with evidence-based assurance. CSA has also launched an automated auditing system, namely, CloudAudit to accomplish a formal audit process.

4.3 Challenges in Trust

A system is not trustable if it provides inadequate information about its capability (Sun *et al*., 2011). There are several challenges that need to be addressed during the establishment and estimation of trust due to its growing demand, adoption, and technological enhancements. Although the existing literature has provided mechanisms to resolve the trust issues in a variety of application scenarios, the randomness of trust value, trust parameter storage, and effective identification and management of trust in distributed environments still need to be further explored.

4.3.1 Trust establishment challenges

Some of the main challenges regarding trust establishment reside in clear and transparent view of cloud targeting the security requirements. The major security measures and trust-related factors such as security management standards, diminishing control, and transparency have been investigated in the different

studies (Sun *et al*., 2011; Khan & Malluhi, 2010). The review of the related literature shows that the problem of trust is widely addressed from a single dimension, A number of few other studies have only considered security and legislation aspects for trust establishment (Guo & Xu, 2012; Abbadi & Alawneh 2012; Sidhu & Singh 2014; Ghosh *et al*., 2015; Harbajanka & Saxena, 2016; Abdallah *et al*., 2017;). There are a number of challenges that need to be addressed while establishing trust in real-world applications: (i) formulation of a single approach that addresses all trust related issues involving SLAs and security requirements, (ii) authentication of users to assess the trust by their own, (iii) trustworthiness strategies for third party cloud audit or broker, (iv) trust models for ubiquitous systems, and (v) trust based on the behavioral histories of the cloud stakeholders. Section 4.4.1 elucidates different contributions on trust establishment along with the potential benefits and limitations.

4.3.2 Trust estimation challenges

The trust estimation techniques in the literature tend to incorporate monitoring and prediction of QoS attributes. Rashidi *et al*. (2012) highlighted the risks associated with cloud computing related to trust estimation and presented a model for the estimation of trust on the basis of the identified risk factors. The researchers have observed that the backup and recovery mechanisms strongly influence the trust of users, followed by availability, privileged user access, regulatory compliance, long-term viability, and data location. Similarly, literature has highlighted the challenges regarding the estimation of trust on the basis of user opinions for QoS values and their validities (Li & Du, 2013; Fan & Perros, 2013; Ding *et al*., 2014; Taneja *et al*., 2015; Ma *et al*., 2015; Machhi & Jethava, 2016; Kumar *et al*., 2016;). However, some of the open issues that still need to be investigated are following: (i) lack of the feedback standardization process for each QoS to remove complications, i.e., user should be able to provide a valid feedback against the quality of service attributes, (ii) the feedback filtration process to identify and remove the malicious feedbacks from trust estimation, (iii) lack of mechanisms to handle negative trust parameters i.e. trust estimation using trust reducing factors along with the trust building factors, (iv) handling of multi-source feedback and their fusion standards in trust evaluation, and (v) evaluation of 'trust as a service' based on reputation and feedback analysis.

Moreover, the literature has also identified certain aspects of trust estimation by ranking methods, multiple criteria decision makings, and recommendations (Saripalli & Pingali, 2011; Ma *et al*., 2014; Garg *et al*., 2012; Ding *et al*., 2014; Sun *et al*., 2013; Sun *et al*., 2016). Nonetheless, there is still a gap to be filled in the field of trust estimation. The main open challenges are following: (i) Multicriteria based reputation analysis incorporating the user preferences and SLA compliance (ii) the identification of rating methodologies and secure floating of rating calculations among cloud stakeholders, (iii) the use of the trust evaluation instrument in the cloud design to maintain several dynamic QoS values, (iv) the group decision making techniques that include cloud users as well as third party cloud audits, and (v) the

identification of a formal validation technique that can be used to validate the trust values for individual as well as group decisions. Furthermore, the limitations of the studies related to the domain of trust estimation are highlighted in Section 4.4.2.

4.4 Cloud Trustworthiness techniques

In order to address Q1, the existing literature of the trustworthiness in cloud computing can be broadly classified into the trust establishment and trust estimation techniques. The trust establishment techniques are meant to set up the trust by typically employing the trust policies. The trust estimation techniques, on the other hand, offer the assessment of overall trust value of cloud services. These classes are further divided into a number of distinct subclasses, based on the available literature, as illustrated in Fig. 8.

4.4.1 Trust Establishment

The review and analysis of the related literature in this (4.4.1) and subsequent (4.4.2) subsections has addressed Q3 and Q4. The literature of the trust establishment techniques can be classified into the policy-based trust and miscellaneous schemes.

4.4.1.1 Policy-based Trust

The legal guarantees are provided to the cloud users so that they can have confidence on a particular cloud service. These legal guarantees take the form of SLAs and security assurance rules to facilitate the trust establishment process. The characteristics of studies, focusing on policy-based trust, are summarized in Table 1.

a. SLA-based Trust

The SLA is a formal commitment between cloud service providers and service users (Serrano *et al*., 2016). The key features of cloud services such as quality, availability, and responsibilities are contracted between the two entities. A number of studies have considered SLA as a basis of the trust establishment in cloud services (Chakraborty & Roy, 2012; Sidhu & Singh, 2014; Manuel, 2015; Singh & Sidhu, 2016).

Chakraborty & Roy (2012) presented a framework which evaluates the trustworthiness of a CSP by employing a quantitative trust model. The framework is based on the two classes of parameters, namely, pre-SLA parameters and post-SLA parameters. The values of the first set of parameters are directly computed from SLA. The values of the second parameters, however, can be obtained from the logs or session histories. Nonetheless, the process of the establishment of trustworthiness is biased towards one parameter. Furthermore, the users should be able to obtain and evaluate the values of the parameters according to their choices in order to get an adequate level of trust value.

Sidhu and Singh (2014) presented a trust computation technique, which depends on the compliance of CSP to the guaranteed SLAs. The technique shows that the compliance-based monitoring mechanisms contribute positively to enhance the reliability, availability, and scalability of cloud services. The

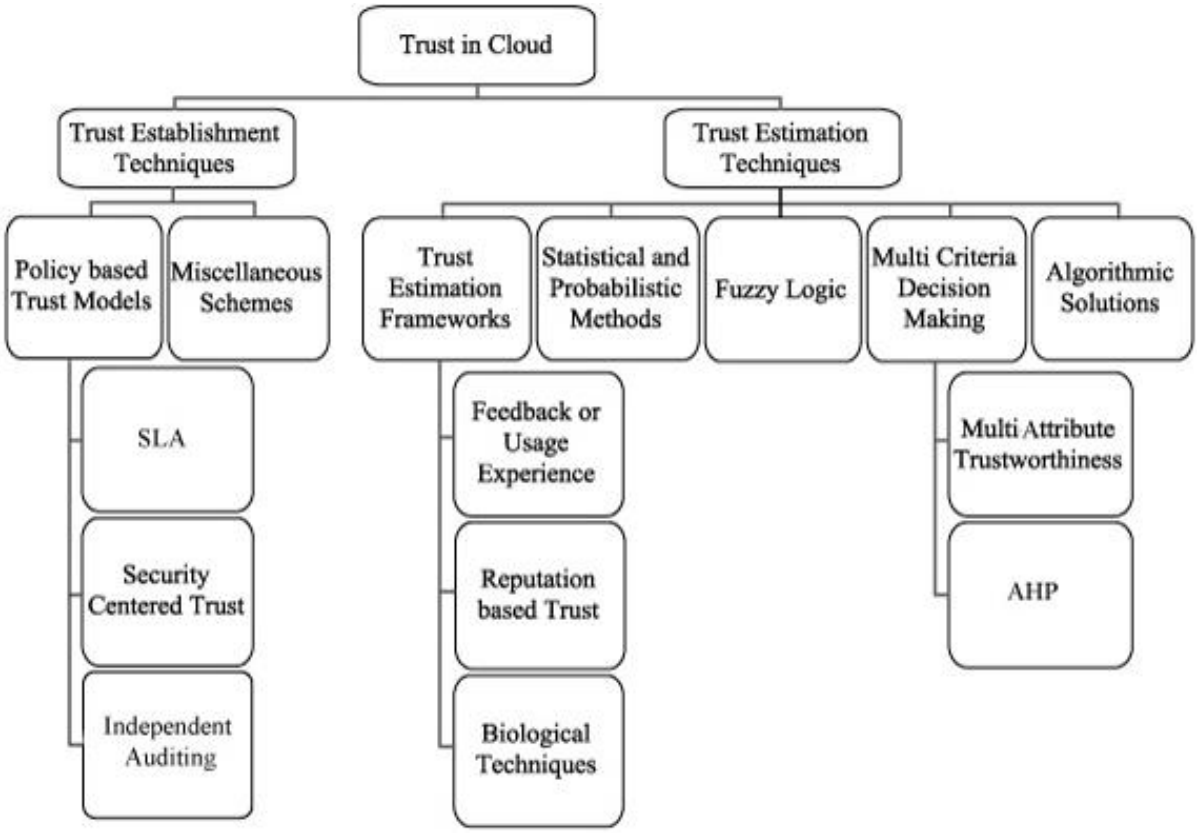


Fig. 8. Trust in cloud computing: A taxonomy

simulation of the proposed technique is carried out using a sample synthetic cloud data on MATLAB. The results demonstrate that the technique can be employed for establishment and estimation of trust in the cloud computing paradigm. Nevertheless, the trust calculation is merely based on the monitoring of SLAs conformance.

A QoS-based trust model, proposed by Manuel (2015), computes the trust values on the basis of the four parameters, viz., reliability, accessibility, efficiency, and integrity. The model also employs the new trust establishment parameters such as utilization of resources, honesty, and return-on-investments. The model explains the SLA preparation by considering the user QoS needs and the abilities of the cloud resources. The simulated experiments have been performed to advocate the supremacy of the presented model as compared to other similar models. Nevertheless, the performance evaluation, on the basis of only four attributes, seems insufficient to achieve a valid calculation of the trust.

Singh and Sidhu (2016) designed and evaluated a Compliance-based Multi-Dimensional Trust Evaluation System (CMTES) to regulate the trustworthiness of CSP by monitoring the services compliance to SLAs. The trust value is computed from the examined compliance of SLAs by employing the improved Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) method. The multiple QoS parameters, for the assessment of trust, are also elucidated in the study. The effectiveness of

Table 1: Summary of the Trust Establishment Techniques (Policy-Based Trust)

References	Trust Factors	Experiment patterns			Benefits	Limitations
		Simulations	Real data Set	Case Study		
Takabi *et al*., 2010	Security				Deals with multiple security related issues	No experiments and Only refers to SLAs
Ko *et al*., 2011	Security, Auditability				Assures the accountability of CSPs	Only theoretical descriptions and No experiments or system implementation
Chakraborty & Roy, 2012	Not mentioned				The flexibility of framework, as all parameters are not required to initiate the trust establishment	User preference may be mishandled as no method of weight assignment is employed
Guo & Xu, 2012	Security				Ensures the security against passive attacks	Other important QoS parameters are neglected
Huang & Nicol, 2013	Security				Security breaches identification on the basis of historical data	No formal modelling
Sidhu & Singh, 2014	Availability, Reliability, Scalability	✓			Monitoring of SLAs conformance	No real world experiments
Manuel, 2015	Reliability, Accessibility, Efficiency, Integrity	✓			SLA preparation by merging user QoS requirements and service abilities	Lacks user preferences for trust estimation
Shaikh, & Sasikumar, 2015	Security in terms of privacy				Assures security by CSA challenges	lacks the concept of trust evaluation against various other QoS values
Rizvi *et al*., 2015	Security				Empowers cloud users to provide security preferences	Experiments are no performed
Meera & Geethakumari, 2015	Security				Provenance audit of cloud services	Experiments are no performed
Ghosh *et al*., 2015	Risk assessment, security			✓	Assessment of transparency in vendor's SLAs	Lacks user preferences
Singh *et al*., 2016	Robustness, Availability, Storage space, Response time, Speed, Ease of use, Price, Technical support, Customer service		✓		Monitoring the services compliance to SLAs	Lacks user preferences
Harbajanka & Saxena, 2016	Security				Data management in cloud servers with security and privacy	Lacks other QoS parameter consideration, no experiments
Lins *et al*., 2016	Reliability and Security				Continuous auditing	No Experiments
Abdallah *et al*., 2017	Integrity, access control, availability, and privacy				Presents countermeasures against existing common attacks	No real-world experiments
Anakath et al., 2017	Security	✓			Securing cloud access through biometric authentication	Lacks trust evaluation from user's perspective
Balasubramanian & Kim, 2017	Security		✓		Secure data storage and sharing	Lacks user preferences for QoS in trust evaluation

CMTES is advocated through the experiments performed by using the real data set from the Cloud Armor Project (CAP, 2012).

b. Security-Centered Trust

Over the years, a few security-centered models have been presented in the literature. Takabi *et al*. (2010) presented a framework with multiple modules. The modules perform tasks, namely, identity management, trust management among clouds, trust management among a cloud and its users, policy integration among multiple clouds, access control, and secure service composition and integration. The trust management module only considers SLAs. The SLAs with unclear clauses and technical specifications can cause undependable trust establishment. Moreover, the framework only provides theoretical descriptions of each module, that is, no experiments have been carried out to analyze the performance of modules. Ko *et al*. (2011) designed a TrustCloud framework on the basis of Cloud Accountability Life Cycle (CALC). The system layer of the framework assures to track the complete virtual machine changes. The data layer maintains the data abstraction and enables the data centric logging. The workflow layer controls the audit trails or governance of the cloud applications. The policy, law, and regulation layers deal with the accessed data items and executed processes. The framework ensures security and auditability on the basis of laws and regulations, but the end users are typically unaware of the rules and their technical details in the cloud computing environment.

Guo and Xu (2012) proposed a scheme, based on the Kamara model, which permits each client to outsource its resources to a number of sub-clients. The proposed cryptographic solution offers security against passive attacks. Huang and Nicol (2013) proposed a general structure of the evidence-based trust judgment. Furthermore, the method of the computation of the chain of trust among cloud services, cloud providers, cloud brokers, and cloud users has also been presented. The researchers have developed a high-level framework for trustworthy cloud analysis, which lacks the proof of correctness.

To facilitate the selection of a CSP, a cloud broker framework SelCSP is recently designed *(*Ghosh *et al*., 2015). SelCSP is a risk model for the selection of reliable CSP. SelCSP focuses on metrics such as number of CPUs and VMs down time and their interaction. The interaction-risk estimation is based on the combination of trustworthiness and competence. The direct interaction experience and reputation feedback of vendors contribute to trustworthiness calculation. The competence is computed by assessing the transparency in SLAs. Nevertheless, SelCSP evaluates the trustworthiness using traditional rating factors rather than the real time user service interaction. Shaikh and Sasikumar presented a trust model to measure the security strength of a cloud service (Shaikh & Sasikumar, 2015). The model trails several security parameters and computes the trust value. The model employs Cloud Service Alliance (CSA) challenges to evaluate the service security. The model validity and adequacy is verified by CSA. The overall trust management system is focused on ensuring security in terms of privacy. Nevertheless, the

presented model cannot incorporate the multiple attributes, namely, availability, response time, and throughput, which may be imperative for the establishment of trust on a cloud service.

Harbajanka & Saxena (2016) designed a trust management system to secure data management and data exchange on the basis of cryptographic measures. However, the filtration mechanism has not been incorporated in the system in order to filter malicious user ratings. Recently, a generic trust model (TRUST-CAP), to address the security problems related to man-in-the-middle and man-at-the-end attacks, was presented by Abdallah *et al*. (2017). The model targets the cloud-based applications that rely on integrity, access control, availability, and privacy for the estimation of trust values. Nevertheless, the authors have only focused on Infrastructure as a Service (IaaS) to offer a security service.

A trust model aiming at the identification of client device in order to preserve the security and privacy of data is proposed by Anakath *et al*., (2017). Biometric authentication is used to identify the secure client. Two aspects password and user profiles are used to summarize the behavior of user to validate the trustworthiness of clients. The system is tested through different experiments to show the optimum false positive rate and resource utilization. However, the study has not considered the trustworthiness of service provider from the perspective of clients.

Balasubramanian and Kim (2017) proposed a scheme to ensure data security in milieu of trust evaluation using compliance of QoS parameters and fuzzy-based approach. The scheme supports the re-encryption of trust value after its generation. The rule generator is employed to evaluate trust on the basis of history and then it is sent to the user to select the service. However, the method does not incorporate user preferences for QoS parameters to evaluate trust of cloud services.

c. *Independent Auditing*

The facility to audit the IT infrastructure increases the level of trust on service provider by mitigating the security problems. Handoko *et al*. (2017) performed a fundamental quantitative research to examine the effect of third party auditor by using partial least square and path analysis. The authors argued that the third party auditors positively affect cloud security and ultimately improve user trust. A few researchers proposed methodologies that enable third party authorities to perform cloud audit in order to increase cloud trust (Rizvi *et al*., 2015; Meera & Geethakumari, 2015; Lins *et al*., 2016). The protection of data integrity of users on cloud can be managed through third party auditing (TPA) which logs and audits the CSP's performance (Mei *et al*., 2013). A trusted enhanced third party auditing scheme is proposed to ensure the reliable auditing, by employing TPM-compatible USBKey to avoid cheating attacks.

Rizvi *et al*. (2015) proposed a framework for security auditing in the establishment of trust. The framework empowers the cloud users to provide security preferences using third party audit. A theoretical method for the validation of security policies is also presented along with the maintenance of database for

CAIQ responses and certificates. However, no experiments have been carried out to validate the utility of the framework.

The provenance audit of cloud services, incorporating the security concerns, is presented by Meera and Geethakumari (2015). The study is aimed at the execution of provenance audit of several guest operating systems on cloud. The traditional cryptographic techniques, such as encryption, checksums, and signature generation, are used for integrity preservation, privacy, and verification purposes. However, the researchers examined the security issues only from service provider's perspective in order to build a trust relationship with the customers. The reliability and security of cloud services require continuous auditing in order to validate the trustworthiness of cloud certifications (Lins *et al*., 2016). A conceptual auditing architecture for cloud is presented with the essential components and implementation need of different processes. The benefits and issues are highlighted which need to be handled to sanctify the concept of continuous auditing.

Third party auditing is an adequate technique to define trust between cloud stakeholders. The auditor is needed to monitor, evaluate, and expose the associated risks with the cloud services. A trusted auditing enables customers to wisely select the required service from a group of similar services (Ko *et al*., 2011). The continuous and timely auditing reduces the trust risks to the customers and helps CSPs to maintain trustworthiness.

4.4.1.2 Miscellaneous Schemes

A model for the efficient reconfiguration and resource allocation is presented by Kim *et al.* (2010). The reconfiguration and resource allocation are carried out on the basis of user requests. The authors defined the trustworthiness of cloud services as $H_i = W_1 RC_i + W_2 RU_i + W_3 T_i + W_4 S_i$, where H_i represents the trust value of a resource i, RC_i, RU_i, T_i, and S_i are trust attributes, and W_1, W_2, W_3, and W_4 are associated weights. The model considers the manual assignment of weights to attributes, even though the scheme supports the multi-attribute evaluation. Therefore, improvements can be made in the context of decision weights allocations by considering user preferences. Abbadi and Martin (2011) argued that trust establishment in cloud computing should consider the requirements of different users by offering them different trust models. Each model should offer adequate level of transparency in trust establishment and technical complexities. The study has also reported the recent results from the TClouds project.

Abbadi and Alawneh (2012) has discussed the importance of establishing secure and trusted Cloud computing by allowing users to control their outsourced data at public Clouds. A basic framework has been presented, which helps to address the challenge of establishing trust in IaaS. A cloud resource trustworthiness assessment framework is designed by Kuehnhausen *et al.* (2012). The framework measures the consumption of resources in order to establish the trustworthiness. This framework only relies on the resource consumption computation to compute the trustworthiness and it does not facilitate the end users to make decisions on the

basis of their preferences.

A Resource Provisioning Scheme, based on the Peer to Peer (P2P) architecture, was proposed by Rahman *et al.* (2013). Each node, from the data center, is provided with its own decision power for resource provisioning. This approach avoids the need of a global decision maker. The decision-making process is based on multiple factors such as availability of computational resources, network bandwidth, migration cost, and Service Level Objective (SLO) constraints. The presented scheme, however, lacks the decision support for the end users. Table 2 provides a summary of the studies which belong to the trust miscellaneous schemes category.

4.4.2 Trust Estimation

The trust estimation literature can be broadly categorized into the trust estimation frameworks, statistical methods, fuzzy logic techniques, and multi-criteria decision making schemes.

4.4.2.1 Trust Estimation Frameworks

The trust estimation frameworks can be further classified into the feedback or usage experience, reputation-based trust, and biological frameworks.

a. Feedback or usage experience

A recommendation method to predict QoS values of web services has been presented by Zheng *et al.* (2011). The presented technique integrates the item and user-based collaborative filtering approaches; hence forms a hybrid approach, in which the predictions are based on the information of the related items and users. The Pearson correlation coefficient method has been employed for the computation of the similarity score. Nonetheless, the performance of the presented method has not been thoroughly investigated.

The idea of employing the customer ratings to establish customer quality profiles has been investigated by Tserpes *et al.* (2012). The similarities, in the service ratings, have been identified by computing the correlation between the customer quality profiles. These similarities further lead to most appropriate service prediction for a specific cloud service consumer. This service recommender mechanism also considers the SLA agreements along with the cost considerations. The mechanism highlights the fact that these factors highly influence the user experience. However, the researchers have ignored to consider the variation of the rating weightages, which may affect the rating results.

Sun *et al*. (2013) formulated a similarity measure for the computation of web services trust by employing the normal recovery collaborative filtering method. The proposed method predicts the nonfunctional QoS attribute values in order to formalize the service recommendation. The researchers conducted comprehensive real world experiments for the nonfunctional attributes prediction. The results indicate that the method yields better accuracy than other competing approaches. Nevertheless, the variance in the QoS attribute values has not been considered in the experiments. The cloud service trust estimation, based on the objective assessment, is presented by Zheng *et al.* (2013). A QoS prediction model, namely, CloudRank, for the optimal selection of

Table 2: Summary of the Trust Establishment Techniques (Miscellaneous Schemes)

References	Trust Factors	Experiment patterns		Benefits	Limitations
		Simulations	Real data Set		
Kim *et al*., (2010)	Efficiency in Resource Allocation		✓	Increases the overall cloud system reliability	Manual weight assignment
Abbadi & Martin, 2011	Transparency			considers the different user requirements by different models	lacks the modeling or experiment research
Abbadi & Alawneh, 2012	Security			Trusted Platform Module (TPM) ensures the security concerns	Only valid for IaaS.
Kuehnhausen *et al*., 2012	Security			Provides the information that how likely and in which ways a resource is compromised.	Lacks the QoS parameter consideration other than security
Rahman *et al*., 2013	Availability, Network bandwidth, Migration cost, Service Level Objectives	✓		Effective provisioning decisions by nodes regarding VM allocation and migration	No decision-support for consumers

cloud services is designed and analyzed. The ranking is computed on the basis of ranking similarity of users. The QoS ranking prediction framework takes the benefit of previous service usage experience of service consumers. Nevertheless, the accuracy of the ranking predictions has not been studied through experiments. A trust management framework, viz., Cloud Armor, works as a credibility model (Noor *et al*., 2013). The model separates trustworthy feedbacks from ambiguous feedbacks. The model employs factors such as majority consensus and density of the feedback. It uses the root-mean-square deviation method for the computation of closeness between trust feedback of a specific consumer and trust feedback of majority. The model also incorporates the feedback density mechanism in order to resolve the misleading feedback problem. Cloud Armor decreases the collision of multiple feedbacks provided by the same consumers. Nonetheless, the model does not handle the conformance of QoS values, which are the main source of trustworthiness of cloud services.

The monitoring of the QoS attributes for a specific cloud service is imperative in order to guarantee SLAs. Li and Du (2013) designed a model, namely, Cloud-Trust, aiming to estimate the quality of cloud services on the basis of opinions of users. The trust analysis, based on the multidimensional trust attributes (evidences), has been computed by employing the rough set theory. The experiment results highlight the lower values of the mean absolute percentage error and the mean absolute deviation. Therefore, the results certify the effectiveness of Cloud-Trust. Nevertheless, the experiments have not considered the distributed nature of data sharing to study the performance of the formulated model. Wu *et al.* (2013) presented a cloud computing trust model

which employs fusion of Dempster–Shafer theory (DST) and sliding windows. The sliding window mechanism is employed for describing interactions between cloud users and service providers. The interactions have been classified into positive, negative and uncertain evidences. The simulation results illustrate that the presented work is effective and extensible. However, the deceptive behavior of CSPs or cloud users cannot be traced which can affect the performance of the presented method. The provided solution, however, does not consider the measurable QoS parameters along with the subjective evaluation, which can compute the more accurate calculations of trust.

The service selection model has been designed in which a mapping table is constructed in order to handle the varying inputs of fuzzy numbers, as the customer feedbacks are composed of the linguistic variables (Qu *et al*., 2013). The model also employs a filtering mechanism to remove the misleading and false values which are provided by the malicious customers. The method is evaluated on the basis of a case study. However, no comparisons have been made with other approaches to show the effectiveness of the model. A trust management framework is designed which enables cloud service users to submit the trust feedback (Fan & Perros, 2013). The filtering mechanism employs the effectiveness of the familiarity and consistency as two important factors in order to filter out the submitted feedback. A number of experiments have been performed in order to show the effectiveness of the model in recognizing the unfairly positive and negative feedbacks. Nonetheless, the model lacks the capability to classify the feedback of new users into positive or negative category. Moreover, the feedback submission criteria could be improved by employing the various QoS attributes according to the user preferences.

Ding *et al.* (2014) designed a framework, namely, CSTrust. The framework combines the subjective and objective assessments, that is, QoS prediction and customer satisfaction. The missing attributes of QoS are estimated by considering the experiences of the similar cloud services along with the customer satisfaction of the qualitative attributes. Moreover, the cloud service trustworthiness computations are performed by employing the collaborative filtering approach with the constant aversion risk utility function.

The utility theory advocates the notion that the higher utility means higher customer satisfaction. However, the credibility of the customer satisfaction needs to be handled properly to improve the results. A QoS selection and a trust model has been presented in which trust of the service provider is calculated by employing the QoS parameters like feedback, user preference, and direct user trust (Filali & Yagoubi, 2015a). The model is validated through the simulated experiments. An optimal cloud service selection can be made by using both the subjective assessment (that is, the user feedback) and the objective assessment (that is, QoS). A credible context-aware cloud service selection model has been presented (Qu *et al*., 2015). The performance of the presented model is analyzed through simulated experiments. A cloud service selection model, which considers, direct, and hybrid trust degrees, has been recently designed (Pan *et al*., 2015). These degrees are the frequencies of the interactions among the service users. The Jaccard coefficient and Pearson correlation

coefficient have been computed to measure the similarity by incorporating experience usability. The trust enhanced similarity is computed by modification of the basic similarity using the degree of trust. The values of the trust have been exploited for the forecast of missing values of the QoS parameters. The data sets employed for experiments consist of throughput and response time values. The cloud service recommendation, nevertheless, does not consider the service utility computation based on the user preferences.

Filali and Yagoubi (2015b) advocated the fact that if the integration of feedback and rating in the service selection problem are not considered significantly, then the results may not be useful for both service providers and cloud consumers. The ratings are further filtered to remove the biased opinions by employing a bias function. The method adopts a hybrid approach for determining similarities by combining the multiple similarity computing algorithms, namely, cosine vector similarity, Pearson correlation, Minkowski distance, Euclidean distance. The users are classified into the different groups to identify the unfair users. The grouping is made according to the ratings of the users by employing the well-known k-means technique. The presented technique, however, does not consider QoS requirements for the computation of similarity score. Taneja *et al.* (2015) designed a trust estimation model which evaluates the trust factor on the basis of the previous experiences. The model is adaptable, as it recommends a particular cloud service provider according to the customer requirements. The model is supported by the simulated experiments. Nonetheless, it lacks the ability to handle the malicious feedbacks.

Sun *et al*. (2016) formulated a similarity measure for the computation of web services trust by employing the normal recovery collaborative filtering method. The proposed method predicts the nonfunctional QoS attribute values in order to formalize the service recommendation. The researchers conducted comprehensive real world experiments for the nonfunctional attributes prediction. The results indicate that the method yields better accuracy than other competing approaches. Nevertheless, the variance in the QoS attribute values has not been considered in the experiments. The trust management framework, to effectively filter out the untrustworthy feedback, has been presented by Machhi and Jethava (2016). The filtering is based on the cloud consumer behavior, majority feedback, aging factor, and exogenous method. Nevertheless, the study only considers the theoretical modeling of the trust calculation process and no experiments have been performed to analyze the performance of the presented framework.

Two novel prediction models, namely, User Context-aware Matrix Factorization (UC-MF) and Service Context-aware Matrix Factorization (SC-MF), which employ the context information of services and users, have been proposed to achieve the QoS prediction accuracy (Xu *et al*., 2016). The models rely on the context information for the identification of users or services similarity. The prediction values are computed on the basis of QoS and neighbor similarity values. The geographical information with respect to the user and company affiliation has been considered for the trust estimation. The experiments, on the basis of two real world data sets, have been performed to analyze the effectiveness of the presented models. Emeakaroha *et al*.

(2016) designed a trust label system for the communication of trustworthiness in cloud services. A preliminary assessment to check the processes and helpfulness is supported by a practical use case. Table 3 summarizes the characteristics of studies focusing on the feedback or usage experience.

b. Reputation-based Trust

A multidimensional trust aware cloud service selection mechanism is designed by Fan *et al.* (2014). The mechanism employs the Evidential Reasoning (ER) method, which integrates the reputation and perception-based trust. These values are computed from the indirect and direct trust evidences. The mechanism considers multiple factors which can affect the selection of the trustworthy services.

Chiregi and Navimipour (2016) presented a novel method for the identification of trusted cloud services. The study evaluates reputation values by considering accessibility, dependability, and ability parameters. The three-topological metrics, namely, out-degree, in-degree, and reputation measures have been used for the estimation of trust. However, the weights considered for three attributes are 0.3, 0.3, and 0.4, that is, without any recommendation or preferences provided by the cloud consumers. Moreover, the weights should be properly formalized using a standardized method.

c. Biological techniques

Li *et al.* (2011) designed a trust model which comprises of direct, initial, and recommendatory trust values of a service. The QoS values produce the initial trust value, the attenuation function produces the direct trust value on the basis of the historical successful and unsuccessful interaction times, and recommendation is computed by an improved cross generation, heterogeneous recombination, and cataclysmic mutation (CHC) genetic algorithm, in order to extract the trust paths. The total trust value is, then, gained by the computation of the initial, direct, and recommendatory values of the trust. The assumption considered in the study, however, seems vague, as the cloud consumers usually do not publish services. Therefore, the recommendation path is difficult to generate. A trust estimation model is proposed by Divakarla & Chandrasekaran (2016). The model considers resources as basic entities for transactions in cloud environment. Therefore, a trust value for building a trust path among cloud resources and a user is calculated using the family gene algorithm. The presented model, nonetheless, does not deal with the QoS values such as security, accessibility, and performance. The end users demand not only the availability of the cloud resources, but also anticipate that the services should conform to QoS and SLAs in order to meet the quality levels.

A hybrid method is proposed by Bharath & Sirriram (2017). The authors employed Genetically Modified Ant Colony Optimization technique to find the optimized parametric values. The degree of the trust between entities is shown as the pheromone concentration in Ant Colony Optimization. Hence, the users are able to choose the secure and optimal service since the ant selects the high concentration pheromone. Furthermore, the experiments are performed on CloudArmor dataset to highlight the accuracy of the proposed scheme. However, the method can be improved by including multiple attributes and sub-attributes of trust in order to

Table 3: Summary of the Trust Estimation Techniques (Feedback Frameworks)

References	Trust factors	Experiment patterns					Benefits	Limitations
		Simulations	Real data Set	Case Study	Comparativestudy	implementation		
Zheng *et al*., 2011	Not mentioned				✓		QoS predictions are based on similar users and items	Only one operation of web service is used for evaluation
Tserpes *et al*., 2012	SLA agreements, Cost					✓	usage of consumer ratings to select most appropriate service for specific consumer	lacks weighted rating techniques
Sun *et al*. (2013)	Not mentioned		✓				finds similar users more accurately and causes better QoS value Prediction	lacks the user preference consideration
Zheng *et al*., 2013	Response time, Throughput		✓				ranking prediction on past usage experience seems close to reality	uncertainty is not considered
Noor *et al*., 2013	Availability, Security Response time						handling of user preferences through feedback	conformance to the QoS values is neglected
Li & Du, 2013	Security, Reliability, Availability	✓					quality measurement according to user opinions	lacks the consideration of distributed data sharing
Wu *et al*., 2013	Reliability	✓					dynamic changes in trust degree are properly handled	uncertainty in the feedbacks is not handled
Qu *et al*., 2013	Availability, Elasticity, Response time, Cost			✓			filtration mechanism is used to handle the misleading feedbacks	objective assessment is neglected
Fan & Perros, 2013	Feedback reliability	✓					Produces results based on the filtered trust feedback	No ranking mechanism on user preferences
Ding *et al*., 2014	Response time, Throughput	✓					Service Utility computation to show user satisfaction	No considerations for uncertainty
Qu *et al*., 2015	Privacy, after-sales services, Availability, Response time	✓					Provides the context-aware credible cloud service evaluation mechanism	Ignores the hardware or VM related limitations
Filali & Yagoubi, 2015a	Power, Response time, Cost, Efficiency, Interoperability, Transparency, Reliability, Security	✓					Opinion model for the subjective and the performance parameters for the objective dimension	Security parameters are neglected
Pan *et al*., 2015	Response time, Throughput	✓					service selection or recommendation based on social network relationships	Neglects the service utility computation
Filali & Yagoubi, 2015b	Not mentioned	✓					The filtration of the ratings regarding the biased opinions	No real world experiments No similarity computation on similar requirements
Taneja *et al*., 2015	Not mentioned	✓					Monitor evaluation by the third party, Adaptable to the customer preferences	Lacks the ability to handle the malicious feedbacks
Machhi & Jethava, 2016	Not mentioned						Filtering of the malicious rating	No experiments
Emeakaroha *et al*., 2016	No explicit definition			✓	✓		Communication of detailed and up-to-date information to consumers	No experiments with end users

incorporate the various QoS. Table 4 provides a summary of the trust estimation by reputation-based and biological techniques.

4.4.2.2 Statistical and Probabilistic Methods

A Bayesian network-based trust-aware service selection model is designed by Hang *et al.* (2009). The Bayesian service selection model identifies the causal relationships between the services. The model empowers the consumers to interact with the services and then constructs and updates its local service composition model. The consumers may exchange referrals with each other. The model employs Root Mean Square Error (RMSE) and Maximum Likelihood Estimation (MLE) methods for trust estimation. The key focus of the presented model is the QoS values which are computed by without considering the end user preferences. A mathematical framework, which formulates the extension of the Bayesian inference standard application, in order to check the trustworthiness of the data is designed by Nevell *et al.* (2010). The framework quantifies the trustworthiness probability of the generic data and provides a view of an intelligent scenario. The presented trust model, however, does not consider the network-based shared resources for the estimation of trust values.

Hang and Singh (2011) designed a service selection method. The method employs the different composition operators for the computation of the trust values. The authors presented two distributed trust-aware service selection approaches. The first approach is based on the Bayesian networks and the second relies on the beta mixture model. The method can be applied to only one quality metric. In the distributed environments, such as cloud computing, it is not realistic assumption to consider only one quality metric. Wang *et al*. (2012) proposed a task scheduling model. The trust relationship among the computing nodes is built and trust for the nodes is computed by using Bayesian cognitive method. The trust estimation method, however, does not consider the preferences of users. Moreover, the calculation process of the trustworthiness of cloud computing nodes employs the self-selected values. The modeling of uncertainty is important in distributed systems for the selection of a resource from multiple options. Over the years, numerous studies have been carried out to examine the aspect of uncertainty in trust estimation. A probabilistic trustworthy web service selection models is proposed by Mehdi *et al.* (2012). The model figures out the web service trustworthiness by employing a probabilistic method on the basis of historical direct interactions with web services. The web service quality estimation is based on Multinomial Dirichlet Distribution (MDD), where probabilities of web services belong to predefined quality classes. The probabilistic relationships among the different variables are handled by Bayesian network. This model estimates the quality of a web service on the basis of predefined quality attributes. However, the presented approach fails to consider preferences specified by end users for trustworthiness estimation. Habib *et al.* (2014) proposed the architectural changes by introducing the registration manager and Consensus Assessment Initiative Questionnaires (CAIQ) module in order to compute the value of trust. The system estimates the trustworthiness of cloud service providers by employing the CAIQ assessment, and then results are converted into certain trust opinion representations. The

Table 4: Summary of the Trust Estimation Techniques (Reputation-Based & Biological Techniques)

References	Trust factors	Experiment patterns				Benefits	Limitations
		Real data Set	Synthetic	Case Study	Comparative study		
Li *et al*., 2011	Response time, Throughput, Availability, Accessibility, Interoperability, Cost		✓			Improved recommendation is made possible	Difficulty to generate recommendation path, uncertainty problem is not handled
Fan *et al*., 2014	Not mentioned					Accurately rank the service options	Uncertainty in the indirect trust
Divakarla & Chandrasekaran, 2016	Availability				✓	Efficient in handling the trust	Not all QoS parameters are considered
Chiregi & Navimipour, 2016	Accessibility, Dependability			✓		Provides the beneficial reputation estimations	Fixed weights are used, should be open for user
Xu *et al*., 2016	Response time, Throughput	✓				QoS prediction accuracy based on the context information	Not all QoS parameters are considered
Bharath & Sirriram , 2017	Security	✓				Reduces the complexity to compute trust score	Lacks user preferences

CAIQ assessment contains yes and no responses, given by cloud service providers. The user requirements, or utility assessments, can be considered in this approach for the better assessment of the trustworthiness of cloud services.

Another recent study models the service selection problem by employing the probability mass function of the fluctuating QoS values (Hwang *et al*., 2015). The proposed heuristic method aims to identify a set of atomic services in order to form a composite service, with the expectation of having the high probability of QoS which satisfy the user requirements. The method first divides global constraints into multiple local constraints; the optimal service selection is then carried out in accordance with local constraints. The experiments have been performed for three QoS attributes, namely, response time, reliability, and fidelity. Nevertheless, the execution time could be problematic in some cases, where multiple iterations are needed. This is more likely to happen in those situations when initial web service assignments do not yield the acceptable global QoS conformances.

Algamdi *et al*., (2017) proposed an infrastructure with cloud trust protocol capability that inquires about the assessments and computes the digital trust value. The digital trust is computed by extracting the user replies to MCQs using subjective logic operators and consensus. The overall method involves Cloud Trust Protocol, Consensus Assessment Initiative Questionnaire, trust aggregation and reputation mechanisms. However, the study lacks the mechanism to detect the malicious user and remove them before the evaluation of trust value.

Mohammed *et al*. (2018) presented a trust model for trust assessment. The model determines the percentage value of trust for cloud consumers using the operational parameters of requested service. Particle Swarm Optimization (PSO), Multiple Regression (MR), Analytic Hierarchical Process (AHP), and PSO-Multiple Regression (MR-PSO) techniques are employed. PSO is identified as the most appropriate method to estimate the trust value. The validity of proposed method is shown by experiments on cloud Armor dataset. Table 5 highlights the imperative aspects of the statistical and probabilistic methods.

4.4.2.3 Fuzzy Logic

The imprecise data are typically handled by employing the fuzzy logic methods. A cooperative society model-based system is presented by Bedi *et al.* (2012), which considers the user rights for trustworthy service selection on the basis of the recommendations of acquaintances. The system is combined with the multi-agent technology which employs Fuzzy Inference System (FIS) to manage uncertainty in recommendations.

Fan *et al*. (2014) developed a novel two stage fuzzy gap evaluation model to solve the trustworthy service selection decision problem. The model employs the evidential reasoning approach. The trustworthiness of cloud services is computed in terms of perception, delivery, and utility importance. The performance of the proposed model is studied through the experiments. However, the evaluation does not focus on the QoS compliance to SLAs, which can be argued as a key trustworthiness criterion. Gu *et al.* (2014) developed a fuzzy logic-based model, which considers the success and failure interactions of entities for the computation of trust. Hence, trust relationship is computed among cloud service providers and consumers with respect to their direct experiences. The trusted computing chain is extended from IaaS to PaaS layer, which ultimately affects the SaaS layer trust. The experiment and simulation results advocate the effectiveness of the model in fraud identification in the trust estimation process. Nevertheless, the proposed model can be improved by the inclusion of the values of cloud service customer preferred QoS attributes in the trust estimation process. A user-based service selection technique is identified by Ma *et al*. (2015). The user preferences are recognized by three different constituents, namely, trust, usage, and cost preferences. The dynamic fuzzy clustering method is employed for the service selection in conformity with user preferences. The experiment results have demonstrated the effectiveness of the proposed technique. However, the results of the method can be affected by the malicious user evaluations.

Kumar *et al*. (2016) developed a fuzzy-based trust management system for the trust value assignment to cloud service providers. The system considers the existing infrastructure of CSPs and their past reputations for the computation of trust value. The system consists of two main modules, viz., Registration Management Service (RMS) and Trust Management Service (TMS). The RMS handles cloud service provider registration, whereas the TMS, with the help of the feedback collector module, submits the required data to the fuzzy-based trust calculator to compute the values of trust factors. The trust factors include efficiency, performance, cost, adaptability, and security. The study considered feedback for the rust value estimation. Nonetheless, it does not

Table 5: Summary of the Trust Estimation Techniques (Statistical and Probabilistic Methods)

References	Trust factors	Experiment patterns			Benefits	Limitations
		Simulations	Synthetic data	Comparative study		
Hang *et al*., 2009	Not mentioned explicitly		✓		deals with the incomplete observations	Does not capture the requirements of the consumers
Nevell *et al*., 2010	Reliability		✓		Trust probability for generic data and provides view for intelligence scenario	Fails to estimate the trust value for the network based shared resources
Hang & Singh, 2011	Not mentioned explicitly	✓			Trust is estimated on the basis of direct and indirect experiences	Fails to handle the multiple quality metrics at a time
Mehdi *et al*., 2012	Not mentioned			✓	Captures the level of goodness or badness of a service	Fails to incorporate the user preferences
Wang *et al*., 2012	Reliability	✓			Reduces the failure probability of task	Lacks user preferred weightage
Habib *et al*., 2014	Not mentioned		✓		Cloud providers are able to specify their competencies and capabilities	No method to translate the user needs and wants, assess the partial inconsistencies
Hwang *et al*., 2015	Not mentioned explicitly		✓		locally optimal candidate service is identified for each task	High time complexity in the case of multiple iterations
Algamdi *et al*., 2017	Not mentioned				The computation of digital trust value	Possibility of opinion from malicious users
Mohammed *et al*., 2018	Not mentioned	✓			Identification of appropriate trust evaluation method	Lacks user preferences in trust computation

consider the cloud user preferences and service utility to rank the services according to the requirements of users. A hybrid multi-criteria decision model is presented to aggregate the user feedback and the assessment data to facilitate the process of cloud service selection (Alam & Ahmad, 2016). The model formulates the requirements by integrating the methodologies, namely, Fuzzy Analytic Hierarchy Process (FAHP), Fuzzy Delphi Methodology (FDM), Fuzzy TOPSIS, and Fuzzy Vikor. However, the performance of the model is neither analyzed through the experiments nor through simulations.

Selvaraj and Sundararajan (2017) focused on a dynamic trust evaluation scheme aimed at cloud services by employing the fuzzy logic. The authors offered an evidence-based mechanism to determine the trustworthiness by making the use of QoS parameters. Furthermore, the induced ordered weight averaging operator is employed to get the cumulative trust value. In a recent study, a smart cloud broker along with the Mapreduce framework has been presented (Nagarajan *et al*., 2018). MapReduce framework is used for preprocessing of feedback of QoS. Then a Fuzzy inference system is employed for broker to process the decision-making on generated feedback values and evaluation of trust value. The experiment result shows the improvement in service selection and trust level identification. Nevertheless, the framework has considered the QoS preferences of decision makers. A summarized view of these studies is provided in Table 6.

Table 6: Summary of the trust Estimation Techniques (Fuzzy Logic)

References	Trust factors	Experiment patterns			Benefits	Limitations
		Simulations	Real data Set	Case Study		
Bedi *et al*., 2012	Not mentioned specifically		✓		Successfully handles the uncertainty in recommendations	QoS factors are ignored to assess the quality
Fan *et al*., 2014	Not mentioned specifically			✓	Generation of the belief structure	No QoS compliance to SLAs
Gu *et al*., 2014	Response time	✓			Computation of direct trust relationship	No way to include the user needs
Ma *et al*., 2015	Reliability, Security, Availability, Efficiency, Maintainability, Portability	✓			Recognition of the user preferences	Malicious user evaluations are not handled
Kumar *et al*., 2016	Performance Cost, Adaptability, Security	✓			Helps to identify a trustworthy provider	Fails to include user preferences
Alam & Ahmad, 2016	Not mentioned specifically				Fuzziness of the feedback is handled	Incomplete modeling
Selvaraj & Sundararajan, 2017	QoS parameters	✓			Dynamic evaluation of trust value	Lacks user preferences
Nagarajan *et al*., 2018	QoS Factors		✓		Preprocessing of feedback to resolve inconsistencies	Lacks decision maker preferences
Lu & Yuan, 2018	QoS		✓		Usage of entropy weight to decrease the false parameter effects	Lacks dynamic trust evaluation

4.4.2.4 Multi-criteria Decision Making

Multiple criteria decision making (MCDM) is a method to facilitate the decision making process by considering the multiple conflicting criteria (Eisa *et al*., 2016). The MCDM techniques can be broadly classified into Multi-attribute trustworthiness and Analytical Hierarchy Process (AHP)-based techniques. The characteristics of the studies included in this section are summarized in Table 7.

a. Multi-attribute Trustworthiness

Habib *et al*. (2011) designed a multiaspect trust management system for cloud services. The system reflects multiaspect nature of trust calculation process by considering resources, multiple attributes, and roots of trust. The system employs user statements and property certificate parameters for the computation of trust. The estimated values are, however, computed without considering the uncertainty of opinions.

Saripalli and Pingali (2011) designed a Simple Additive Weighting (SAW) method to rank alternative cloud services. The hierarchy of six attribute tuples forms the service selection criteria. Moreover, a modified Wide-band Delphi computation method is presented to find comparative weighting values for attributes according to the workload of CSPs. These weights are then used to compute the relative ranks. The SAW method is employed for the value function generation. However, the ranking accuracy is not compared with

Table 7: Summary of the Trust Estimation Techniques (Multi-Criteria Decision Making)

References	Trust factors	Experiment patterns					Benefits	Limitations
		Real data Set	Synthetic Data	Case Study	Comparative study	implementation		
Habib *et al*., 2011	Not mentioned						Trust estimation by multiple attributes	opinions uncertainty is not handled
Saripalli & Pingali, 2011	Not mentioned						Comparative weighting values for the attributes per workload	No comparisons
Garg *et al*., 2011	Accountability, Agility, Cost, Performance, Security, Privacy, Usability			✓			CSMIC defined key performance indicators are used	No standardized weight assignment procedure
Garg *et al*., 2012	Accountability, Agility, Cost, Performance, Security, Privacy, Usability			✓			creates a strong competition among service providers	Variations in QoS attributes are not considered
Sun *et al*., 2013	Response time, Throughput, Availability, Reliability, Cost			✓			transforming qualitative preference of users into quantitative numeric weights	SLA conformance with QoS is not considered
Wang & Wu, 2014	Common factors: Feedback rating, Time, recommendation, Friendship, Risk, Special factors: Speed, Capability, Availability, Security	✓					uncertainty of a random variable is controlled	Consumer preferences are over looked
Ding *et al*., 2014	Response time, Throughput					✓	Missing value prediction	Missing QoS factors
Ma *et al*., 2016	Service cost, risks				✓		Risk sensitive service selection with performance consideration	Lacks other important factors of QoS
Singh & Sidhu, 2017	Compliance to SLA		✓				Performance monitoring and compliance evaluation	Lacks the timeliness and propagation handling of trust
Li *et al*., 2016	Not specified	✓					Service controllability	Lacks user preferences for weights
Hajizadeh & Navimipour, 2017	availability, reliability, interaction evolution and identity					✓	Better reliability and availability than QoS-based models	Only four parameters are considered, Decrease in reliability with the increase in service groups
Alhanahnah *et al*., 2018	Not mentioned explicitly			✓			User preferences are considered	Chances of uncertainties

other ranking methods. A framework has been designed to develop measurable trust metrics by employing entropy with the unified scale (Wang & Wu, 2014). The multi-criteria analysis approach is employed for the estimation of trust factors. Nevertheless, the trust factors have not captured the essence of the preferences of consumers.

Ding *et al.* (2014) proposed a personalized service selection method which employs enhanced item-based collaborative filtering approach. Moreover, the Pearson Correlation Coefficient (PCC) method has been used for the evaluation of the recommendation system. The imputation of the missing data is carried out to facilitate the personalized selection of cloud services. However, only two QoS parameters, namely, the response time

and the throughput have been considered for the trust estimation. A time series analysis approach, combined with the Interval Neutrosophic Set (INS) theory, is proposed to solve the MCDM service ranking problem (Ma *et al*., 2016). The developed ranking method is named as Cloud Service Interval Neutrosophic Set (CINS). The problems addressed in the study are the fluctuating QoS service cost, potential risks with tradeoffs among potential risks, and performance costs. The performance of the method is analyzed through a comparative analysis. The study, nevertheless, does not consider the QoS factors and it is only focused on the performance of cloud services. Hajizaeh and Navimipour proposed a method to evaluate the trust of service providers by employing the behavioral graphs (Hajizadeh & Navimipour, 2017). The trust evaluation is made on the basis of availability, reliability, interaction evolution, and identity. The method is evaluated by implementing simulator in terms of precision, error hit, availability, and reliability. The results show better reliability and availability as compared to QoS-based models. However, the study is limited to only four parameters. Furthermore, the number of groups has inverse relation with reliability which limits the performance of the proposed method when the number of groups increases.

b. Analytical Hierarchy Process

Garg *et al*. (2011) presented an Analytical Hierarch Process (AHP) framework to rank cloud services. The framework attempts to evaluate cloud services by employing multiple Key Performance Indicators (KPIs) which have been defined by Cloud Services Measurement Initiative Consortium (CSMIC) (2011). The ranking procedure is comprised of three steps, namely, decomposition, priority aggregation, and priority judgment. The first step involves the identification of the hierarchical structure. The second step performs pairwise comparisons. Finally, the third phase determines the ranks of cloud services. Nevertheless, the weight assignment to QoS need to be adjusted according to the requirements of user needs to empower them to select the suited cloud services.

Garg *et al.* (2012) advocated that multiple services with same functionality, but with different quality attributes, are generally available for selection. Therefore, a framework has been presented to measure the service quality for cloud service ranking using the AHP method. The presented framework creates a healthy competition among service providers in order to fulfill their SLAs with the improvements in QoS. Nonetheless, the framework has not considered variations in the performance and security levels in the process of cloud service ranking. The preferences of individual and multiple users are considered by a consumer centered service selection method (Sun *et al*., 2013). The method considers pre-defined QOS criteria which is based on throughput, response time, reliability, availability, and cost with comparison metrics which are defined by consumers. However, the trustworthiness evaluation values do not depict the direct interaction experiences of users. Moreover, the results do not validate the conformance of SLA and QoS. Singh & Sidhu (2017) presented a trust evaluation framework based on the compliance monitoring mechanism. An improved Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) along with AHP is employed to

process the compliance and to find the trust. The authors claimed that Cloud Auditor interim as a third-party aid trust via monitoring of QoS and SLAs. However, the transparency can be increased by having a separate control point other than CA so that the standardized Cloud SLAs can be adopted.

Li *et al.* (2016) proposed a scheme of service selection that computes trust on the basis of Analytic Hierarchy Process (AHP) using service attribute weights and data delivery. The results are produced from an instance and synthetic data which showed the effectiveness of the scheme for service selection. Recently, a novel TOPSIS trust evaluation system, with the combination of objective and subjective feature, is introduced by Lu and Yuan (2018). The objectivity of services is considered based on the QoS source reliability and usage of entropy weight to decrease the false parameter effects. Furthermore, the preferences for trust are considered to implement the subjectivity. The feasibility and effectiveness of the study is demonstrated by experiments on the real web services datasets. However, the study can be improved by dynamic trust evaluation mechanisms. A trust framework Context-Aware Multifaceted Trust (CAMTF) for the trust evaluation of service providers is proposed by Alhanahnah *et al*., (2018). The mathematical techniques AHP and Fuzzy Simple Additive Weighting with the characteristics of services, perspective of user, and trust factors are employed. The existing standards and user preferences are also considered. The method has the capability to adapt diverse contexts. The applicability of the study is validated through a practical case study. However, the chances of uncertainties are not controlled. Furthermore, the security concerns are also overlooked by authors.

4.4.2.5 Algorithmic Solutions

Liu *et al.* (2012) presented a three-layered hierarchical structure. The optimal service selection job is carried out in the first layer functionality, the criterion is selected in the second layer functionality, and the nine additional QoS parameters are chosen in the third layer functionality. The criterion is based on security, timeliness, and stability parameters. The utility function is employed to derive an objective function. The theoretical analysis and experiment results have been provided to show that the optimal solution can be computed by the algorithm. Nevertheless, the algorithm can be improved by incorporating the enterprise business process collaboration in the context of specific users in cloud computing environment.

Ding *et al.* (2014) presented a method which considers historical records of cloud service performances for service recommendation. These records formally standardize multi-attribute comparisons among cloud user demands and service provider solutions. The method is based on a resource matching algorithm which considers the functional and non-functional (that is, QoS) attributes for the recommendation of resources. The algorithm integrates, group customer estimation, a multi-attribute comparison metric, and price utility in the recommendation process. The algorithm, however, lacks a formalized mechanism to perform the mapping of the trusted SaaS specifications and QoS requirements of the users.

Rathi *et al.* (2015) formulated a user trust model, based on the algorithmic specifications, to find trust

parameters in cloud environment. The ten parameters, namely, transparency, data location, data safety, data distribution, accessibility, data access privileges, backup and recovery, compliance to audits and certifications, work longevity, and timely user acceptance to changes have been selected and surveyed among cloud users estimate the trust value of cloud services. Jrad *et al*. (2015) designed and analyzed a utility-based matching algorithm. The algorithm focuses on an automatic matching procedure, which is developed to check the conformance of cloud providers with cloud user requirements. The utility-based matching algorithm and Sieving algorithm have been implemented to compare their performance. The development of a utility-based algorithm enables the profit maximization of cloud users. Some additional components have also been developed to monitor SLA and deployment management issues. Nevertheless, the selection strategy only considers objective quality parameters. The subjective parameters such as the security concerns cannot be overlooked in the process of trust estimation for cloud services. Table 8 provides the summary of studies that focus on algorithmic solutions.

The systematic literature review, in the context of trust estimation techniques in cloud services, has shown that a significant portion of the literature has been focused on user experience-based mathematical or statistical frameworks. A few statistical methods-based approaches have been proposed to predict QoS to better satisfy consumer requirements. A relatively less number of studies have considered the preferences of consumers and tried to integrate them into the service selection process. Fig. 9 (a) provides a percentage-wise view of the cloud trustworthiness techniques. Fig. 9 (b), on the other hand, depicts the number of papers per class view of the related literature. Finally, Fig. 9 (c) shows the citation of papers in each class.

Table 8: Summary of the Trust Estimation Techniques (Algorithmic Solutions)

References	Trust factors	Experiment patterns		Benefits	Limitations
		Simulations	Synthetic Data		
Liu *et al*., 2012	Security, Timeliness, Stability		✓	Flexibility in specifying constraints	Lacks real time cloud experiment
Ding *et al*., 2014	Not mentioned	✓		Enables multi-attribute comparisons of solutions and user need	No standardized mapping
Rathi *et al*., 2015	Transparency, data location, data safety, data distribution, accessibility, data access, backup and recovery, compliance to audits and certifications, workability, user acceptance to timely changes	✓		Trust evaluation on both the functional and QoS attributes	Lacks flexibility
Jrad *et al*., 2015	Response time, Throughput, Availability	✓		Enables the automatic matching procedure to map the user needs with the provider solutions	Only valid for the objective quality parameters

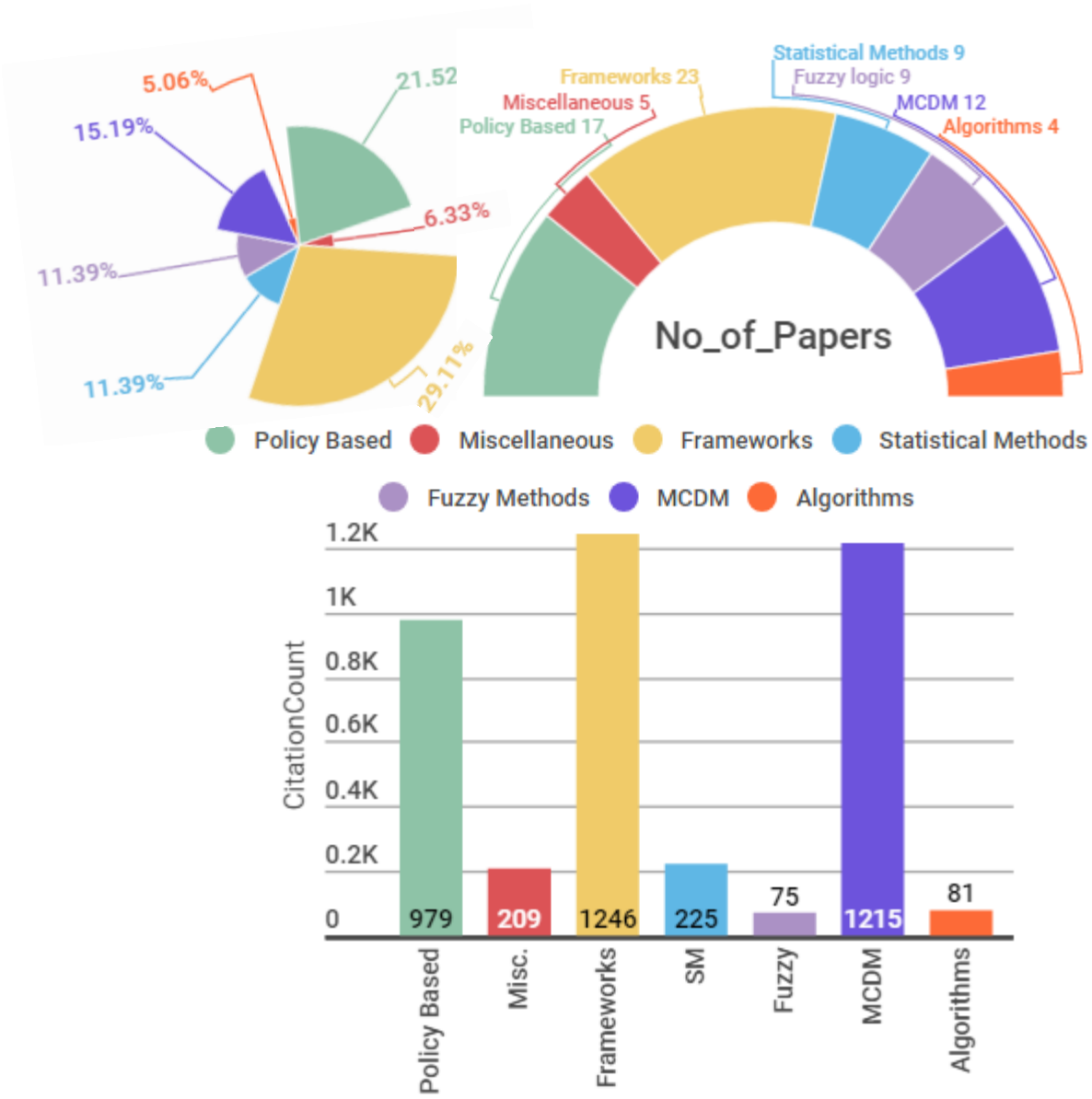


Fig. 9. (a) The cloud trustworthiness techniques, (b) the number of papers in each class, and (c) the citation of papers in each class

5. Research Directions

The cloud computing paradigm has been recently widely adopted in the wide range of business applications due to its ability to drive down business costs and to avoid large capital expenditures. The adoption of the plethora of cloud computing applications is, however, highly dependent on the trust of consumers on cloud services. Over the years, the research community has presented a number of methods for the establishment and estimation of trust. Nevertheless, there are still several potential avenues which can be further explored. The elucidation of these research directions has been presented in this section in order to address Q5.

- *Trust Transparency for Domain-Specific Solutions:* The trust transparency, unlike security and other non-functional requirements, is one of the least explored research domains in the existing literature. Most of the existing trust models are either non-transparent to users or lack the ability to consider consumer preferences on nonfunctional requirements. The cloud service selection process is thus required to be improved according to the domain-specific needs of users.
- *Utility of Cloud Services:* The goal of cloud users, as decision makers, is to maximize the utility of cloud services. The utility of a cloud service can be formulated and then analyzed through the cardinal and ordinal utilities. The former can be employed for the analysis of relative ranking, whereas the latter can be used for studying absolute ranking. The objective functions can then be formulated to maximize the utility of cloud services.
- *Bio-Inspired Methods:* A relatively recent tendency of the research community is to employ the bio-inspired methods such as Bees algorithms (Firdhous *et al*., 2011) for the establishment and computation of trust in cloud services. A number of other nature-inspired algorithms, namely, firefly, flower pollination, cuckoo search, ant colony, and others can also be employed to mimic the behavior of living organisms in studying the trustworthiness problem in cloud services.
- *Trust in Mobile Cloud Computing:* The integration of mobile applications and cloud computing technology has realized the concept of a cross cutting technology, namely, Mobile Cloud Computing (MCC). The establishment of trust is more challenging in MCC unlike traditional cloud computing where cloud users tend to establish trust on large organizations which are already conscious about their reputation. The methods for the establishment of trust on cloud services running on cloudlets, on the other hand, need to integrate the mutual authentication mechanisms with trust management schemes to empower users to use trustworthy cloud services.
- *Higher-Order Statistics:* A significant portion of the existing literature is based on simple multivariate analysis. The higher order statistics, as used in skewness and kurtosis of the distributions of the past interactions of users with cloud service, have not been considered in formulation and analysis of trust evaluation methods in cloud services. The study of analyzing the impact of integrating the long term variations in the trust establishment and estimation of cloud services by means of higher order statistics in conjunction with the covariance and correlation methods may yield some novel results.
- *Evidence-based Trust:* In interactive environments, the value of trust is perceived by a user on the basis of its interaction with others. The popularity of online markets, online social interactions, and service-oriented computing demands evidence aiding in decision-making. The values of related set of attributes of a service can be used as evidences that are desirable to predict the expectancy of user.

6. Conclusions

This study has provided a detailed analysis of methods, techniques, and frameworks from 79 studies which have been published during 2010 to 2018. The related literature is classified into two broad classes, namely, the trust establishment and trust estimation. These classes are then further classified into two and five subclasses, respectively (as shown in Fig. 9 (a) and (b)). The analysis shows that the most researched subclass is the trust estimation frameworks (29.11%) and the least applied are the algorithmic solutions (5.06%). On the other hand, the citation count result shows the interest of researchers in the trust estimation frameworks and MCDM techniques (as depicted in Fig. 9 (c)).

The 9 different QoS parameters, on the basis of their popularity as trust factors in the literature since 2010, have been chosen for the analysis. The analysis indicates that the security is the most repeated trust factor (24%), among total 101 repetitions, being included in the 24 studies. We can conclude from the findings of this study that the trustworthiness of cloud services is highly dependent on the QoS factors, namely, security (24%), response time (22%), availability (15%), reliability (12%), cost (10%), throughput (9%), accessibility (5%), integrity (2%), and scalability (1%) in their given order, which also addresses Q2. These results are depicted in Fig. 10 (a) and (b).

The literature review shows that there are a number of research domains which have not yet been fully explored. The exploration of research domains, namely, trust transparency for domain-specific solutions, utility of cloud services, bio-inspired methods, trust in mobile cloud computing, and higher-order statistics have a potential to yield new findings in the domain of trustworthiness of cloud services.

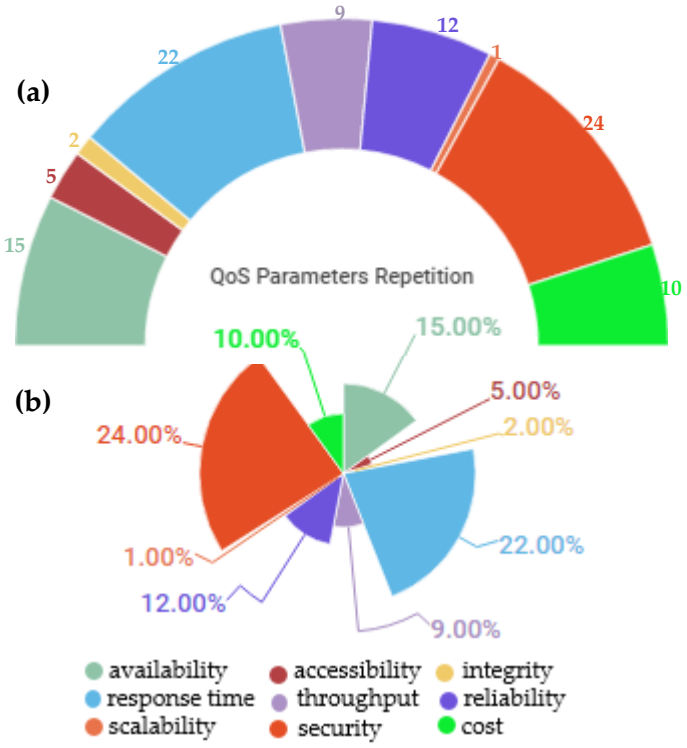


Fig. 10. (a) the number of repetition of QoS parameters and (b) the repetition percentage of the QoS parameters.

References

Abbadi, I. M., & Alawneh, M. (2012). A framework for establishing trust in the cloud. *Computers & Electrical Engineering*, 38(5), 1073-1087.

Abbadi, I. M., & Martin, A. (2011). Trust in the cloud. *Information Security Technical Report*, 16(3–4), 108–114.

Abdallah, E. G., Zulkernine, M., Gu, Y. X., & Liem, C. (2017). TRUST-CAP: A Trust Model for Cloud-Based Applications. In *IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, 2, 584-589.

Abdul-Rahman, A., & Hailes, S. (2000). Supporting trust in virtual communities. In *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, 9.

Abrams, M. D., & Joyce, M. V. (1995). Trusted system concepts. *Computers & Security*, *14*(1), 45-56.

Alam, K., & Ahmad, R. (2016). A Hybrid Fuzzy Multi-Criteria Decision Model for Cloud Service Selection and Importance Degree of Component Services. *Knowledge Engineering and Decision Making, Proceedings of the 12th International FLINS Conference*, 334-340.

Algamdi, A., Coenen, F., & Lisitsa, A. (2017). A trust evaluation method based on the distributed Cloud Trust Protocol (CTP) and opinion sharing. *Provider*, *5*(17), 18.

Alhanahnah, M., Bertok, P., Tari, Z., & Alouneh, S. (2018). Context-Aware Multifaceted Trust Framework for Evaluating Trustworthiness of Cloud Providers. *Future Generation Computer Systems*, *79*, 488-499.

Aljoumah, E., Al-Mousawi, F., Ahmad, I., Al-Shammri, M., & Al-Jady, Z. (2015). SLA in cloud computing architectures: A comprehensive study. *International Journal of Grid Distribution Computing*, 8(5), 7-32.

Anakath, A. S., Rajakumar, S., & Ambika, S. (2017). Privacy preserving multi factor authentication using trust management. *Cluster Computing*, 1-7.

Anisetti, M., Ardagna, C. A., & Damiani, E. (2014). A certification-based trust model for autonomic cloud computing systems. In *IEEE International Conference on Cloud and Autonomic Computing (ICCAC)*, 212-219.

Anisetti, M., Ardagna, C., Damiani, E., & Gaudenzi, F. (2017). A semi-automatic and trustworthy scheme for continuous cloud service certification. *IEEE Transactions on Services Computing*.

Anisetti, M., Ardagna, C. A., Damiani, E., Gaudenzi, F., & Veca, R. (2015). Toward security and performance certification of open stack. *In IEEE 8th International Conference on Cloud Computing (CLOUD)*, 564-571.

Balasubramanian, M., & Kim, H. (2017). Trust Evaluation Scheme for Cloud Data Security using Fuzzy based Approach. *International Journal of Applied Engineering Research*, *12*(13), 3908-3913.

Bedi, P., Kaur, H., & Gupta, B. (2012). Trustworthy service provider selection in cloud computing environment. *Proceedings - International Conference on Communication Systems and Network Technologies*, 714–719.

Bharath, J., & Sriram, V. S. (2017). Genetically Modified Ant Colony Optimization based Trust Evaluation in Cloud Computing. *Indian Journal of Science and Technology*, *9*(48).

Bianco, P., Lewis, G. A., & Merson, P. (2008). Service level agreements in service-oriented architecture environments. *Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst*, No. CMU/SEI-2008-TN-021.

Burkon, L. (2013). Quality of service attributes for software as a service. *Journal of Systems Integration*, 4(3), 38.

Buyya, R., Shin, C., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6), 599–616.

Cahill, V., Gray, E., Seigneur, J. M., Jensen, C. D., Chen, Y., Shand, B., & Wagealla, W. (2003). Using trust for secure collaboration in uncertain environments, *Pervasive Computing*, 2 (3), 52 – 61.

Carbone, M., Nielsen, M., & Sassone, V. (2003). A formal model for trust in dynamic networks. In *IEEE Proceedings First International Conference on Software Engineering and Formal Methods*, 54-61.

Chakraborty, S., & Roy, K. (2012). An SLA-based framework for estimating trustworthiness of a cloud. *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 937-942.

Chiregi, M., & Navimipour, N. J. (2016). Trusted services identification in the cloud environment using the topological metrics. *Karbala International Journal of Modern Science*, 2(3), 203–210.

Cimato, S., Damiani, E., Zavatarelli, F., & Menicocci, R. (2013). Towards the certification of cloud services. In *IEEE Ninth World Congress on Services (SERVICES)*, 92-97.

Cloud Armor. The Project Website. URL: http://cs.adelaide.edu.au/~cloudarmor

Cloud Service. Measurement Index Consortium (CSMIC), SMI framework. URL: http://betawww. cloudcommons.com/servicemeasurementindex.

Darwish, N. R., Mohamed, R. E., & Elsayed, D. H. (2015). A Proposed Approach for Monitoring Quality of Web Services Using Service Level Agreement. *International Journal of Computer Science and Information Security*, 13(1), 29.

Ding, S., Xia, C. Y., Zhou, K. Le, Yang, S. L., & Shang, J. S. (2014). Decision support for personalized cloud service selection through multi-attribute trustworthiness evaluation. *PLoS ONE*, 9(6), 1–11.

Ding, S., Xia, C., Cai, Q., Zhou, K., & Yang, S. (2014). QoS-aware resource matching and recommendation for cloud computing systems. *Applied Mathematics and Computation*, 247, 941–950.

Ding, S., Yang, S., Zhang, Y., Liang, C., & Xia, C. (2014). Combining QoS prediction and customer satisfaction estimation to solve cloud service trustworthiness evaluation problems. *Knowledge-Based Systems*, 56, 216–225.

Divakarla, U., & Chandrasekaran, K. (2016). Trusted path between two entities in Cloud. In *Cloud System and Big Data Engineering (Confluence), 6th International Conference*, 157-162.

Dorey, P. G., & Leite, A. (2011). Commentary: Cloud computing - A security problem or solution? *Information Security Technical Report*, 16(3–4), 89–96.

El-Gazzar, R. F. (2014, June). A literature review on cloud computing adoption issues in enterprises. In Springer *International Working Conference on Transfer and Diffusion of IT*, 214-242.

El-Gazzar, R., Hustad, E., & Olsen, D. H. (2016). Understanding cloud computing adoption issues: A Delphi study approach. *Journal of Systems and Software*, *118*, 64-84.

Eisa, M., Younas, M., Basu, K., & Zhu, H. (2016, March). Trends and Directions in Cloud Service Selection. In *2016 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 423-432.

Emeakaroha, V., Fatema, K., Vanderwerff, L., Healy, P., Lynn, T., & Morrison, J. (2016). A Trust Label System for Communicating Trust in Cloud Services. *IEEE Transactions on Services Computing*.

Eymann, T., König, S., & Matros, R. (2008). A framework for trust and reputation in grid environments. *Journal of Grid Computing*, *6*(3), 225-237.

Fan, W., & Perros, H. (2013). A reliability-based trust management mechanism for cloud services. *Proceedings - 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2013*, 1581–1586.

Fan, W., Yang, S., & Pei, J. (2014). A novel two-stage model for cloud service trustworthiness evaluation. *Expert Systems*, 31(2), 136–153.

Fan, W.-J., Yang, S.-L., Perros, H., & Pei, J. (2014). A multi-dimensional trust-aware cloud service selection mechanism based on evidential reasoning approach. *International Journal of Automation and Computing*, 12(2), 208–219.

Filali, F. Z., & Yagoubi, B. (2015a). Global Trust: A Trust Model for Cloud Service Selection. *International Journal of Computer Network and Information Security*, 7(5), 41–50.

Filali, F. Z., & Yagoubi, B. (2015b). Classifying and filtering users by similarity measures for trust management in cloud environment. *Scalable Computing*, 16(3), 289–302.

Firdhous, M., Ghazali, O., & Hassan, S. (2011). Applying Bees Algorithm for Trust Management in Cloud Computing. *Bio-Inspired Models of Networks, Information, and Computing Systems: 6th International ICST Conference*, 224 – 229.

Frey, S., Reich, C., & Lüthje, C. (2013, September). Key performance indicators for cloud computing SLAs. In *The Fifth International Conference on Emerging Network Intelligence, EMERGING*, 60-64.

Garg, S. K., Versteeg, S., & Buyya, R. (2011). SMICloud: A framework for comparing and ranking cloud services. *Proceedings - 2011 4th IEEE International Conference on Utility and Cloud Computing*, 210–218.

Garg, R., & Stiller, B. (2015). Factors Affecting Cloud Adoption and Their Interrelations. In *Closer*, 87-94.

Garg, S. K., Versteeg, S., & Buyya, R. (2012). A framework for ranking of cloud computing services. *Future Generation Computer Systems*, 29(4), 1012–1023.

Ghosh, N., Ghosh, S. K., & Das, S. K. (2015). SelCSP: A framework to facilitate selection of cloud service providers. *IEEE Transactions on Cloud Computing*, 3(1), 66-79.

Grabner- Kräuter, S. (2009). Web 2.0 social networks: The role of trust. *Journal of Business Ethics*, 90, 505 –522.

Grabner-Kräuter, S., & Bitter, S. (2015). Trust in online social networks: A multifaceted perspective. *Forum for Social Economics*, Vol. 44, No. 1, pp. 48-68.

Gu, L., Wang, C., Zhang, Y., Zhong, J., & Ni, Z. (2014). Trust Model in Cloud Computing Environment Based on Fuzzy Theory. *International Journal of Computers Communications & Control*, 9(5), 570-583.

Guo, S., & Xu, H. (2012). A non-interactive secure outsourced computation scheme in multi-party cloud. *Proceedings of the 2012 4th International Conference on Intelligent Networking and Collaborative Systems*, 15–19.

Gupta, P., Seetharaman, A., & Raj, J. R. (2013). The usage and adoption of cloud computing by small and medium businesses. *International Journal of Information Management*, *33*(5), 861-874.

Habib, S. M., Ries, S., & Muhlhauser, M. (2011). Towards a Trust Management System for Cloud Computing. *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, 933–939.

Habib, S.M., Ries, S., Mühlhäuser, M., & Varikkattu, P. (2014). Towards a Trust Management System for Cloud Computing Marketplaces: Using CAIQ as a Trust Information Source. *Security and Communication Networks*, 7(11), 2185-2200.

Hajizadeh, R., & Jafari Navimipour, N. (2017). A method for trust evaluation in the cloud environments using a behavior graph and services grouping. *Kybernetes*, 46(7), 1245-1261.

Handoko, B. L., Widuri, R., & Sarjono, H. (2017). The effect of third party auditor and quality of service through cloud storage security to cloud user trust. *In IEEE 9th International Conference on Communication Software and Networks (ICCSN)*, 1397-1401.

Hang, C. W., & Singh, M. P. (2011). Trustworthy service selection and composition. *ACM Transactions on Autonomous and Adaptive Systems*, 6(1), 5.

Hang, C. W., & Singh, M. P. (2009). Selecting trustworthy service in service-oriented environments. *The 12th AAMAS Workshop on Trust in Agent Societies*, 1-12.

Harbajanka, S., & Saxena, P. (2016). Security Issues and Trust Management in Cloud Computing. In *Proceedings of the ACM Symposium on Women in Research*, 1-3.

Haug, K. C., Kretschmer, T., & Strobel, T. (2016). Cloud adaptiveness within industry sectors–Measurement and observations. *Telecommunications Policy*, 40(4), 291-306.

Heilig, L., & Voß, S. (2014). Decision analytics for cloud computing: a classification and literature review. *Tutorials in Operations Research–Bridging Data and Decisions*, 1-26.

Hsu, P. F., Ray, S., & Li-Hsieh, Y. Y. (2014). Examining cloud computing adoption intention, pricing mechanism, and deployment model. *International Journal of Information Management*, 34(4), 474-488.

Huang, J., & Nicol, D. M. (2013). Trust mechanisms for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, 2(1), 9.

Hwang, S. Y., Hsu, C. C., & Lee, C. H. (2015). Service selection for web services with probabilistic QoS. *IEEE Transactions on Services Computing*, 8(3), 467-480.

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision support systems*, *43*(2), 618-644.

Jrad, F., Tao, J., Streit, A., Knapper, R., & Flath, C. (2015). A utility-based approach for customized cloud service selection. *International Journal of Computational Science and Engineering*, 10(1/2), 32.

Jula, A., Sundararajan, E., & Othman, Z. (2014). Cloud computing service composition: A systematic literature review. *Expert Systems with Applications*, 41(8), 3809–3824.

Katopodis, S., Spanoudakis, G., & Mahbub, K. (2014). Towards hybrid cloud service certification models. In *IEEE International Conference on Services Computing (SCC)*, 394-399.

Kaur, P., & Singh, H. (2015). An Analytical Review of Quality Attributes of Service-Oriented Architecture. *Trends in Information Management*, 10(1).

Khan, K. M., & Malluhi, Q. (2010). Establishing trust in cloud computing. *IT Professional*, *12*(5), 20–27.

Khan, K. S., Kunz, R., Kleijnen, J., & Antes, G. (2003). Five steps to conducting a systematic review. *Journal of the Royal Society of Medicine*, 96(3), 118–121.

Kim, H., Lee, H., Kim, W., & Kim, Y. (2010). A trust evaluation model for QoS guarantee in cloud systems. *International Journal of Grid and Distributed Computing*, 3(1), 1-10.

Ko, R. K., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., & Lee, B. S. (2011). TrustCloud: A framework for accountability and trust in cloud computing. *2011 IEEE World Congress on Services*, 584–588.

Ko, R. K., Lee, B. S., & Pearson, S. (2011). Towards achieving accountability, auditability and trust in cloud computing. In *International Conference on Advances in Computing and Communications*, *Springer*, 432-444.

Krotsiani, M., Spanoudakis, G., & Mahbub, K. (2013). Incremental certification of cloud services. In *SECURWARE7th International Conference on Emerging Security Information, Systems and Technologies*, 72-80.

Kuehnhausen, M., Frost, V. S., & Minden, G. J. (2012). Framework for assessing the trustworthiness of cloud resources. *2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, 142–145.

Kumar, S., Mittal, S., & Singh, M. (2016). Fuzzy Based Trust Management System for Cloud Environment. *Advances in Science and Technology Research Journal*, 10(30), 32–37.

Li, B., Cao, B. Q., Wen, K. M., & Li, R. X. (2011). Trustworthy assurance of service interoperation in cloud environment. *International Journal of Automation and Computing*, 8(3), 297–308.

Li, X., & Du, J. (2013). Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing. *Information Security, IET*, 7(1), 39–50.

Li, X., Liang, H., & Zhang, X. (2016). Trust Based Service Selection in Cloud Computing Environment. *International Journal of Smart Home*, *10*(11), 39-50.

Lin, A., & Chen, N. C. (2012). Cloud computing as an innovation: Perception, attitude, and adoption. *International Journal of Information Management*, *32*(6), 533-540.

Lins, S., Grochol, P., Schneider, S., & Sunyaev, A. (2016). Dynamic certification of cloud services: Trust, but verify!. IEEE Security & Privacy, 14(2), 66-71.

Lins, S., Schneider, S., & Sunyaev, A. (2016). Trust is good, control is better: Creating secure clouds by continuous auditing. *IEEE Transactions on Cloud Computing*.

Liu, M., Wang, M., Shen, W., Luo, N., & Yan, J. (2012). A quality of service (QoS)-aware execution plan selection approach for a service composition process. *Future Generation Computer Systems*, 28(7), 1080–1089.

Lu, L., & Yuan, Y. (2018). A Novel TOPSIS Evaluation Scheme for Cloud Service Trustworthiness Combining Objective and Subjective Aspects. *Journal of Systems and Software*.

Ma, H., & Hu, Z. gang. (2015). User preferences-aware recommendation for trustworthy cloud services based on fuzzy clustering. *Journal of Central South University*, 22(9), 3495–3505.

Ma, H., Hu, Z., Li, K., & Zhang, H. (2016). Toward trustworthy cloud service selection: A time-aware approach using interval neutrosophic set. *Journal of Parallel and Distributed Computing*, 96, 75–94.

Machhi, S., & Jethava, G. B. (2016). Feedback based Trust Management for Cloud Environment. *In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, 114.

Manuel, P. (2015). A trust model of cloud computing based on Quality of Service. *Annals of Operations Research*, 233(1), 281–292.

Manuel, P. D., Selvi, S. T., & Abd-El Barr, M. I. (2009). Trust management system for grid and cloud resources. In *IEEE First International Conference on Advanced Computing, ICAC*, 176-181.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision support systems*, *51*(1), 176-189.

Meera, G., & Geethakumari, G. (2015). A provenance auditing framework for cloud computing systems. *In IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES)*, 1-5.

Mehdi, M., Bouguila, N., & Bentahar, J. (2012). Trustworthy web service selection using probabilistic models. *Proceedings - 2012 IEEE 19th International Conference on Web Services, ICWS 2012*, 17–24.

Mehdi, M., Bouguila, N., & Bentahar, J. (2016). Trust and reputation of web services through QoS correlation lens. *IEEE Transactions on Services Computing*, *9*(6), 968-981.

Mei, S., Liu, C., Cheng, Y., Wu, J., & Wang, Z. (2013). TETPA: A case for trusted third party auditor in Cloud environment. In IEEE *Conference Anthology*, 1-4.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *NIST Special Publication*, 145, 7.

Mohammed, A. M., Morsy, E. I., & Omara, F. A. (2018). Trust model for cloud service consumers. In *IEEE International Conference on Innovative Trends in Computer Engineering (ITCE)*, 122-129.

Muchahari, M. K., & Sinha, S. K. (2013). A Survey on Web Services and Trust in Cloud Computing Environment. *National Workshop on Network Security*, 1-13.

Nagarajan, R., Thirunavukarasu, R., & Shanmugam, S. (2018). A Fuzzy-Based Intelligent Cloud Broker with MapReduce Framework to Evaluate the Trust Level of Cloud Services Using Customer Feedback. *International Journal of Fuzzy Systems*, *20*(1), 339-347.

Nevell, D. a, Maskell, S. R., Horridge, P. R., & Barnett, H. L. (2010). Fusion of data from sources with different levels of trust. *13th International Conference on Information Fusion*, 1–7.

Noor, T. H., Sheng, Q. Z., Ngu, A. H. H., Alfazi, A., & Law, J. (2013). Cloud Armor: a platform for credibility-based trust management of cloud services. *Proceedings of the 22nd ACM International Conference on Information and Knowledge Management*, 2509–2512.

Pan, Y., Ding, S., Fan, W., Li, J., & Yang, S. (2015). Trust-enhanced cloud service selection model based on QoS analysis. *PLoS ONE*, 10(11), 1–19.

Papazoglou, M. (2007). Web services: principles and technology. *Pearson Education. Prentice-Hall*

Phaphoom, N., Wang, X., Samuel, S., Helmer, S., & Abrahamsson, P. (2015). A survey study on major technical barriers affecting the decision to adopt cloud services. *Journal of Systems and Software*, *103*, 167-181.

Qu, L., Wang, Y., Orgun, M. A., Liu, L., Liu, H., & Bouguettaya, A. (2015). CCCloud: Context-aware and credible cloud service selection based on subjective assessment and objective assessment. *IEEE Transactions on Services Computing*, 8(3), 369-383.

Qu, L., Wang, Y., & Orgun, M. A. (2013). Cloud service selection based on the aggregation of user feedback and quantitative performance assessment. *IEEE International Conference on Services Computing (SCC)*, 152-159.

Rahman, R., Imran, A., Gias, A. U., & Sakib, K. (2013). A peer to peer resource provisioning scheme for cloud computing environment using multi attribute utility theory. *3rd International Conference on Innovative Computing Technology*, 132–137.

Ram S., M., & Vijayaraj, V. (2011). Analysis of the characteristics and trusted security of cloud computing. *International Journal on Cloud Computing*, *1*, 61-69.

Rashidi, A., & Movahhedinia, N. (2012). A Model for User Trust in Cloud Computing. *International Journal on Cloud Computing: Services and Architecture*, 2(2), 1–8.

Rathi, K., Kumari, S., & Chhotu, D. (2015). Model for User's Trust in Cloud Service Providers in Cloud Environment. *International Journal of Engineering and Computer Science*, 4(7), 13474–13483.

Rezaei, R., Chiew, T. K., Lee, S. P., & Aliee, Z. S. (2014a). A semantic interoperability framework for software as a service system in cloud computing environments. *Expert Systems with Applications*, 41(13), 5751–5770.

Rezaei, R., Chiew, T. K., Lee, S. P., & Aliee, Z. S. (2014b). Interoperability evaluation models: A systematic review. *Computers in Industry*, 65(1), 1-23.

Rizvi, S., Karpinski, K., Kelly, B., & Walker, T. (2015). Utilizing Third Party Auditing to Manage Trust in the Cloud. *Procedia Computer Science*, 61, 191-197.

Rocha, F., Abreu, S., & Correia, M. (2011). The final frontier: Confidentiality and privacy in the cloud. *Computer*, 44(9), 44-50.

Safari, F., Safari, N., & Hasanzadeh, A. (2015). The adoption of software-as-a-service (SaaS): ranking the determinants. *Journal of Enterprise Information Management*, *28*(3), 400-422.

Sahal, R., Khafagy, M. H., & Omara, F. A. (2016). A Survey on SLA Management for Cloud Computing and Cloud-Hosted Big Data Analytic Applications. *International Journal of Database Theory and Application*, 9(4), 107-118.

Saripalli, P., & Pingali, G. (2011). MADMAC: Multiple attribute Decision methodology for Adoption of clouds. *Proceedings - 2011 IEEE 4th International Conference on Cloud Computing*, 316–323.

Schneider, S., Lansing, J., Gao, F., & Sunyaev, A. (2014). A taxonomic perspective on certification schemes: development of a taxonomy for cloud service certification criteria. In *IEEE International Conference on System Sciences (HICSS)*, 4998-5007.

Shaikh, R., & Sasikumar, M. (2015). Trust Model for Measuring Security Strength of Cloud Computing. *Procedia - Procedia Computer Science*, 45, 380–389.

Selvaraj, A., & Sundararajan, S. (2017). Evidence-Based Trust Evaluation System for Cloud Services Using Fuzzy Logic. *International Journal of Fuzzy Systems*, 19(2), 329-337.

Serrano, D., Bouchenak, S., Kouki, Y., de Oliveira Jr, F. A., Ledoux, T., Lejeune, J., & Sens, P. (2016). SLA guarantees for cloud services. *Future Generation Computer Systems*, *54*, 233-246.

Sidhu, J., & Singh, S. (2014). Compliance based trustworthiness calculation mechanism in cloud environment. *Procedia Computer Science*, 37, 439–446.

Sidhu, J., & Singh, S. (2017). Improved TOPSIS method based trust evaluation framework for determining trustworthiness of cloud service providers. *Journal of Grid Computing*, 15(1), 81-105.

Sikeridis, D., Papapanagiotou, I., Rimal, B. P., & Devetsikiotis, M. (2017). A Comparative Taxonomy and Survey of Public Cloud Infrastructure Vendors. *arXiv preprint arXiv:1710.01476*.

Singh, S., & Sidhu, J. (2017). Compliance-based Multi-dimensional Trust Evaluation System for determining trustworthiness of Cloud Service Providers. *Future Generation Computer Systems*, *67*, 109–132.

Smith, A., Bhogal, J., & Sharma, M. (2014). Cloud computing: adoption considerations for business and education. In *IEEE International Conference on Future Internet of Things and Cloud (FiCloud)*, 302-307.

Sun, D., Chang, G., Sun, L., & Wang, X. (2011). Surveying and analyzing security, privacy and trust issues in cloud computing environments. *Procedia Engineering*, 15, 2852–2856.

Sun, H., Zheng, Z., Chen, J., & Lyu, M. R. (2013). Personalized web service recommendation via normal recovery collaborative filtering. *IEEE Transactions on Services Computing*, 6(4), 573–579.

Sun, M., Zang, T., Xu, X., & Wang, R. (2013). Consumer-Centered Cloud Services Selection Using AHP. *International Conference on Service Sciences (ICSS)*, 1-6.

Takabi, H., Joshi, J. B. D., & Ahn, G. J. (2010). SecureCloud: Towards a comprehensive security framework for cloud computing environments. *Proceedings - International Computer Software and Applications Conference*, 393–398.

Taneja, S., & Rathi, K. (2015). A Trust Evaluation Model to Recommend a Service Provider to a Customer in Cloud Environment. *International Journal of Computer Applications*, 121(2), 975–8887.

Tarhini, A., Masa'deh, R. E., Al-Badi, A., Almajali, M., & Alrabayaah, S. H. (2017). Factors influencing employees' Intention to use Cloud Computing. *Journal of Management and Strategy*, *8*(2), 47.

Tserpes, K., Aisopos, F., Kyriazis, D., & Varvarigou, T. (2012). A recommender mechanism for service selection in service-oriented environments. *Future Generation Computer Systems*, 28(8), 1285–1294.

Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2009). A break in the clouds: towards a cloud definition. *ACM SIGCOMM Computer Communication Review*, 39(1), 50-55.

Wang, L., & Wu, Z. (2014). A Trustworthiness Evaluation Framework in Cloud Computing for Service Selection. *2014 IEEE 6th International Conference on Cloud Computing Technology and Science*, 101–106.

Wang, W., Zeng, G., Zhang, J., & Tang, D. (2012). Dynamic trust evaluation and scheduling framework for cloud computing. *Security and Communication Networks*, 5(3), 311-318.

Wu, X., Zhang, R., Zeng, B., & Zhou, S. (2013). A trust evaluation model for cloud computing. *Procedia Computer Science*, 17, 1170–1177.

Xu, Y., Yin, J., Deng, S., N. Xiong, N., & Huang, J. (2016). Context-aware QoS prediction for web service recommendation and selection. *Expert Systems with Applications*, 53, 75–86.

Zheng, Z., Ma, H., Lyu, M. R., & King, I. (2011). QoS-Aware Web Service Recommendation by Collaborative Filtering. *IEEE Transactions on Services Computing*, 4(2), 140-152.

Zhang, S., Zhang, S., Chen, X., & Huo, X. (2010). Cloud computing research and development trend. In *IEEE Second International Conference on Future Networks, ICFN'10*, 93-97.

Zheng, Z., Wu, X., Zhang, Y., Lyu, M. R., & Wang, J. (2013). QoS ranking prediction for cloud services. *IEEE Transactions on Parallel and Distributed Systems*, *24*(6), 1213–1222.