[1] **Dr.K.K.Baseer**

[2] **Dr M Jahir Pasha**

[3] **Dr Jyoti Prasad Patra**

[4] **C.Rohith Bhat**

[5] **Dr. S.Gomathi**

[6] **Bramah Hazela**

Trust based Reputation Framework for Data Security in Cloud Environment

Abstract: - Cloud computing relies on the Internet and is susceptible to numerous attacks, hence security is the most significant issue.It takes a long time to create trust values for trust authority and cloud servers.Research into trust relationships and trust-based security mechanisms in cloud environments is important because trust has been regarded as a security relationship that is more important than authorization.In a cloud computing environment, trust should exist between cloud users and service providers.As a result, a trust-based reputation framework with fuzzy rules for cloud data security is proposed.The trust values of data centers (DCs) and cloud users (CUs) are independently determined within this framework.The DC examines the CU's reputation and disregards it if it is poor.The user evaluates the serving DC's reputation during transmission to the user and disregards low reputations.The results achieved demonstrate that the trust of the proposed framework performs better.

Keywords: Cloud Security, Trust Evaluation, Trust, Cloud computing, Reputation

I. INTRODUCTION

Cloud computing is a novel business model and paradigm for computing.Through the pay as you go model, it cuts costs and avoids expenses.Users deploy and manage cloud services from a data center [1]. Despite the fact that cloud computing presents significant opportunities for the software industry, the technology's development is still in its infancy, and there are still a number of issues to be resolved [2]. Reputation and Trust (RT) frameworks are successfully employed in a variety of application scenarios to assist customers in diagnosingconsistent as well as trustworthy providers, such as Amazon, eBay, and mobile app markets [3].

The cloud computing paradigm faces significant challenges in trust and security, both of which impede cloud adoption and cloud growth.A trust evaluation and management model are being developed in this location to improve the cloud computing paradigm's security [4].Trust is eliminated as the primary obstacle that must be overcome in cloud computing from the aforementioned challenges.A tangible trust bondamongCloud Providers (CP), Cloud Service Providers (CSP), and Cloud Service Users (CSU) is required for the implementation of an efficient multi-cloud environment [5, 6]. This is supported by a number of previous works. A user reputation-based cloud service selection framework and a user reputation scheming method called MeURep, thatcomprises L1-MeURep as well as L2-MeURep [7], a reputation-based trust management (RTM)as well as a collaborative SLA answer for a federated cloud environment [8].

In addition, a conceptual zerotrust strategy for the cloud environment and a lightweight trust management algorithm rooted on subjective logic known as InterTrust [9] have been proposed. A decentralized approach is incorporated into the proposed framework with the intention of minimizing any single entity's control over digital assets in the CC/CbC space [10]. The model, which delivers a conceptual typology of perceptions along with philosophies for gaining trust in cloud services [11], provides an adaptive formal method for security policy administration in a cloud environment.

[1] Professor, Department of Information Technology, Mohan Babu University (Erstwhile SreeVidyanikethan Engineering College), Tirupati, Andhra Pradesh, India, *1baseerphd@yahoo.com

[2] Associate Professor, Department of Computer Science and Engineering (Data Science), Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal, Andhra Pradesh, India, jahir4444@gmail.com

[3] Faculty Electrical Odisha University of Technology and Research Outr Mahalaxmi ViharGhatikia Techno Campus, Bhubaneswar, Odisha, India, jpp42003@yahoo.co.in

[4] Professor, Department of CSE, Simats School of Engineering, Chennai, Tamilnadu, India, rohithbhat2000@gmail.com

[5] Professor, Computer Science and Business Systems, Francis Xavier Engineering College, Tirunelveli, Tamilnadu, India, gomathy@francisxavier.ac.in

[6] Assistant Professor, Department of Computer Science & Engineering, Amity School of Engineering & Technology, Amity University, Uttar Pradesh, India, bramahhazela77@gmail.com

This method models the user's cloud-based actions as a process algebra expression using a new version of the Algebra Communication Process with reputation integration [12]. A framework for protecting privacy is proposed. Second, we examine and discuss fundamental ABE [13]. Cloud Armor, a reputation-rooted trust management framework with a set of functionalities, was proposed by the system [14]. Lightweight blockchain-based trust the executive's system that is reasonable for IoT gadgets. The most well-known ICN architecture is called Named Data Networking (NDN) [15]. Our framework's Peer-to-Peer (P2P) network is built with high-resource devices [16].

A. Contribution of the proposed framework

The paper's primary objective is to make a trust-based reputation framework for trust assessment service authority data sharing and storage.The trusted authority and cloud servers receive their own trust value.The trusted authority and cloud server parameter values are obtained from the cloud service.The cloud user receives the trust value that has been calculated using the history by the rule generator, also known as fuzzy rules.Based on their requirements, the cloud user will choose a cloud server.

The following is how the following part of this paper is laid out.Section 2 reviews the existing trust-based reputation framework.The trust-based reputation framework is briefly explained in section 3. The experimental study of the proposed framework is discussed in Section 4. Section 5 concludes the work, followed by the references.

II. LITERATURE ASSESSMENT

Challagidadet al. [17] discussed the quantity of data stored in cloud storage is rapidly growing.Despite the fact that the issue of cloud computing trust is a top concern for the majority of businesses to the point where it is extensivelyobserved as atop barrier to the adoption and cloud computing expansion.As a result, a trust model that measures the cloud service provider (CSP) trustworthiness is required to assist cloud customers in selecting the provider that best meets their trust requirements.A trustevaluation algorithm that takes into accountserver rejection rate, customer feedback, and server workload is the basis for our reputation-based trust model that we propose in this paper.

Srinivas et al. [18] made research about the difficulty to identify risks when the data in cloud storage undergoes a sudden and significant change.Cloud computing relies heavily on security, and trust is a most intriguing and capableaspects for preventing uncertainty.Later the company has direct control over the data, it relies on the service provider to possess it safe.By sending and storing static data using reputable results, customers ensure that the service provider maintains data confidentiality.A strategy for reputation-based interactions is presented in this paper. It is categorized by the trust that is essential for cloud data persistence and the potential of acquiring a competitive advantage.

A multi-dimensional reputation as well as trust estimation model for cloud computing is presented by Singh, Ashish, and Kakali Chatterjee [19]. This model, integratednumerous trust factors that improve the model's performance.The WeightedMoving Average and Ordered Weighted Averaging (WMA-OWA) grouping algorithm is used to energeticallyallocate a weight to each reputation and trust factor.

Wang et al. [20] introduced a model that combines gray correlation analysis and weights is proposed.First, a comprehensive trust that includes direct trust, trust based on recommendations, and reputation provides anaddedprecise overall trust.Second, for the direct trust, the AHP-based method as well as the rough set theory are utilized.A gray relational investigation technique is analysed to compute the recommendation trust degree similarity in the meantime.A dynamic trust update mechanism is proposed in this paper to guarantee the accuracy of direct trust.Last but not least, the cloud services trust evaluation model (CSTEM)'s superiority over the other three approaches is demonstrated through the simulation experiment.It safeguards against intruders;simultaneously, it may increase interaction success rates and user satisfaction.

Ghafoorianet al. [21] describe the security objectives that are in consideration when developing an effective trust-oriented scheme.Next, a trust as well as reputation-based RBAC model is proposed that is scalable and has a reasonable execution time in addition to being able to resist the security issues posed by trust-oriented RBAC models.

Alsenaniet al. [22] introduced a model called ProTrust. This model is a probabilistic framework for defining a host's trust in VCC. Two new metrics and the trust concept in VCC are developed by us:1) trustworthiness affected by behavioral change and 2) trustworthiness grounded on the task priority, which is called loyaltyin the beginning, the work used analtered Beta distribution function, and the resources behaviour is divided into various levels of loyalty.Then, this work presented a conduct location strategy to reflect late changes in conduct.

A brand-new security metric called trustability (trust–reliability) and an innovative method for calculating it were presented by Ruan, Yefeng, and Arjan Durresi [23].The degree to which a system can withstand a particular attack vector is known as its trustability.The design space for resource configuration can be explored using trustability to find the optimal compromise between trustability and redundancy costs.

Li et al. [24] described a clever trust evaluation system for the security as well as notoriety of cloud services is proposed.This system empowers the trust assessment of cloud administrations to guarantee the cloud-based IoT security setting by means of incorporating security as well asnotoriety-rooted trust valuation strategies.The cloud

service security is assessedby the cloud-specific security metrics in the security-grounded trust valuation method.Moreover, the reputation-based trust valuation method uses feedback ratings on cloud service quality to evaluate a cloud service's reputation.

III. PROPOSED TRUST BASEDREPUTATION FRAMEWORK

There are two different ways to demonstrate peer trust or distrust:that is, reputation and trust.Numerous reputation-based computational trust models demonstrate that reputation acts a crucial part in establishing trust.The accuracy along with efficiency with which the reputation system is updated on a regular basis are the primary indicators of its quality.It is the most important trust building strategy because the opinions of various cloud service users determine the service's reputation, either positively or negatively.Trust can be transitive however not really symmetric between two gatherings.One of the biggest barriers to cloud computing adoption is trust. Uncertain and inconsistent trust exists between the Cloud Customer as well as the Cloud Provider.Further to solve the security problems, trust-based security models are needed.As a result, this work proposes a trust-based reputation frameworkwhere the trust assessment will be grounded on customer feedback, server workload, and request rejection rates.

A. The Proposed Framework's Architecture

The individualexpectancy of an entity about another in a particular context at a particular time is trust. Asdepicted in Figure 1, which is aproposed trust-based reputation framework architecture, this trust can be a resultant from various factors. These factors includeserver workload, customer feedback, and the count of request rejections done by the server. Thegivenproposed framework's goal is to create a trust-based reputation framework that can be used to assess trust between a service provider and a client or customer. In the framework the client will lead a request over the network to the server for the use of the service, such as to upload,store, play, or download the client's datafrom or to the cloud. The server selection for customer service will be made during request transmission grounded on cloud server feedback,request delay and rejection.

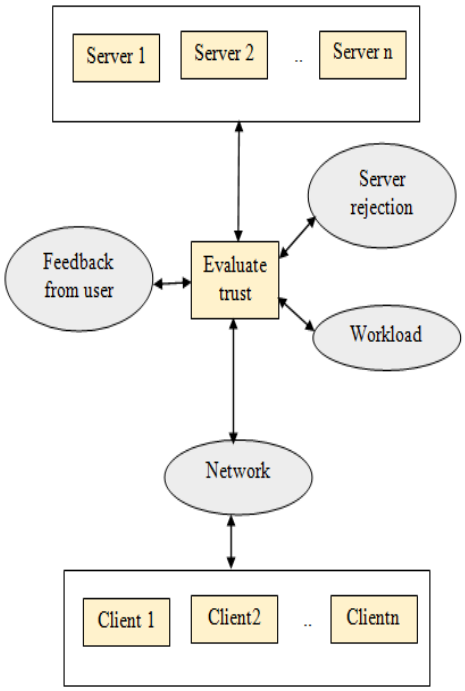

Figure 1 indicates Flowchart of Framework

Trust: Initially the trust is considered. It is related with specific credits like truthfulness, unwavering quality, security, genuineness, dependability, competence and so forth, of the confided in elements to go about true to form. However, entities do not have a predetermined trust value.Rather, their trust value fluctuates over time and in specific contexts.

Reputation: A person's perception of an entity is based on the observations of another person at a specific time and in a particular setting.

Trustworthiness: The service provided by a provider of quality services is characterized by trustworthiness.

Feedback: By responding to the different questionnaires in included in the form of afeedback, the user can provide feedback to the service provider grounded on their level of satisfaction. The Cloud Server feature marks are used to assess the cloud server's trustworthiness.

Rate of server rejection: Each server with a total capacity for handling requests, such as [k=10], for instance. Here k is considered as the number of servers. The threshold level necessary to process a customer request exists on

the servers. Let's say the threshold level is 7 and the capacity is 10. The server will check their threshold level as it accepts the new request. If no.if a request exceeds the threshold, the server takes corresponding action to reject the subsequent request.The number of the server rejecting is considered as X. Hence the trust evaluation will be determined by observing each server's rejection rate.

Demand on the server: At first all server is great, thus in the proposed framework the servers considered are [S1=0, S2=0, S3=0].Based on the service of "first come, first served," the first request will be made to the first server S1.At the point when client sends next requests, all solicitation will be in line to get administration. "Queue Work Load Calculation" is used to handle the queue request and sends a new server call with the least number of work load. In this process the work (or load) is determined by relative evaluations of transaction time. Observe the workload of the other server; and the server having the less load will score higher if the server has more workload (delays in handling the current request). The server's delay time will be taken into account when calculating each server's trust rating.

Evaluation of Trust (Final Score): The trust evaluation will be conducted based on customer feedback marks, request rejection, server workload, and server selection for customer service while sending requests will be based on this trust evaluation. The following formula is used to determine the final score:

$$Final\ score = weight\ feedback + weight\ queueload + weight\ rejection \quad (1)$$

where, $$weight\ feedback = feedback(i)/Total\ feedback \quad (2)$$

$$weight\ queueload = 1 - (queueload(i)/Total\ queueload) \quad (3)$$

$$weight\ rejection = 1 - (rejection(i)/Total\ rejection\ ) \quad (4)$$

B. The Proposed Framework's Dataflow Diagram

Figure 2 depicts the proposed framework's dataflow diagram, which depicts the process by which a registered or authentic user submits a request to upload data and receives confirmation from the administrator. The user can select the data to be sent once the request is confirmed, and that data will be retrieved from the cloud storage. The user will then be able to view the final value of the trust or result after using the server's services and providing feedback about them. These comments will be directed to the administrator for additional trust estimation. Also, utilizing these trust esteems, the course of choosing the server will be done.

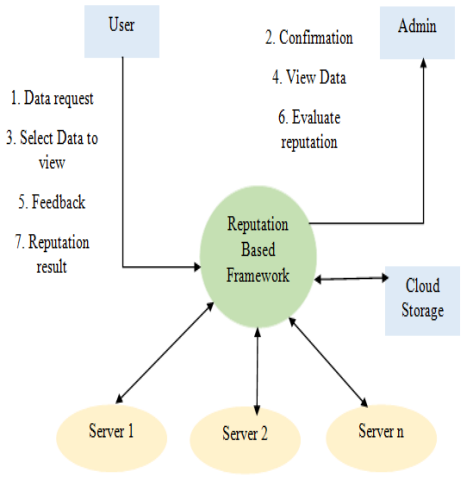

Figure 2 indicates the Data Flow Diagram

C. Approach based on fuzzy logic

The inference procedure typically consists of five major steps, as depicted in Fig.3.

Engine for Inference: The inference engine determines the fuzzy logic operators and defuzzifier utilized in the inference process.

Benefits of Membership: The membership function determines to what extent the fuzzy element is a part of the associated fuzzy set. The membership function maps the values to membership degrees between 0 and 1. The fuzzy inference system assigns its own set of membership functions to each and every input and output variable.

Rulebase:Rulebase, a collection of "If-Then" rules, defines the inference model.

Fuzzification: The input values are transformed into membership functions for a particular fuzzy set-in order to obtain the corresponding membership degrees for each input variable.

Defuzzification: A value is created from an aggregated fuzzy set by employing a specified defuzzification algorithm.

The trust value is generated as a result and delivered to the intended user. Users send data with a high trust value after receiving the trust value. Finally, based on trustworthiness, cloud users can download data from the cloud.

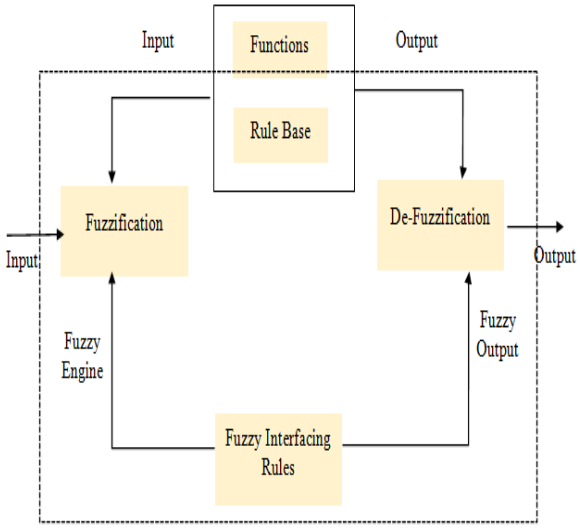

Figure 3 indicates the Fuzzy Inference Process

D. Algorithm and Flowchart of Reputation Computation

The pseudocode for the reputation computation algorithm is described in this subsection. The inputs for this algorithm are feedback from clients, rejection rates from servers, and server queue loads. Additionally, the output of the algorithm is the server's final trust level.

1. INPUT: Rejection score of the server, Feedback of the server, Servers Queue load
2. OUTPUT: Final trust computation score of the server
3. Start
4. Let k be the count of servers
5. Compute the total score of the server’s form feedback and save it in the variable Total Feedback. Estimate the servers total score form queue load and save it in Total Queueload.
7. Compute the servers total score from the rejection as well as save it in the variable total rejection.
8. The Final_Score is initialized as 0
9. for i=1 to k
10.Get the score of the feedback, score of the queue score and the servers rejection scores
11.Computeequation (2)
12.Compute equation (3)
13.Compute equation (4)
14.Compute equation (1)
15.End for
16.if FinalScore<1 then the Trust value is consideredas LOW
17.else FinalScore>3 then the Trust value is considered as HIGH
18.else Trust is considered as MEDIUM
19.End

IV. SIMULATION RESULTS

The experiments of the proposed trust-based reputation framework are carried out to evaluate the proposed trust evaluation framework's effectiveness and accuracy. After utilizing a server's service, the user's cumulative feedbackis displayed in the tablesgiven below for each server.

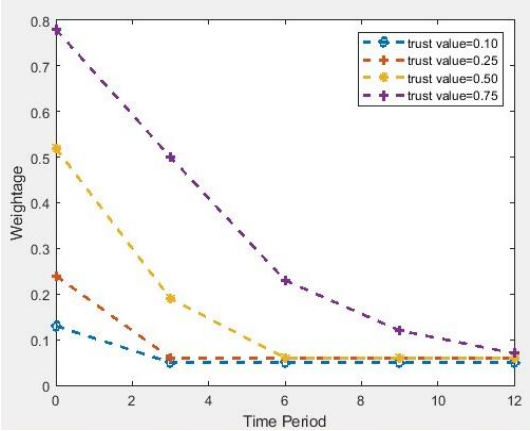

Figure4 indicates Weightage of the cloud services in accordance with trust and time values

The feedback that trustworthy users provide to their recommenders can be used to project the local trust value.Since the services' trust values are always between 0 and 1, Fig. 4 shows that if the trust value is 0.1, the time period is used to calculate the services' weight.The weightage is below 0.1 for the extensive time period as well as the lowest trust value. If the trust value is 0.25, the weightage value computation is beneath 0.2, if it is 0.50, the weightage value computation is beneath 0.4, and lastly, if the trust value is 0.75, the weightage value computation is closest to 0.5.

Table 1. Server feedback scores.

Servers	Feedback
1	80
2	95
3	56

The formula for determining the feedback weight for all the server will be based on the feedback score.

$$Weight\_feedback(k) = feedback(k)/Sum\_feedback \quad (5)$$

where kis the identity (ID) of the server.For instance, the following formula determines the weight of feedback for server 1:

$$Weight\_feedback(k) = 80/255$$

Correspondingly, for everyserver the corresponding feedback weights are estimated as well asthe result is represented as revealed in the below figure 5.

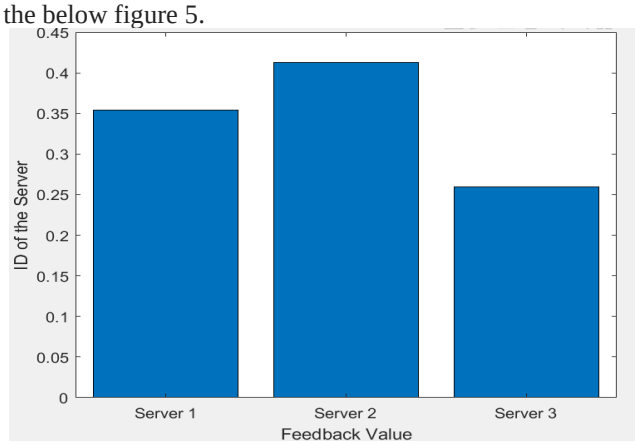

Figure 5 indicates Feedback score for every Server

The number of requests rejected by each server when handling customer requests is another important aspect of the proposed trust-based reputation framework. The rejections by each server are shown in the table.

Table 2. Server rejection scores.

Servers	Score for rejection
1	12
2	47
3	40

Based on the weight of rejection for each server will be determined using the formula

$$Weight\_Rejection(k) = 1 - (Rejection\ (k)/Sum\_rejection) \quad (6)$$

where kis theid of the server.For instance, the following formula is used to determine server 1's rejection weight:

$$Weight_{feedback(k)} = 1 - (12/104) = 0.8846$$

The weight for each server's rejection will also be estimated, and the output is illustrated in figure 6.

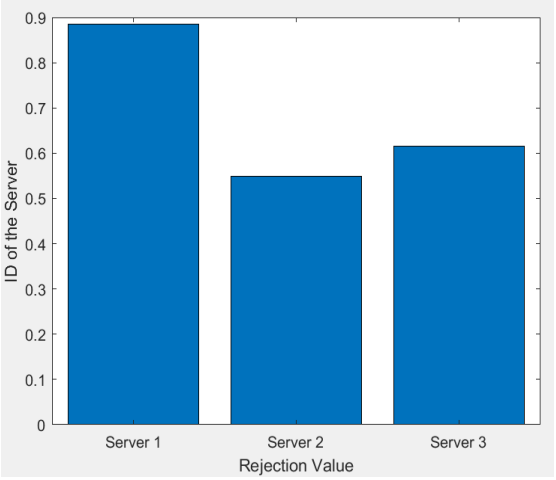

Figure 6 indicates the Every Server Rejection value

The trust evaluation process also takes into consideration workload. The load each server experiences when processing requests is shown in the table.

Table 3. The workload scores of the Server

Servers	Score of workloads
1	33
2	38
3	32

Grounded on the workload weight for all server is estimated using the following mathematical expression

$$Weight\_Workload(k) = 1 - (Workload\ (k)/Sum\_workload) \quad (7)$$

where k is the id of the server.Server 1's workload weight, for instance, is determined as follows:

$$Weight\ workload\ (k) = 1 - (33/110) = 0.7$$

The weight for each server's workload will be calculated similarly, as shown in figure 7.

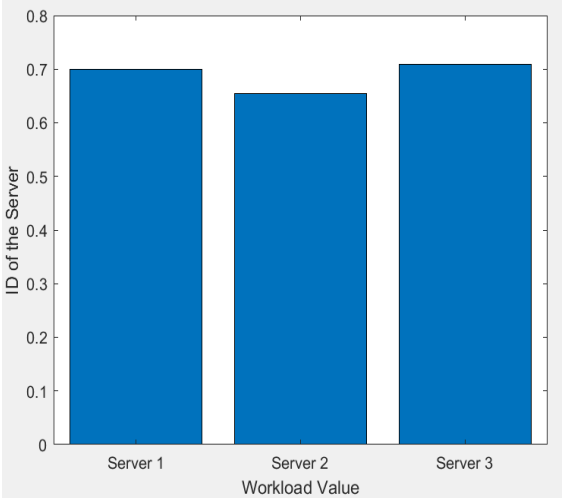

Figure 7 indicates Server's Workload value

Each server's final trust value will be determined by taking into account all three factors-feedback, rejection, and workload—for instance, server 1 has a final trust value of 1.9383, which is the sum of the weights for server 1's feedback, rejection, and workload. The final trust will be calculated similarly for each server, and the trust values that result are shown in figure 8.

Table 4. Final trust value of the server

Servers	Overall trust
1	1.9383
2	1.6151
3	1.5839

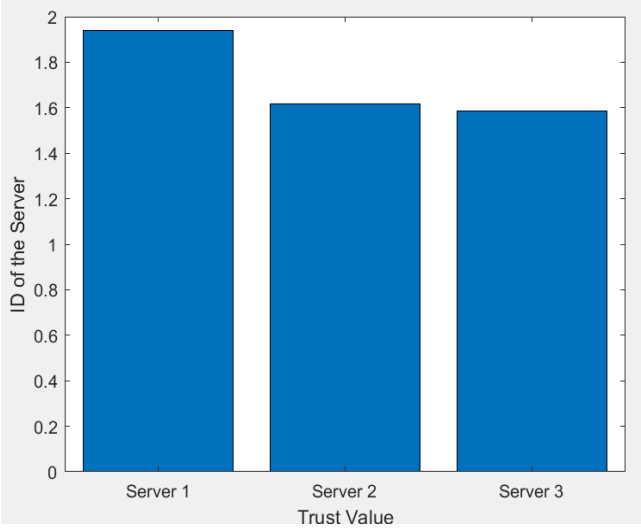

Figure 8 indicates the Final Server's Trust value

In figure 9, the trust accuracy is plotted against the count of user ratings, with the accuracy increasing with the number of ratings. The comparison is done with the existing Trust based reputation framework and the proposed trust-based reputation framework with fuzzy approach. From graph it is obvious that the proposed fuzzy based framework shows high accuracy.

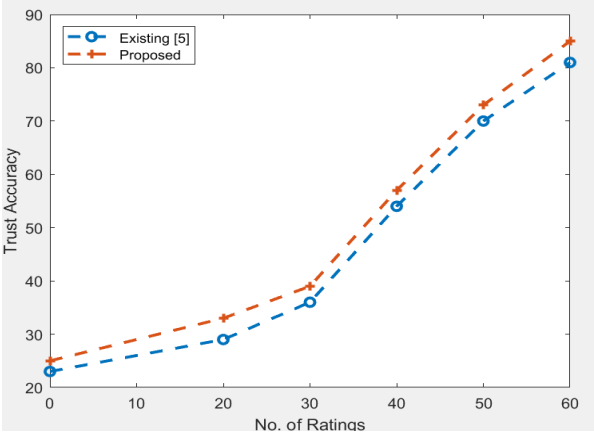

Figure 9 indicates the Trust accuracy

V. CONCLUSION

Cloud computing has arisen as an exciting as well as rapidly expanding area of research along withexpansion in recent years. However, the issue of trust in cloud computing is a main concern for the majority of cloud customers, to the point where trust is widely regarded as one of the greatest barriers to cloud computing adoption and growth. A trust model must be created in order to evaluate trust management systems. A reputation-based trust framework for assessing trust is given in this paper, taking into account the server's rejection rates, queue load, and user feedback in great detail. The experimental findings demonstrate that the proposed algorithm is effective at establishing trust among service providers and customers. The future plan is to begin research on the solution to the trust revision problem, trust timeliness, trust storage, and trust propagation in the cloud.

REFERENCES

[1] Balasubramanian, Muthusenthil, and Hyunsung Kim. "Trust evaluation scheme for cloud data security using fuzzy based approach." Int. J. Appl. Eng. Res 12, no. 13 (2017): 3908-3913.

[2] Fernandez, George. "An overview: Trust and reputation in cloud services." National Journal on Advances in Computing and Management 6, no. 2 (2015).

[3] Mangla, Neeraj, Sanjeev Rana, and Manpreet Singh. "Trust based cloud framework for service provider selection." In Advances in Computational Sciences and Technology, vol. 10, no. 8, pp. 2519-2525. Research India Publications, 2017.

[4] Birje, Mahantesh N., Praveen S. Challagidad, R. H. Goudar, and Manisha T. Tapale. "Cloud computing review: concepts, technology, challenges and security." International Journal of Cloud Computing 6, no. 1 (2017): 32-57.

[5] Prithi, S., D. Sumathi, T. Poongodi, and P. Suresh. "Trust Management Framework for Handling Security Issues in Multi-cloud Environment." In Operationalizing Multi-Cloud Environments, pp. 287-306. Springer, Cham, 2022.

[6] Bhavyashree, S. P., J. Thriveni, and K. R. Venugopal. "Integration of Wireless Sensor Network and Cloud Computing Using Trust and Reputation Technique." In Emerging Research in Electronics, Computer Science and Technology, pp. 69-82. Springer, Singapore, 2019.

[7] Xu, Jianlong, Xin Du, Weihong Cai, Changsheng Zhu, and Yindong Chen. "MeURep: A novel user reputation calculation approach in personalized cloud services." PloS one 14, no. 6 (2019): e0217933.
[8] Papadakis-Vlachopapadopoulos, Konstantinos, Román Sosa González, IoannisDimolitsas, DimitriosDechouniotis, Ana Juan Ferrer, and SymeonPapavassiliou. "Collaborative SLA and reputation-based trust management in cloud federations." Future Generation Computer Systems 100 (2019): 498-512.
[9] Kurdi, Heba, AuhoodAlfaries, Abeer Al-Anazi, Sara Alkharji, MaimonaAddegaither, Lina Altoaimy, and Syed Hassan Ahmed. "A lightweight trust management algorithm based on subjective logic for interconnected cloud computing environments." The Journal of Supercomputing 75, no. 7 (2019): 3534-3554.
[10] Ahmed, Monjur, and Krassie Petrova. "A Zero-Trust Federated Identity and Access Management Framework for Cloud and Cloud-based Computing Environments." (2020).
[11] Mehraj, Saima, and M. Tariq Banday. "Establishing a zero trust strategy in cloud computing environment." In 2020 International Conference on Computer Communication and Informatics (ICCCI), pp. 1-6. IEEE, 2020.
[12] Benmenzer, Faiza, and Rachid Beghdad. "An adaptive formal parallel technique with reputation integration for the enforcement of security policy in the cloud environment." Computer Communications 196 (2022): 207-228.
[13] Sun, Pan Jun. "Privacy protection and data security in cloud computing: a survey, challenges, and solutions." IEEE Access 7 (2019): 147420-147452.
[14] VENKATESH, NAKKA, PATHIPATI VENKATA PRASANNA KUMAR, and K. BHARATH KUMAR. "CLOUD SERVICES FOR SUPPORTING REPUTATION BASED TRUST MANAGEMENT."
[15] Kapetanidou, IoannaAngeliki, Christos-Alexandros Sarros, and Vassilis Tsaoussidis. "Reputation-based trust approaches in named data networking." Future Internet 11, no. 11 (2019): 241.
[16] Zhao, Tianyu, Ernest Foo, and Hui Tian. "A Lightweight Blockchain-Based Trust Management Framework for Access Control in IoT." In Secure and Trusted Cyber Physical Systems, pp. 135-175. Springer, Cham, 2022.
[17] Challagidad, Praveen S., Vani S. Reshmi, and Mahantesh N. Birje. "Reputation based trust model in cloud computing." Internet Things Cloud Comput 5, no. 5-1 (2017): 5-12.
[18] Srinivas, Vegi, Vatsavayi Valli Kumari, and K. V. Raju. "Perseverance of Uncertainty in Cloud Storage Services through Reputation Based Trust." Int. J. Netw. Secur. 20, no. 5 (2018): 951-959.
[19] Singh, Ashish, and Kakali Chatterjee. "A multi-dimensional trust and reputation calculation model for cloud computing environments." In 2017 ISEA Asia Security and Privacy (ISEASP), pp. 1-8. IEEE, 2017.
[20] Wang, Yubiao, Junhao Wen, Xibin Wang, Bamei Tao, and Wei Zhou. "A cloud service trust evaluation model based on combining weights and gray correlation analysis." Security and Communication Networks 2019 (2019).
[21] Ghafoorian, Mahdi, DariushAbbasinezhad-Mood, and Hassan Shakeri. "A thorough trust and reputation based RBAC model for secure data storage in the cloud." IEEE Transactions on Parallel and Distributed Systems 30, no. 4 (2018): 778-788.
[22] Alsenani, Yousef S., Garth V. Crosby, Khaled R. Ahmed, and Tomas Velasco. "ProTrust: a probabilistic trust framework for volunteer cloud computing." IEEE Access 8 (2020): 135059-135074.
[23] Ruan, Yefeng, and Arjan Durresi. "A trust management framework for clouds." Computer Communications 144 (2019): 124-131.
[24] Li, Xiang, Qixu Wang, Xiao Lan, Xingshu Chen, Ning Zhang, and Dajiang Chen. "Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach." IEEE Access 7 (2019): 9368-9383.