Mansoura Journal For Computers and Information Sciences

A Trust Evaluation System for Cloud Environment

Doaa Trabay[1], Azezza Asem[1], Hazem M. El Bakry, [1] and Ibrahim El-Henawy[2]
[1]Department of Information System, Faculty of Computers and Information, Mansoura University, Egypt, Email: Doaawagdy2010@yahoo.com
[2]Department of Computer Science, Faculty of Science, Zagazig University, Egypt

ABSTRACT

Cloud computing (CC) has become a common desire as an alternative for investing in new IT systems, as it allows easy access to a network request to share configurable computing resources. It helps to speed up and enhance the flexibility of data management at less cost. Many cloud customers cannot choose a suitable Cloud Service Provider (CSP) due to the increase in CSPs and competition in service provision. While cloud computing is widely used, trust becomes an apprehension to everyone who uses Cloud Services (CSs). Despite the critical role of trust mechanisms and methods, rarely comprehensive evaluation methods help the customer select the right CSPs. Thus, the paper's contribution is surveying the main challenges in cloud environments, the role of service level agreements (SLAs), the Quality of Services (QoS), and finally, presents the trust evaluation system to rank the CSPs based on fuzzy logic.

Keywords

Cloud Computing, Service Level Agreements (SLA), Cloud-Analyst, Fuzzy Logic, and Trust Evaluation System.

1. INTRODUCTION

CC refers to computer resources and systems available on-demand via the network. This technology aims to facilitate access to all services without owning them or entering into technical details. The purpose of the cloud is to provide on-demand technical resources online, instead of purchasing, owning, and maintaining actual data centers; also, the customer can benefit from technology services, such as computing capabilities, storage, and databases.

*The customers can benefit from the cloud as follows [1]: y*Access their files and applications through magical services.

- Supports running programs and applications to large servers that require high-spec hardware, and customers do not need these specifications
- Customers do not need to purchase software, and thus software costs are saved. Users only need a computer connected to a fast internet line.
- This technology helps save labor and software maintenance costs
- Once the data is stored in the cloud, it becomes easier to get back up and restore, a time-consuming process in on-premises technology.

However, this technology has several disadvantages, including:

- The problem of internet availability, especially in developing countries, where the service requires constant communication.
- One of CC's shortcomings that might bother authors is the lack of protection for intellectual property rights issues.
- The most significant potential downside of using CC is downtime. CSPs may sometimes experience technical outages that can occur due to various reasons, such as power loss, low internet connection, data center out of service for maintenance, etc. So it may result in a temporary interruption of the cloud service.
- Cloud customers may face limited control over their deployments due to cloud services run on remote servers that are entirely owned and managed by CSPs, making it difficult for companies to get the level of control they want over the back-end infrastructure.

- Trust problem is some customers' fear of dealing with the cloud due to their lack of confidence, which is the main problem in our research.

The cloud business market arises instantly to satisfy customers' desires. As the market grows faster, it is imperative to determine the efficiency of CSPs continually. Many cloud providers offer similar functions, but there is a big difference in the quality of Services (QoS) provided to CSPs in such a competitive market. Therefore, there is an essential missing link between customers and cloud services, representing a lack of proper customer trust in the cloud.

Despite the protection provided by CSPs, cloud data trust is the CSPs' responsibility, so it should play an essential role in spreading trust and providing an effective cloud-operating environment. Although the trust mechanisms of CC are a vital part, comprehensive insight and basic studies on the CC trust assessment technique are extremely rare [2].

In CC environments, CSP needs to be aware of customers' needs in advance, so there is a need to establish the SLA. The SLA is an agreement that determines the QoS between CSPs and Cloud Service Users (CSUs), which usually depends on the price of services and the level of quality specified by the service's cost, for example, a CSP can charge a higher fee to a consumer who needs a high service quality level. The paper discusses the publications in the last decade and presents the evaluation of trust in the CC environment and customer response to CSPs by surveying authors' opinions and presenting various methods and technologies.

The primitive aim of Fuzzy Logic (FL) is to provide mysterious inference based on an inference engine, which is usually the process of mapping a given input set to an output set. So the paper will focus the evaluation with FL using parameters of performance and cost.

The main problem is finding out which CSPs are best suited to meet CSUs' needs and gain their confidence. Moreover, an accurate evaluation of CSP trust cannot be obtained. Therefore, the paper focuses on the FL techniques used in CC trust for each CSP based on the performance and cost parameters.

The paper is organized as follows; Section 2. Related Works, Section 3. The proposed model for evaluating trust, Section 4. Results of applying the CA and FL technique, and Section 5. Conclusion and future works.

2. RELATED WORKS

CC is a long-term dream as a utility for both CSP and CSU, as it has played an integral role in the development of Information Technology (IT), making software more attractive as a service. Developers no longer need a huge capital to provide hardware or human costs. Companies with large batch-oriented tasks can also get outputs as quickly as their software can scale since using 1000 servers for one hour costs nothing more than using one server for 1000 hours. This flexibility of resources without paying a premium on a massive scale is unprecedented in IT history.

Recently, the number of CSPs has increased dramatically, allowing customers to make the most suitable selection, but many CSUs do not have enough experience to solve the problem of selecting CSPs. This section, firstly presents the development of CC from its inception to our era, followed by various studies related to SLAs between CSUs and CSPs, including studies of QoS. Also present trust models and how to evaluate them in light of CC.

2.1 Evolution of Cloud Computing

CC concept began in the late sixties, and the term was inspired by the cloud shape that was frequently used to personify the internet in the form of graphs and maps [3]. In the late sixties, many developments occurred in CC according to the evolutions of computers from mainframe computers to PC, then the period of distributed computing [4] (See Figure 1).

With CC's development, a new computing paradigm is needed to provide efficient services to meet huge users' needs. However, CC applications did not appear until the beginning of 2000 when Microsoft expanded the concept of using software across the web, followed by many companies. Still, the company that played an essential role in the field of CC is Google, which launched many services based on this technology. Google is not limited to launch its services to take advantage of applications; in 2009, it launched an integrated operating system for computers running the CC concept [5].

Through studies, cloud computing has developed significantly over the last decade, beginning in 2010; Bhardwaj [6] published a research paper about the role of IaaS in the cloud environment. In 2013, Fernando et al. [7] conducted a comprehensive study on the mobile cloud, focusing on the threats it faces and discussing methodologies to address the challenges. With the help of the Internet of Things (IoT), the internet's quality can be increased, and store data in the cloud.

In 2016, Bhutta et al. [8] presented a survey combining CC and IoT, beginning with an analysis of IoT and CC fundamentals and a discussion of their complementarities while explaining the current drive for integration between them. In 2019 to date, some surveys have addressed comprehensive studies on CC and the challenges it faced, highlighting performance, service efficiency, and customer satisfaction with the service provided. Siddiqui et al. [9] surveyed cloud issues related to data resources, data privacy, data storage, and performance cost while developing solutions, such as managing data storage and controlling access to it, and saving energy. Bhandayker and Yeshwanth [10] presented a comprehensive study on CC, which included the general structure of CC including, its characteristics and types, then

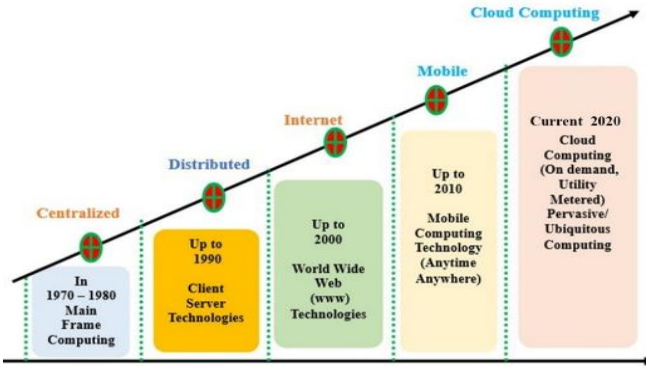

Figure 1. Growth of Cloud Computing

provided an overview of cloud architecture, CC challenges, the role of SLA, recently the trends in CC, and the extent of user service's needs. Sugumaran et al. [11] conducted a comprehensive survey to schedule CC to achieve desired performance while minimizing wasted time and developing methodologies to overcome the constraints. The study is organized into three primary consideration of methods, applications, and metrics based on the parameters used.

2.2 OVERVIEW OF CLOUD COMPUTING

NIST defined cloud computing as an integrated model that includes fast and comfortable access on-demand to share resources such as servers, applications, and services without any administrative effort, ownership, or interaction of CSPs [1].

CC technology is based on many current computing technologies, including the availability of high-speed broadband networking facilities, inexpensive storage, advanced virtualization technologies, distributed computing, grid computing, and utility computing [12]. The theoretical concept of CC is shown in Figure 2.

2.2.1 Cloud Computing Layers

- Infrastructure as a service (IaaS). An essential part of the cloud, where CSUs can lease storage, process, and communicate via cloud providers' virtual machines.
- Platform as a Service (PaaS). Developers can rent everything they need to create an application, relying on a CSP for development tools, infrastructure, and operating systems.
- Software as a Service (SaaS). Provided to customers who can utilize it directly from it without having to install any software.

2.2.2 Cloud Computing Deployment Models

The cloud service models can be presented through four different cloud service deployments models: private, community, public, and hybrid, depending on end-users' needs. This is explained briefly as follows [1]:

- Private Cloud: Cloud infrastructure is building for a particular use by a single organization with more users, but it is considered costly compared to previous clouds.
- Public Cloud: Allow systems and services to be accessible to all. This cloud may be less safe because it is available to everyone.
- Community Cloud: The resources are provided to the organization community to attain a particular purpose.
- Hybrid Cloud: It consists of two or more clouds, private, community, or public, that keep distinctive objects but are linked to each other by a unique technology that allows data and application transfer.

2.2.3 Cloud Computing Features

The following are the characteristics of CC [1]:

1. Customers can select the needed resources and reach information at anytime and anywhere.
2. Computing resources are flexibly scaled up to scale based on cloud consumers.
3. Measuring services control the overall business process "pay as you go model."
4. The cloud service (CS) owns the resources pooling and the scaled up or down based on the customer or organization's needs.
5. Cloud applications allow building co-operation among the organization's members and easily share information in real-time.

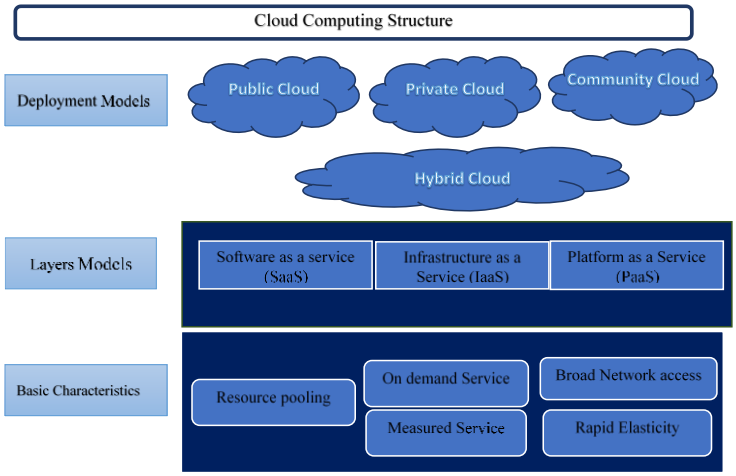

Figure 2. Cloud Computing Structure

2.3 Services Level Agreements (SLA)

Emphasis should be placed on the SLA for cloud services as it is a fundamental and vital component of our research. Most customers do not realize its importance due to its complexity and difficulty in understanding its contents. SLA is an agreement that specifies QoS between CSP and CSU. In general, SLA consists of several components summarized in the SLA tree form as follows [13] (See Figure 3).

1. Parties: Signatory parties consist of one CSP and one CSU, or the third party works on behalf of either or both of the signers.
2. Service description: Service objects represent the description terms and include SLA parameters, which contain properties and indicate quantitative and qualitative measures.
3. Obligations: The CSP defines the guarantee in the form of obligations, either as Service Level Objectives (SLO) or as action guarantees. SLO are measurable goals that a CSP undertakes to achieve while performing the service. SLO values can be verified through monitoring and auditing. The guarantee refers to the tasks performed by the CSP.

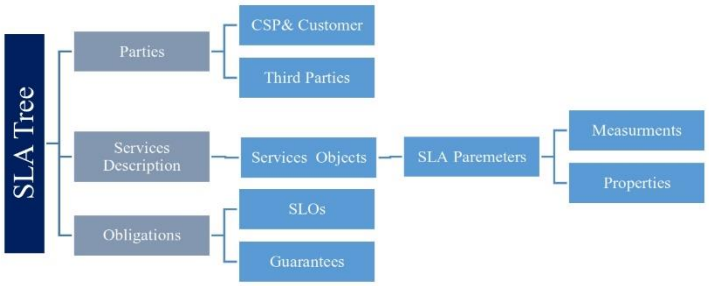

Figure 3. SLA Tree

Therefore, SLAs' role is to establish all CSPs provisions to ensure efficient services that reach cloud beneficiaries. If CSPs fail to comply with the terms of the agreement, this may result in their customers' loss. The provisions must be clear to the CSUs as well as the strengths of the agreement according to the suitability of the terms to their needs as follows:

- Acceptable performance according to the agreement.
- The time for providing you with an acceptable performance as per the agreement.
- Dealing with data according to the terms of the agreement.
- Overall performance review and evaluation.

Hence, SLA is becoming more critical as most organizations transfer all their data and applications to the network. Therefore, we present the latest studies that focused on SLA and its relevance in CC. Anwar et al. [14] suggested a framework to discuss SLA parameters in terms of cost, performance, and challenges to satisfy CSUs and generate the most revenue. The framework monitors CSPs' performance about the terms agreed with the customer and penalized those who violate the agreement's terms. The proposal also achieved trust between CSP and the CSU. Nastic et al. [15] combined SLO with SLAs to create a new flexible, performance-based framework and identify key research challenges, insight, and approaches for the original SLO paradigm in the next generation of CC. Pascal et al. [16] introduced a framework for SLA

assurance, which can be used by both CSPs and CSUs to evaluate and test the performance of different applications using simulation software. Gerser et al. [17] provided a comprehensive survey of previous literature on SLAs and IoTs; they discussed, analyzed SLAs in light of the IoTs, and identified loopholes for developing future solutions. Mubeen et al. [18] surveyed 328 papers and classified them into seven sections: SLA management, SLA definition, SLA modeling, SLA negotiation, SLA monitoring, SLA abuse and trustworthiness, and development of SLA. A comprehensive study was conducted on the role of SLA in the IoTs, and the results showed that most of the studies presented were limited to academic experiences and away from real and tangible industrial environments, so the authors focused on the qualitative and quantitative evaluation of QoS in SLA.

Regarding the importance of security in SLAs, Casola et al. [19] discussed parameters that help establish SLA between CSP and CSU, such as confidentiality, integrity, reliability, availability, and privacy. They clarified the importance of the agreement before signing the SLA. They also listed the different CC models in SLAs and discussed the challenges and advantages of the models. Rak et al. [20] also proposed a technique for automatically creating a security SLA based on the CSP announcement and the services that make up the app.

Trust can be established by conducting successful transactions and meeting all SLA parameters drawn up between two interacting parties. Macías et al. [21] provided a mathematical model for calculating trust values, which does not require a central entity to manage it and does not allow the participants to have undesirable behavior. The trust model was incorporated into SLA negotiations, and reliability gives customers a priority and stimulates accurate trust reports from clients. Finally, the study evaluated and analyzed the trust model's validity under various dishonest customers and CSPs attacks.

Due to the increasing use of cloud services (CSs), the Quality of Cloud Services (QoCS) has become an essential and primary issue due to the many open challenges that need to be addressed. The QoS can be divided into measurable and non-quantifiable parameters. While it is easy to measure quantitative parameters, non-quantifiable parameters are difficult to measure easily due to these parameters' subjective nature, so we will present some studies that dealt with the QoCS. S. Wang [22] proposed an accurate approach to evaluate QoCS using fuzzy artificial decision, also used a cloud paradigm to measure uncertainty in CSs that depend on QoCS data monitored. Upadhyaya et al. [23] proposed a comprehensive study about QoS models in light of CC through the practical application of the higher education sector, where the model contributed to improving the service provided. Varol et al. [24] proposed a comprehensive study on the role of service quality in the SLA and studied the gaps in terms of the agreement. The study was classified according to the QoS parameters, namely; trust, resource management, security, and task scheduling. Batista et al. [25] created a system to define QoS parameters and modified computational resources based on the cloud environment's results of service performance and security mechanisms.

2.4 Trust Models for Cloud Computing

The trust in a cloud environment is not written in an agreement, but rather something acquired and can be defined in various ways. Experts described the concept of trust as a way to deal with risks with increasing technological advances. Further, trust is a subjective and measurable relationship between interacting services willing to act consistently, safe, and reliable manner [26]. The evaluation process of system trust is called trust modeling. Trust models are created based on contracts and an agreement between CSPs and CSUs. The contracts most commonly used are SLA and service policy reports. It contains security documents and QoS parameters to establish trust between the two parties.

There are many recent studies on how trust is applied and evaluated in light of CC. Chiregi et al. [27] presented a model based on trust and reputation measures through the opinions and recommendations of leaders, where trust evaluated based on five factors: accessibility, reliability, data integrity, identity, and ability, the results of the research were that it provided the integrity and security, but it suffered from lack of confidentiality and the inability to expand. Similarly, Wang et al. [28] suggested that a cloud trust model reduces threats and risks related to leasing CSs. The results showed the model's effectiveness, as it reduced the risks of internal attacks. The proposed mechanism provided better reliability and security, but its scalability, confidentiality, and reliability were low. Lynn et al. [29] proposed a new trust model which categorized as follows: a historical summary of service level (such as latency and uptime), CSs such as (data site, back up), and CSPs such as (data location)) using the Delphi method with 28 CC experts to benefit from the classification and encourage perceptions about the trust value. The proposed mechanism provided better reliability, security, integrity, and dynamism, but it suffers from safety and scalability.

Also, Chahal and Singh [30] proposed an expert system to evaluate the trust value for five CSPs based on the following criteria: security, performance, usability, and reliability using the fuzzy method, and they relied on trust assessment by combining general review, direct trust, and auditor's confidence, It provided sufficiently security, reliability, and scalability, but suffered from low dependability, low confidentiality, and inadequate safety. Singh and Sidhu [31] proposed a multi-dimensional compliance-based trust rating system that allows community businesses to determine a CSP's trust. The framework enabled users to evaluate a CSP's trust from different perspectives. The proposed method was distinguished by sufficient scalability and reliability but suffered from a low security and confidentiality level. Tang et al. [32] presented a new technique for determining the moderating influence of confidence on adopting cloud-based services to determine confidence factors in the CSs hypothesis in semiconductor industries. The proposed method provided adequate safety, but it suffered low dependability and dynamic. Selvaraj and Sundararajan [33] presented a confidence assessment scheme for

CSs using fuzzy logic. The system used QoS parameters to assess confidence for CSPs. The results were determined in terms of the efficiency and effectiveness of the model through simulation. It provided adequate security, reliability, and dynamics but suffered low integrity, low confidentiality, and insufficient safety. Navimipour et al. [34] conducted a comprehensive study and survey about the techniques used to assess CSPs trust and classified them into two parts, namely; centralization and distributed, also discussed the applications of trust, including monitoring and tracking, and identified trust characteristics from the perspectives of integrity, security, availability, reliability, safety, dynamism, confidentiality, and scalability. Chiregi et al. [35] conducted a comprehensive study. They analyzed all previous studies from 2012 to 2017 to assess CSs trust in the integrity, security, reliability, reliability, safety, dynamism, confidentiality, and scalability, and they compared all of these mechanisms. As a result, they concluded that these factors did not act reasonably in all of the fields. Wang et al. [36] suggested a framework to evaluate a dynamic CSs trust based on SLA. First, they proposed a model that conducted an overall trust assessment consisting of direct and indirect trust and reputation. Second, the CSs were divided into five levels based on their service capabilities, and the SLA was analyzed to determine the QoS. Empirical results show that the proposed model effectively relies on service preferences, customer satisfaction, and the avoidance of harmful interference.

Trust management plays a vital role in IoT to enable reliable data collection, context awareness, and improve user privacy. Thus, Khan et al. [37] conducted a comprehensive survey that includes confidence techniques in light of the IoT and showed the advantages and disadvantages of each study. The survey was significant for the IoT research community to understand the views and issues that the IoTs faces in managing the trust. Still, the study's drawbacks were not divided into lists to help researchers delve into the research, which was accomplished in the Borgbelah study in 2019. Borgbelah et al. [38] developed the role of trust to include the IoT and divided the research into four main lists, recommendations-based, forecast-based, policy-based, and reputation-based, then compared, discussed, and analyzed to measure trust based on several factors such as integrity, accuracy, privacy, reliability, scalability, and adaptability.

Wang et al. [39] provided an effective and objective trust model to assess and assist in selecting a CSP using the QoS requirement. They used grey correlation analysis and the Analytic Hierarchy Process (AHP) to calculate both objective and subjective factors. Moreover, the model proposed an updated dynamic direct confidence mechanism. Finally, the model achieved user satisfaction and interaction success rate. Also, Wang et al. [40] created a model for evaluating trust through business transaction bases, monitoring both historical cloud ratings and service satisfaction, then using the time decay function to characterize the change of service satisfaction over time and at the same time. The cloud service model proved efficiency, accuracy, and user satisfaction, especially in large data transactions.

The study of Jino et al. [41] provided comprehensive, detailed reviews that addressed services related to CC trust from the users' view by dividing the paper into three stages: surveying the most recent studies on cloud trust models, classifying contributions to cloud trust, and discuss challenges paper problems related to cloud trust models.

This study differs from other previous studies because it is somewhat closer to security than trust. In recent days, Mobile Edge Computing (MEC) has emerged as a modern computing model that pushes computing resources towards the edge of the internet and close to the end-users. More scientists are starting to conduct various types of research within the framework of advanced computing. Unlike CC, advanced computing often lacks a centralized security mechanism, which increases security risks to resource consumers. Deng et al. [42] established a trust-rating model based on MEC and proposed a trust rating based on reputation. The model was categorized into three levels, trust in identity, confidence in abilities, and trust in behavior. The model achieved more than doubled the terminal network's transaction success rate compared to the network without the trust rating mechanism. Chahal et al. [43] proposed a new model for interaction among social objects in the name of the Social Internet of Things (SIoT), focusing on managing trust, setting criteria, and assessing confidence, while taking into account various challenges and limitations.

Regarding trust scheduling, Rjoub et al. [44] developed a methodology for big data tasks called “Big Trust Scheduling” that contained 3 phases: VMs' trust level computation, tasks priority level determination, and trust-aware scheduling. The model's idea was to extract the trust value from each virtual machine based on its performance, then cost and resource requirements are determined. The proposal achieved high efficiency in intruder detection and access control. Also, the model can be expanded to encompass other environments, including IoTs, and parallel computing.

3. PROPOSED MODEL FOR EVALUATING TRUST

The paper presents steps for ranking to evaluate the trust value for five CSPs from CSP1 to CSP5 as follows (See Figure 4):

Step1: Input data of each services providers (See Table 1).

Step2: Applying the parameters of (Cost, and Performance) as the input [Number of Virtual Machines (VMs), Number of Data Center (DC), Number of Processors (NP), Memory Size in GB, Number of Physical Units] [VM cost per hour, Storage Cost, Transfer Cost] respectively, using Cloud-Analyst (CA) application.

Step3: Calculating the trust ratio using the Mamdani FL technique in Simulink Matlab2007 program [45].

Step4: Ranking the trust for performance and cost parameters and then choose the most suitable for CSU.

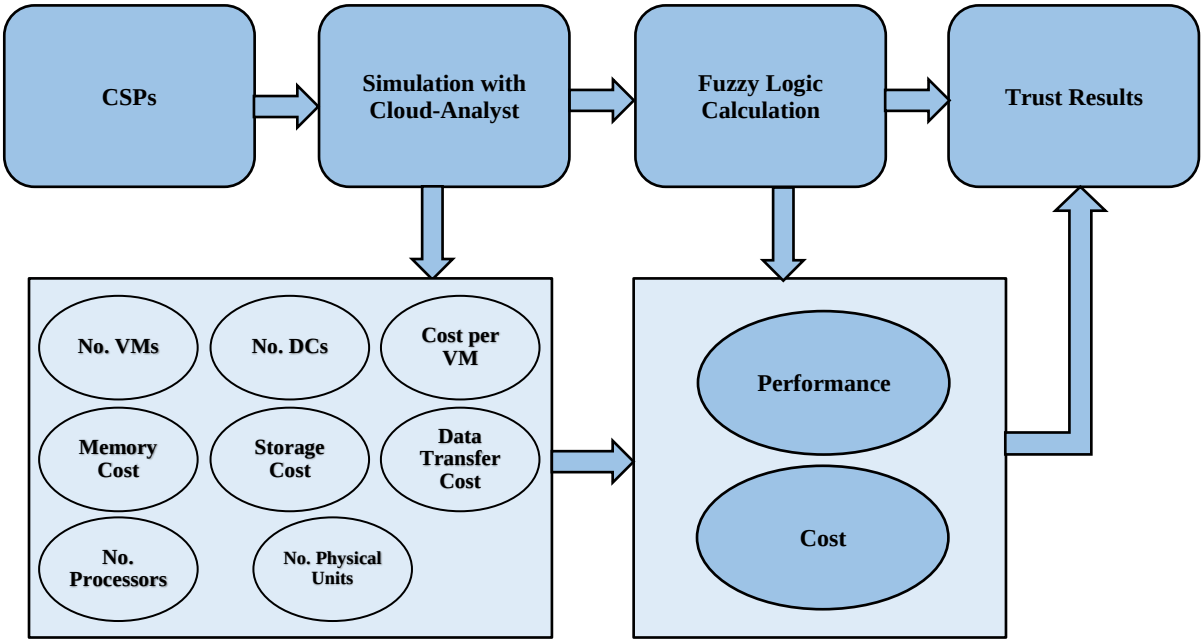

Figure 4. Evaluation of Trust Model

Table1. Simulation Parameters of CA

	Performance					Cost		
	No. of VM	No. of DC	Memory Size (GB)	No. of processor	No .of Physical Units	V.M Cost/Hr.($)	Storage Cost/GB($)	Data Transfer Cost/GB($)
CSP1	50	10	10	80	20	0.4	0.15	0.15
CSP2	30	6	3	40	10	0.2	0.20	0.12
CSP3	18	3	3	45	15	0.05	0.08	0.05
CSP4	20	2	4	75	20	0.8	0.25	0.09
CSP5	8	4	8	16	8	0.15	0.15	0.12

4. RESULTS OF APPLYING THE CA and FL TECHNIQUE

According to the steps followed in the previous section, the optimal CSP can identify based on the criteria of the performance and cost that satisfy customers' requirements based on their priorities.

4.1 Simulation of Cloud Providers Using Cloud-Analyst

In the beginning, we implement the Cloud-Analyst application based on their attributes: Data Center (DC) locations across the globe, allocation of Virtual Machines (VMs) in each DC, and User-Base (UB), which is responsible for forming a UB and generating traffic that represents the users, the description of the UB is also maintained constant for analyzing the

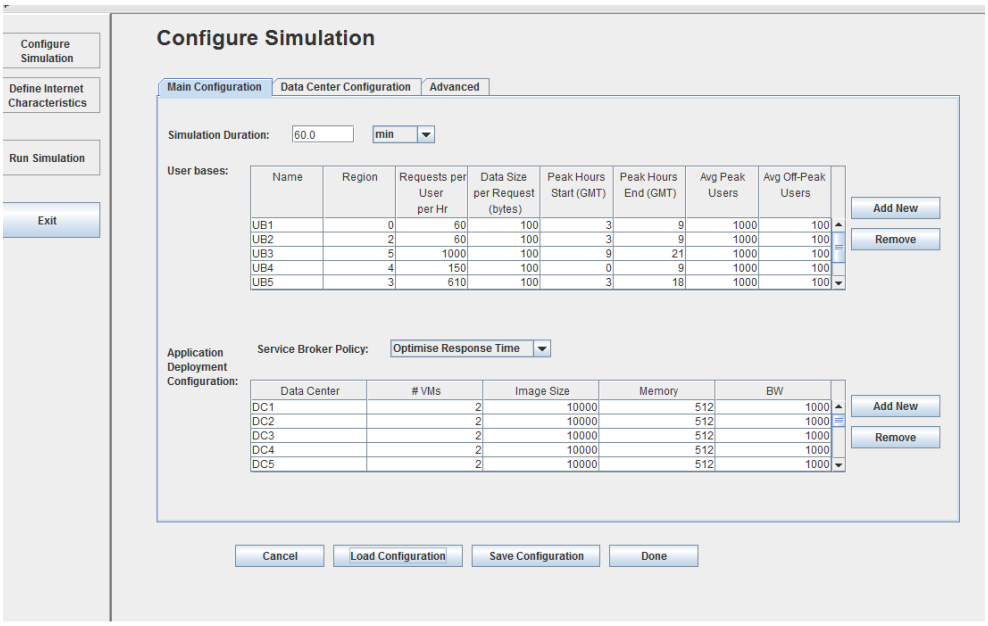

Figure 5. Configure Simulation Screen

performance of different CSPs with the same load as shown in Table 2, and configure simulation screen in Figure 5.

All CSPs separately are simulated with distributed DCs, to obtain the Response Time (RT), Processing Time (PT), VM cost, and data transfer cost as results (See Table 2 and Figure 6).

Table2. CA Results

CSPS	RT	PT	Total VM Cost($)	Total Transfer Cost
CSP1	50.14	0.43	120.01	135.23
CSP2	50.18	0.44	21	107.02
CSP3	217.50	0.16	9	150.45
CSP4	530.15	0.2	96	42.11
CSP5	145.98	0.83	240.15	74.28

4.2 Fuzzy Based Trust Model

Trust FL is the final-fuzzy trust that implements both performance and cost parameters using Mamdani FL in Simulink Matlab program to get the crispy outputs. The implementation of Simulink MATLAB2007 needs membership functions to define membership values, which will assume low (L), medium (M), and high (H), as per the requirements.

The trust values are calculated by passing the fuzzy sets through fuzzy inference rules. By drawing the trust values using the triangular membership function, a graph can be generated for trust, as shown in Figure 7 and Table 3.

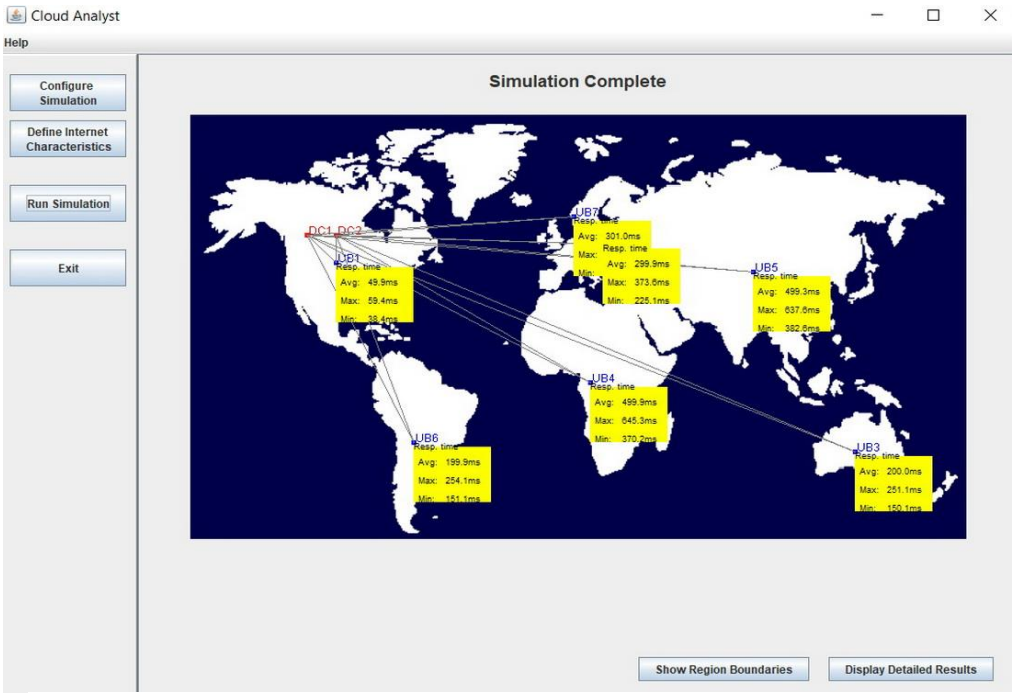

Figure 6. Simulation Results for CSP3

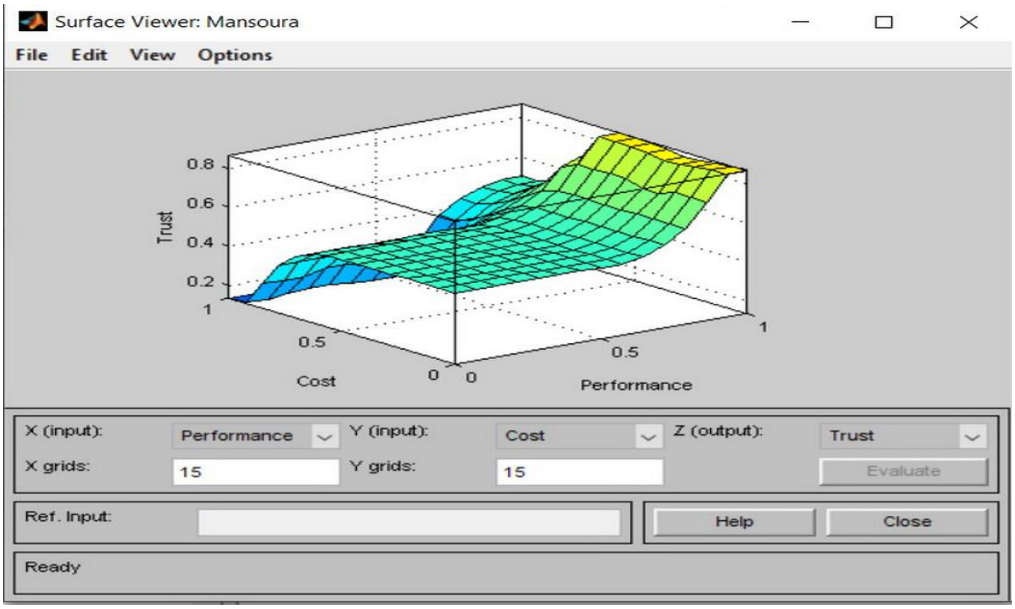

Figure 7. Final Trust Surface Viewer

Table3. Trust Results and Ranks

CSPs	Performance	Cost	Trust	Trust Rank
CSP1	0.888	0.204	0.802	H
CSP2	0.716	0.390	0.560	M
CSP3	0.615	0.454	0.505	M
CSP4	0.570	0.695	0.455	L
CSP5	0.380	0.655	0.478	L

The main comparison of results depend on a greater NP, RAMs capacity, and lows of PT and RT so that these attributes are a complement to each other

As in Table 3, the trust rating generated for CSP1 is the best CSPs as compared to other CSPs, it also achieved the better performance with the lowest PT and RT. Although the CSP1 achieved high performance, it is not the least cost compared to the rest of the CSPs, so the CSU should choose the most suitable decision, whether performance or cost. Also the sensitivity and accuracy of the results appeared when changing inputs, which close to each other, and led to a change in the CSPs' ranking.

5. Conclusions and Future Works

Cloud computing is a paradigm shift in distributed computing due to the way resources are saved. The importance of trust is a sensitive topic for both customers and service providers. Therefore, more authors have provided their ideas to assess the trust of CSPs, and for this, the paper reviewed the most recent works carried out in this field that included the literature on the evolution of CC and the most important studies of SLA, QoS, and provided the considered trust models. The research focused on assessing CSP's trust using geographical distribution and data using Cloud-Analyst application and carried out the FL technique depending on the parameters of performance and cost as the easiest method to rank the best CSP, which helps the customer to choose the best CSP.

Future work can be extended to other parameters in evaluating the trust model to improve outcomes such as; security and usability. It will also suggest MCDM and Fuzzy MCDM methods to obtain near-realistic results.

ACKNOWLEDGMENTS

Our thanks to the anonymous reviewers to improve the paper, and Prof. Wajeb Gharibi from UMKC, MO. USA, for his valuable comments and encouragement.

REFERENCES

[1] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

[2] Lin, G., Bie, Y., & Lei, M. (2013). Trust Based Access Control Policy in Multi-domain of Cloud Computing. *JCP*, *8*(5), 1357-1365.

[3] Durkee, D. (2010). Why cloud computing will never be free. *Communications of the ACM*, *53*(5), 62-69.

[4] Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008, November). Cloud computing and grid computing 360-degree compared. In *2008 grid computing environments workshop* (pp. 1-10). Ieee.

[5] McDonald, P. (2010). Introducing Google App Engine+ our new blog: Abgerufen am

[6] Bhardwaj, S., Jain, L., & Jain, S. (2010). Cloud computing: A study of infrastructure as a service (IAAS). *International Journal of engineering and information Technology*, *2*(1), 60-63.

[7] Fernando, N., Loke, S. W., & Rahayu, W. (2013). Mobile cloud computing: A survey. *Future generation computer systems*, *29*(1), 84-106.

[8] Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. *Future generation computer systems*, *56*, 684-700.

[9] Siddiqui, S., Darbari, M., & Yagyasen, D. (2019). A comprehensive study of challenges and issues in cloud computing. In *Soft Computing and Signal Processing* (pp. 325-344). Springer, Singapore.

[10] Bhandayker, Y. R. (2019). A Study on the Research Challenges and Trends of Cloud Computing. *RESEARCH REVIEW International Journal of Multidisciplinary*, *4*.

[11] Arunarani, A. R., Manjula, D., & Sugumaran, V. (2019). Task scheduling techniques in cloud computing: A literature survey. *Future Generation Computer Systems*, *91*, 407-415.

[12] Marinescu, D. C. (2017). *Cloud computing: theory and practice*. Morgan Kaufmann.

[13] Butler, J. M., Yahyapour, R., & Theilmann, W. (2011). Motivation and overview. In *Service Level Agreements for Cloud Computing* (pp. 3-11). Springer, New York, NY.

[14] Badshah, A., Ghani, A., Shamshirband, S., Aceto, G., & Pescapè, A. (2020). Performance-based service-level agreement in cloud computing to optimise penalties and revenue. *IET Communications*, *14*(7), 1102-1112.

[15] Nastic, S., Morichetta, A., Pusztai, T., Dustdar, S., Ding, X., Vij, D., & Xiong, Y. (2020). Sloc: Service level objectives for next generation cloud computing. *IEEE Internet Computing*, *24*(3), 39-50.

[16] Ibrahim, A. A. Z. A., Kliazovich, D., & Bouvry, P. (2016, May). Service level agreement assurance between cloud services providers and cloud customers. In 2016 16th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid) (pp. 588-591). IEEE.

[17] Girs, S., Sentilles, S., Asadollah, S. A., Ashjaei, M., & Mubeen, S. (2020). A Systematic Literature Study on Definition and Modeling of Service-Level Agreements for Cloud Services in IoT. *IEEE Access*, *8*, 134498-134513.

[18] Mubeen, S., Asadollah, S. A., Papadopoulos, A. V., Ashjaei, M., Pei-Breivold, H., & Behnam, M. (2017). Management of service level agreements for cloud services in IoT: A systematic mapping study. *IEEE Access*, *6*, 30184-30207.

[19] Casola, V., De Benedictis, A., Rak, M., & Villano, U. (2015, September). SLA-based secure cloud application development: The SPECS framework. In *2015 17th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)* (pp. 337-344). IEEE.

[20] Rak, M., Suri, N., Luna, J., Petcu, D., Casola, V., & Villano, U. (2013, December). Security as a service using an SLA-based approach via SPECS. In *2013 IEEE 5th International Conference on Cloud Computing Technology and Science* (Vol. 2, pp. 1-6). IEEE.
[21] Macías, M., & Guitart, J. (2016). Analysis of a trust model for SLA negotiation and enforcement in cloud markets. *Future generation computer systems*, *55*, 460-472.
[22] Wang, S., Liu, Z., Sun, Q., Zou, H., & Yang, F. (2014). Towards an accurate evaluation of quality of cloud service in service-oriented cloud computing. *Journal of Intelligent Manufacturing*, *25*(2), 283-291.
[23] Upadhyaya, J., & Ahuja, N. J. (2017, February). Quality of service in cloud computing in higher education: A critical survey and innovative model. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 137-140). IEEE.
[24] Raza, M. R., & Varol, A. (2020, June). QoS parameters for viable SLA in cloud. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-5). IEEE.
[25] Batista, B. G., Ferreira, C. H. G., Segura, D. C. M., Leite Filho, D. M., & Peixoto, M. L. M. (2017). A QoS-driven approach for cloud computing addressing attributes of performance and security. *Future Generation Computer Systems*, *68*, 260-274.
[26] Chiregi, M., & Navimipour, N. J. (2017). A comprehensive study of the trust evaluation mechanisms in the cloud computing. *Journal of Service Science Research*, *9*(1), 1-30.
[27] Chiregi, M., & Navimipour, N. J. (2016). A new method for trust and reputation evaluation in the cloud environments using the recommendations of opinion leaders' entities and removing the effect of troll entities. *Computers in Human Behavior*, *60*, 280-292.
[28] Wang, Y., Chandrasekhar, S., Singhal, M., & Ma, J. (2016). A limited-trust capacity model for mitigating threats of internal malicious services in cloud computing. *Cluster computing*, *19*(2), 647-662.
[29] Lynn, T., Van Der Werff, L., Hunt, G., & Healy, P. (2016). Development of a cloud trust label: a Delphi approach. *Journal of Computer Information Systems*, *56*(3), 185-193.
[30] Chahal, R. K., & Singh, S. (2017). Fuzzy rule-based expert system for determining trustworthiness of cloud service providers. *International Journal of Fuzzy Systems*, *19*(2), 338-354.
[31] 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.
[32] Tang, M., Dai, X., Liu, J., & Chen, J. (2017). Towards a trust evaluation middleware for cloud service selection. *Future Generation Computer Systems*, *74*, 302-312.
[33] 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.
[34] Chiregi, M., & Navimipour, N. J. (2017). A comprehensive study of the trust evaluation mechanisms in the cloud computing. *Journal of Service Science Research*, *9*(1), 1-30.
[35] Chiregi, M., & Navimipour, N. J. (2018). Cloud computing and trust evaluation: A systematic literature review of the state-of-the-art mechanisms. *Journal of Electrical Systems and Information Technology*, *5*(3), 608-622.
[36] Wang, Y., Wen, J., Zhou, W., & Luo, F. (2018, August). A novel dynamic cloud service trust evaluation model in cloud computing. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 10-15). IEEE.
[37] Din, I. U., Guizani, M., Kim, B. S., Hassan, S., & Khan, M. K. (2018). Trust management techniques for the Internet of Things: A survey. *IEEE Access*, *7*, 29763-29787.
[38] Pourghebleh, B., Wakil, K., & Navimipour, N. J. (2019). A comprehensive study on the trust management techniques in the Internet of Things. *IEEE Internet of Things Journal*, *6*(6), 9326-9337.
[39] Wang, Y., Wen, J., Wang, X., Tao, B., & Zhou, W. (2019). A cloud service trust evaluation model based on combining weights and gray correlation analysis. *Security and Communication Networks*, *2019*.
[40] Yang, X., Wang, S., Yang, B., Ma, C., & Kang, L. (2019). A service satisfaction-based trust evaluation model for cloud manufacturing. *International Journal of Computer Integrated Manufacturing*, *32*(6), 533-545.
[41] Balcão Filho, A., de Franco Rosa, F., Ruiz, R., Bonacin, R., & Jino, M. (2019, November). A Study on Trust Models in Cloud Computing. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)* (pp. 1-8). IEEE.
[42] Deng, X., Liu, J., Wang, L., & Zhao, Z. (2020). A trust evaluation system based on reputation data in Mobile edge computing network. *Peer-to-Peer Networking and Applications*, 1-12.
[43] Chahal, R. K., Kumar, N., & Batra, S. (2020). Trust management in social Internet of Things: A taxonomy, open issues, and challenges. *Computer Communications*, *150*, 13-46.
[44] Rjoub, G., Bentahar, J., & Wahab, O. A. (2020). BigTrustScheduling: Trust-aware big data task scheduling approach in cloud computing environments. *Future Generation Computer Systems*, *110*, 1079-1097.
[45] Haj-Ali, A., & Ying, H. (2002, June). Structure analysis of Mamdani fuzzy PID controllers with nonlinear input fuzzy sets. In *2002 Annual Meeting of the North American Fuzzy Information Processing Society Proceedings. NAFIPS-FLINT 2002 (Cat. No. 02TH8622)* (pp. 19-21). IEEE.