Internet of Things and Cloud Computing
2017; 5(5-1): 5-12
http://www.sciencepublishinggroup.com/j/iotcc
doi: 10.11648/j.iotcc.s.2017050501.12
ISSN: 2376-7715 (Print); ISSN: 2376-7731 (Online)

Reputation Based Trust Model in Cloud Computing

Praveen S. Challagidad[1], Vani S. Reshmi[1], Mahantesh N. Birje[2]

[1]Department of Computer Science and Engineering, Basaveshwar Engineering College (Autonomus), Bagalkot, India
[2]Center for Post Graduate Studies, Visvesvaraya Technological University (VTU), Belagavi, India

Email address:
praveensc07@gmail.com (P. S. Challagidad), vani.reshmi24@gmail.com (V. S. Reshmi), mnbirje@yahoo.com (M. N. Birje)

To cite this article:
Praveen S. Challagidad, Vani S. Reshmi, Mahantesh N. Birje. Reputation Based Trust Model in Cloud Computing. *Internet of Things and Cloud Computing*. Special Issue: Advances in Cloud and Internet of Things. Vol. 5, No. 5-1, 2017, pp. 5-12.
doi: 10.11648/j.iotcc.s.2017050501.12

Received: July 4, 2017; **Accepted**: July 5, 2017; **Published**: August 25, 2017

Abstract: Cloud computing offers cost-effective dynamic, scalable and shared services for enterprises from remote data centre. The data stored in cloud storage is increasing day by day dramatically. Though the problem of trusting cloud computing is a highest concern for most enterprises in such a way that trust is widely regarded as one of the top obstacles for the adoption and growth of cloud computing. So there is a need of trust model which help cloud consumers to find the provider that best satisfies their trust concerns in cloud computing by measuring the trustworthiness of Cloud Service Provider (CSP). In this paper we propose a reputation based trust model which will evaluate the reputation of service provider by using a trust evaluation algorithm that will take customers feedback, server rejection rate and server workload into consideration. The experiments show that the trust result is more efficient.

Keywords: Cloud Computing, Feedback, Trust, Trust Evaluation

1. Introduction

Now-a-days Cloud Computing has grabbed the attention of many as a new computing paradigm with obsequious and on-demand infrastructures, platforms and software as service. It provides a way by which one can get access to the applications as utilities over the internet. So it is the biggest trend in current technology where the main idea is "when you can rent what is the need to buy".

According to NIST (National Institute of Stands and Technology) three types of delivery models for delivering cloud services are SaaS, Paas and IaaS. In IaaS resource like memory, database, storage, hardware, servers are made available to the customer. In PaaS applications can be developed by user with reduced cost and development time as he need not to worry about purchasing, installing and maintaining of hardware or software. In SaaS using internet applications are available to the customers which are provided by the different service providers or vendors.

Cloud Computing has public cloud, private cloud, community cloud and hybrid cloud as the deployment models which defines the type of admittance to the cloud. The public cloud makes services and system to be accessible to public. The private makes services and system to be accessible within organization. Community cloud makes services and system to be accessible by group of organization. Hybrid cloud is blend of public and private cloud.

1.1. Benefits of Cloud Computing

a) Scalability-one of the benefit of using cloud computing is scalability which means we can add storage, Random Access Memory (RAM), Central Processing Unit (CPU) and many as our needs grow.

b) Resilience- to minimize the downtime cloud providers have the mirrored solutions.

c) Homogeneity- An open cloud environment makes it easy to work with other groups without bought ring which cloud provider an organization uses.

d) On-Demand self service- A customer can provision computing capabilities automatically.

e) Broad network access- Capabilities are available over the network and can be accessed by different clients.

f) Resource polling- Customer has no knowledge over exact location of provided resource i.e. location

independence.

g) Pay for use and as needed.

Though there are many benefits of cloud computing there exists many challenges to adopt cloud computing some of them are listed below.

1.2. Challenges of Cloud Computing

a) Security is all about confidentiality, integrity and availability of data or information [1, 10].

b) Privacy is protection and appropriate use of customer's personal data.

c) Trust revolves around assurance and confidence about people, data or process will function in expected way.

d) Interoperability in cloud comes to existence when the customer is given freedom to switch between alternative providers since there exists difference in the use of platforms, hypervisors and policies.

e) SLA is service level agreement which guarantees the delivery of service from the provider.

Trust and security are the two major challenges in cloud computing paradigm which hinders the growth of the cloud and hampers the cloud acceptance [1]. To enhance the security of cloud computing paradigm a trust evaluation and management model is being designed here. From the above listed challenges trust is taken out to be as a main hurdle that needs to addressed in cloud computing therefore, trust in cloud computing is explained in next section.

1.3. Trust and Reputation in Cloud Computing

In every social transaction trust and reputation are considered as indispensable elements which are slightly different from each other. In particular context, trust can be defined as subjective anticipation or expectation for one entity by another. Trust is considered to happen between two people and takes time and effort to build and can be lost easily.

Features of Trust

The main features of Trust are as follows:

a) Subjective, uncertainty and fuzzy. Trust pertains to personal mindset or experience and it is not attached to particular boundary.

b) Asymmetry. If two entities say A and B have to set trust association, A's estimated trust for B can be diverse from B for A.

c) Faithlessness and context-sensitive. Trust will get revolutionized along with particular time and particular context.

d) Condition based transitivity. A's trust value for B is not always the same to the recommended trust that is gained from entity C.

On other hand Reputation is a belief about an entity by the community. Entities prior interactions can be used to derive this belief that is from direct or indirect experiences. Direct experience in the sense the trust that is formed based on direct interaction between the customer and provider, while indirect experience means trust is built from observations of interaction between entities or from recommendation given by other entities.

In a community if an entity has high reputation then it is said to be trusted by many in that community. Therefore the trust level of an entity can be calculated using its reputation. Reputation is very essential in cloud computing since it will influence the cloud users therefore cloud providers must try to attain higher reputation. Complete score based on global opinion and score for the performance will show the reputation of an entity. The reputation based trust model will collect the feedback and opinions from the cloud users and evaluate trust of service provider that is the trust model will select the most reliable and trustworthy CSP by evaluating the user's feedback.

2. Literature Survey

In paper [2], author proposed Hierarchical Attribute-based User Classification algorithm to prevent the access of information from less privileged users that is meant for highly privileged users. To do so author proposed delegation approach. Further to provide the physical control of data to data owner author has divided the data into three categories (such as PNR: Privacy Not Required, PRTP: Privacy Required with Trusted Provider and PRNTP: Privacy Required with Non-Trusted Provider). Results and analysis section shows that their proposed algorithm is efficient.

In paper [3], the survey of various trust based model in cloud computing were studied and analyzed. And discussion is made on how the security of cloud computing environment can be enhanced using trust models. And author has also discussed about various security measures and trust mechanism.

A dynamic method of trust evaluation which deals with the behavior of user by using Entropy method has been described in [4] which reveals the user behaviors regular pattern with this author has used AHP to fit subjective expectations of the users in result. Thus keeps a balance between subjective and objective expectations in final trust evaluation result.

A model for trust evaluation on the bases of Expectancy Disconfirmation Theory model and Bayesian network has been discussed in [5]. This model has four main components firstly the Expectation which defines customer's anticipation about service & its performance, then comes perceived performance which indicates customer's experience after using service then disconfirmation is another component which indicates difference between expectation and performance and the last one is satisfaction based on disconfirmation and perceived performance user can tell his satisfaction level which directly proportional to trust.

In paper [6], author proposed a trust model where according to the needs of the customer, he will select the service provider (SP) based on the trustworthiness of SP in market. Here trust evaluation is carried out by using three different viewpoints, one is a trusted third party monitors the cloud users and cloud providers interaction and gives score to

the provider, also customers feedback and past experience are also considered to find the trustworthiness of provider.

A reputation based trust management framework is described in [7] which serves trust as a service and includes credibility model to measure the credibility of the feedback given by the customer, and has an availability model to implement the decentralization of trust service.

A trust management model based on multi-agent and trust evaluation has been described in [8]. It adopts the centralized distribution management mode and sets up multiple third-party agents in the cloud; furthermore, it can manage the users and cloud services by the collaboration of the agents effectively. By using multiple third-party agents, it can reduce the single-agent's pressure of computation, storage and the users' waiting time. The experiment shows that the trust management model is effective. This paper proposes a cloud trust model based on multi-agent, using centralized distribution management mode to manage users and cloud services. It uses direct trust-value, indirect trust-value and comprehensive trust-value to make the trust evaluation of users and service providers. The experiment shows that using multi-agent can reduce the pressure of storage and it can also reduce the user's waiting time when there are large numbers of notes. The trust management model is effective.

In paper [9], the author proposed a trust model based on fuzzy mathematics where the trust between the cloud entities will be built using fuzzy relation theory that is a trust model which is built on the basis a fuzzy recommendation in cloud environment.

A SLA aware trust model is proposed by an author in [11], which calculates the trust using weight based metrics and many SLA parameters like availability, throughput, efficiency, response time etc, between customer and provider are also considered.

A reputation revision method which filters the unfair ratings or feedback given by the user has been discussed in [12] to do so it uses prior knowledge as base while calculating average rating with this they have also used market mechanism which increases the performance by allowing the users and providers to adjust their choice of service and its configurations.

Author presents a feedback based model to calculate trust is described in paper [13]. It removes collusive users and irresponsible users from rating user set using mathematical formula and the evaluates service reputation from several angles with multiple attributes for example for security service attributes considered are access control, encryption, data security, key management etc.

A model for trust evaluation where the trust score of each service provider participating is determined based on feedback from the users and third party assessment has been discussed in paper [14]. This assessment is done by third party auditor by taking CSA guideline or some standards of security.

In paper [15], author addressed the security, privacy and trust challenges of cloud computing, and proposed some solutions by analyzing the technological, operational and legal issues of cloud computing, taking into consideration of cloud customers. Cloud providers have to safeguard the Privacy and Security of personal and confidential data of organizations and users to provide and support trustworthy cloud computing services. Author has reviewed many papers related to Cloud security, privacy and trust issues, and discussed the various security challenges faced by the Cloud computing by proposing some solutions.

In paper [16], author argues the advantages and the disadvantages of user's satisfaction. In Three turns a trust model has been projected between the cloud provider and the customer. At first turn author considers the users previous experience about the service provided by cloud provider, at second turn user must have information about what are the Advantages and Dis-Advantages of using the cloud and what are all the SLA s associated with it and what level of security it is providing. Now at third turn owner/ user is in the position that he says he trusts or relies on cloud. It also verified that after going through such turns both cloud providers and users can be transparent to each others. Such transparency can develop a trust on cloud providers and their environments.

The problem of setting up trust in hybrid cloud environment is discussed in [17]. The author proposed a distributed framework that allows trust based interaction between the cloud customer and service provider. According to this structure or framework the customer can assign appropriate weights to the services provided by CSP i.e. he will give feedback rates to the provider and this work abets successful dilution of falsified feedback rates.

3. Proposed Model

Trust is one of the top obstacle for the adoption of cloud computing. Trust between the Cloud Customer and the Cloud Provider is unclear and inconsistent. There is a need of trust based security models to overcome the security issues. Hence, we propose a trust model where customer's feedback, servers workload and the number of request rejections of server will be counted for trust evaluation.

3.1. Architecture of Proposed Model

Trust is the subjective expectation of one entity about another within specific context at given time. This trust can be derived from customer's feedback, servers workload and the number of request rejections made by the server as shown in the figure 1 which an architecture of proposed model. The purpose of above architecture is to develop a Trust model that is used for evaluation of trust between the service provider and the customer or client. Where the client will send there request to the use of service provided by the server through network i.e the client will send the request to store or upload/ to play or download his video on to/from the cloud. Based on request delay, request rejection and customer feedback of cloud server, the server selection will be done for customer service while sending the request.

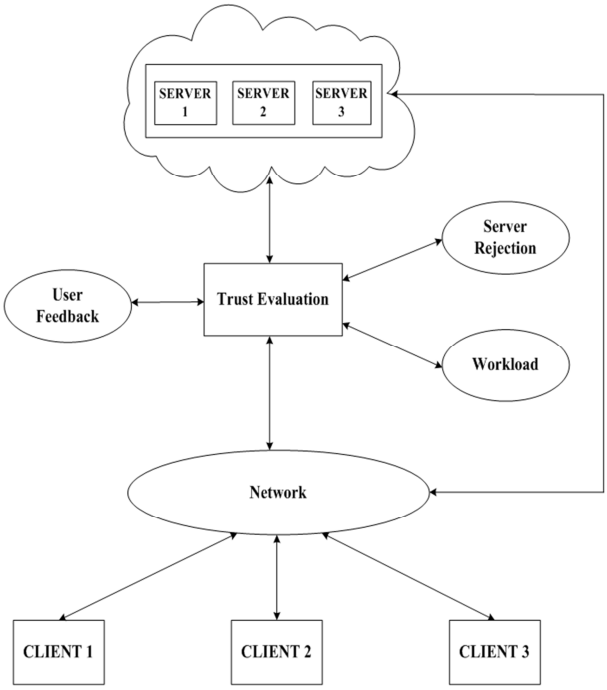

Figure 1. *System Architecture.*

The main factors for the proposed model are as follows:

Trust: Trust is associated with certain attributes such as truthfulness, reliability, security, honesty, depandability, cometence etc, of the trusted entities to act as expected. But entities have no fixed trust value associated with it, it changes accoring to time in specific contexts.

Reputation: Reputation is a belief about an entity based on other entities observation at particular time and context.

Trustworthiness: The quality of service providers service is indicated by trust trustworthiness.

Feedback: Based on the satisfaction user can give the feedback to the service provided by the service provider by answering the set of questionnaires provided in the feedback form. The Cloud Server feature marks will be count for evaluating the trust of the cloud server.

Server Rejection rate: Each server having the Total capacity of request handling, for example let say the capacity be [n=10]. The servers have the threshold level to process the customer request. [Let, Threshold level=7 and Total capacity=10;] While accepting the new request the server will check their threshold level. If no. of request is done with threshold level, then the server will reject the coming new request. [No. of Rejecting of server = X;] The Number of rejection of each server will be observed to calculate the trust evaluation.

Server workload: Initially all server will be ideal, let's say [S1=0, S2=0, S3=0]. First Request will be sent to the server S1 based on first come first service. When Client send next requests, all request will be in queue to get service. To Handle the Queue request, "Queue Work Load Calculation" is done which routes a new call to the server that has the least work load, where work (i.e., load) is based on relative estimates of transaction time. If server having more workload (delay to handle current request) to finish the request then observe other server's workload the server with less load will score more. Server's Delay time will be observed while calculating the Trust evaluation of each server.

Trust Evaluation (Final Score): Based on the Customer feed-back marks, Request Rejection and on workload of server, the trust evaluation will be done and based on this trust evaluation server selection will be done for customer Service while sending request. The formula used for calculating the Final Score is:

$$\text{Final\_Score}=\text{Weight\_Feedback}+\text{Weight\_Queueload}+\text{Weight\_Rejection}.$$

where, $\text{Weight\_Feedback}=\text{Feedback}(i)/\text{Sum\_Feedback}$,

$$\text{Weight\_Queueload}=1-(\text{Queueload}(i)/\text{Sum\_Queueload})$$

& $\text{Weight\_Rejection}=1-(\text{Rejection}(i)/\text{Sum\_Rejection})$

3.2. Dataflow Diagram

The figure 2 shows the dataflow diagram of proposed model where the registered or authentic user will send request to upload a video this request will be confirmed by the admin. Once the request is confirmed the user will select the video to be played and that video will be fetched from the cloud storage. Then after using the services provided by the server the user will give this feedback about the service these will be sent to the admin for further trust evaluation and then the final trust value or result will be available to the user. And using these trust values the process of server selection will be carried out.

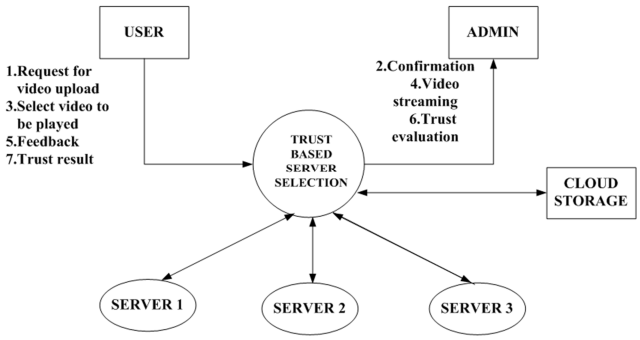

Figure 2. *Dataflow Diagram.*

3.3. Algorithm and Flow Chart of Trust Evaluation

The pseudocode for trust evaluation algorithm is as given below where the input are feedback given by the client, rejection rate made by server and queue-load of the server. And the out is final trust level of the server.

1. INPUT: Feedback of the server, Rejection score of the server, Queueload of server
2. OUTPUT: Final trust evaluation score of the server
3. Begin
4. Let N be the number of server
5. Calculate the servers total score form feedback and store it in Sum_Feedback

6. Calculate the servers total score form queue load and store it in Sum_Queueload
7. Calculate the servers total score form Rejection and store it in Sum_Rejection
8. Initialize Final_Score=0
9. for i=1 to N
10. Fetch the feedback score, queue score & rejection score of servers
11. Calculate Weight_Feedback=Feedback(i)/ Sum_Feedback
12. Calculate Weight_Queueload=1-(Queueload(i)/ Sum_Queueload)
13. Calculate Weight_Rejection=1-(Rejection(i)/ Sum_Rejection)
14. Calculate Final_Score= Weight_Feedback+ Weight_Queueload+ Weight_Rejection
15. End for
16. if Final_Score<1 then Trust Evaluated is LOW
17. else Final_Score>3 then Trust Evaluated is HIGH
18. else Trust Evaluated is MEDIUM
19. End

The flow of the trust calculation process is as shown in below figure 3.

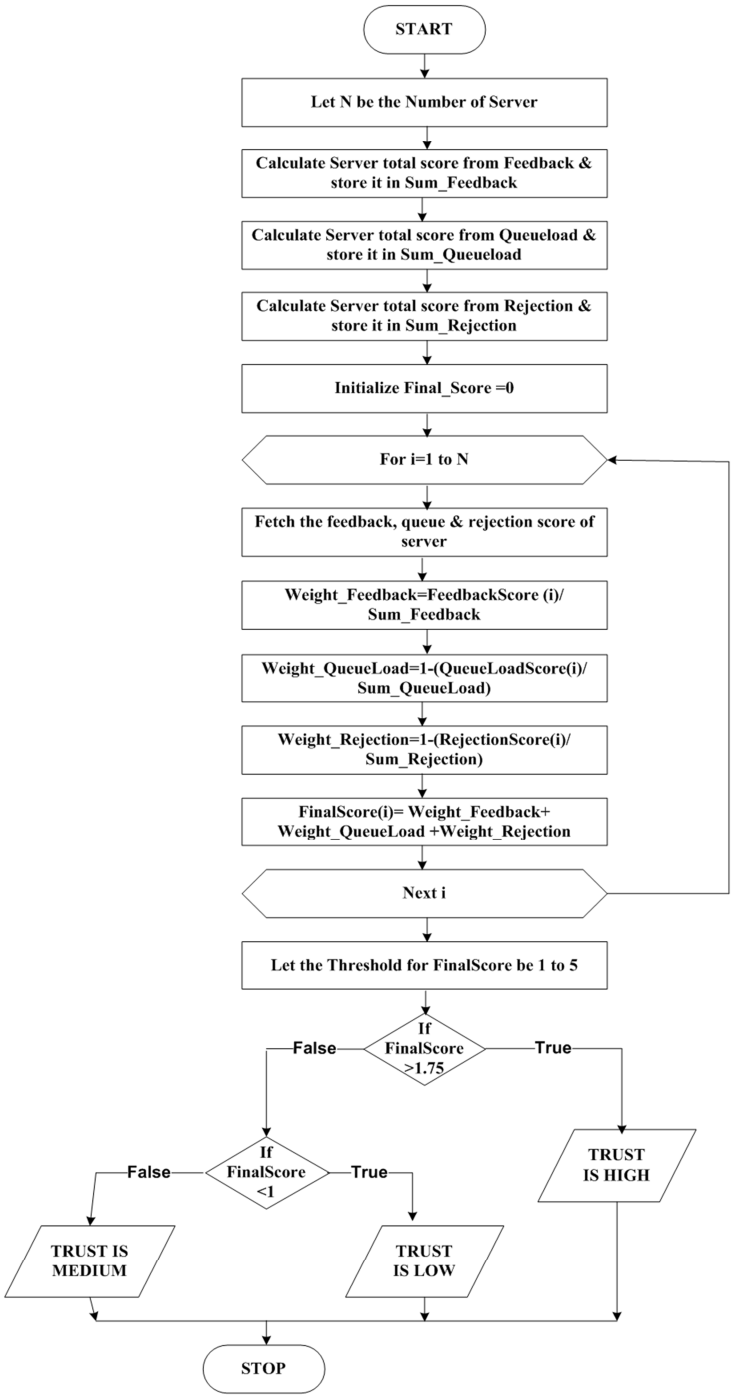

Figure 3. *Flow Diagram of Trust Evaluation Algorithm.*

4. Result Analysis

The Experiments are conducted to measure the efficiency and accuracy of proposed trust evaluation model.

The below table shows the cumulative user feedback given by the user for each server after using the service provided by the server.

Table 1. *Sever feedback scores.*

Server_ID	Feedback _Score
1	78
2	92
3	55

Based on the feedback score weight of feedback for each server will be calculated according to the formula Weight_Feedback (i) = Feedback (i)/ Sum_Feedback, where i is the server id.

For example, the weight of feedback for server 1 is calculated as follows

Weight_Feedback (1) = 78/255=0.3466, similarly for each server the respective feedback weights are calculated and the result is represented as shown in the below figure 4.

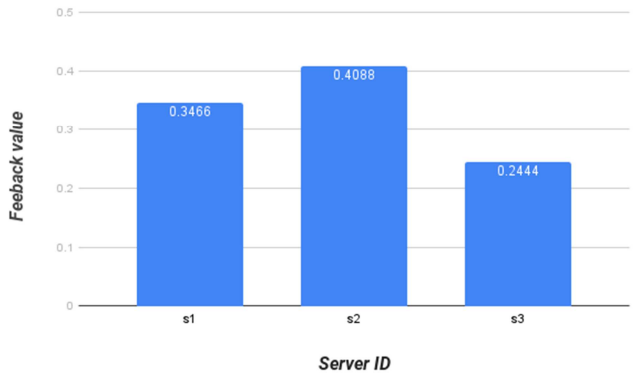

Figure 4. *Feedback score for each Server.*

Another important factor of a proposed model is request rejections made by each server at the time of handling the requests made by customer. The table shows the rejections made by each server.

Table 2. *Sever rejection scores.*

Server_ID	Rejection_Score
1	14
2	48
3	42

Based on the rejection score weight of rejection for each server will be calculated according to the formula Weight_ Rejection (i) = 1-(Rejection (i)/ Sum_ Rejection), where i is the server id.

For example, weight of rejection for server 1 is calculated as follows:

Weight_ Rejection (1) =1-(14/104) =0.8653, similarly weight for rejection of each server will be calculated and the result of same is as shown in figure 5.

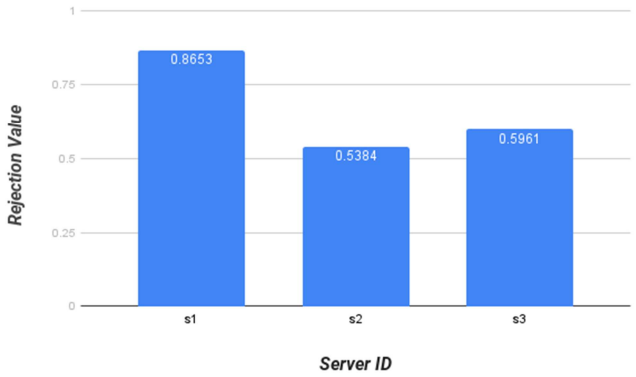

Figure 5. *Rejection value for each Server.*

Workload is another factor that is considered for the trust evaluation process. The table shows the load on each server while handling the requests.

Table 3. *Sever workload scores.*

Server_ID	Workload _Score
1	36
2	40
3	34

Based on the workload weight for each server is calculated using the formula Weight_ Workload (i) = 1-(Workload (i)/ Sum_ Workload), where i is the server id.

For example workload weight for server 1 is calculated as follows

Weight_ Workload (1) =1-(36/110) =0.6727, similarly weight for workload of each server will be calculated and the result of same is as shown in figure 6.

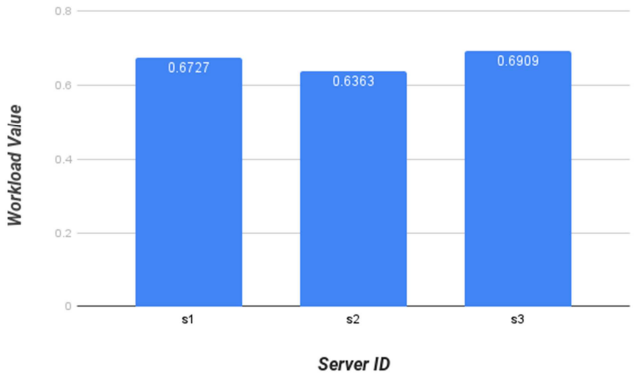

Figure 6. *Workload value for Server.*

The final trust value of each server will be calculated by considering all the three factors that is feedback, rejection and workload of each server for example server 1 has the final trust value of 1.8848 which is of summation value of weight for feedback, rejection and workload of server 1.

Similarly for all the servers the final trust will be calculated and the resulting trust values are as represented in figure 7.

Table 4. *Sever final trust values.*

Server_ID	Total_Trust
1	1.8848
2	1.5837
3	1.5315

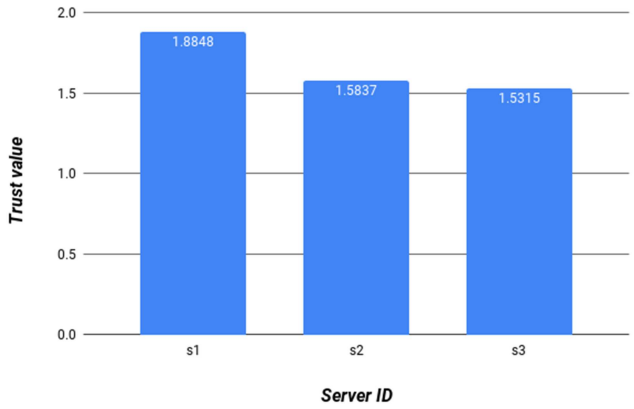

Figure 7. *Final Trust value for Server.*

In figure 8 the trust accuracy is plotted against the number of ratings provided by user where the accuracy will increase as the no of ratings will increase.

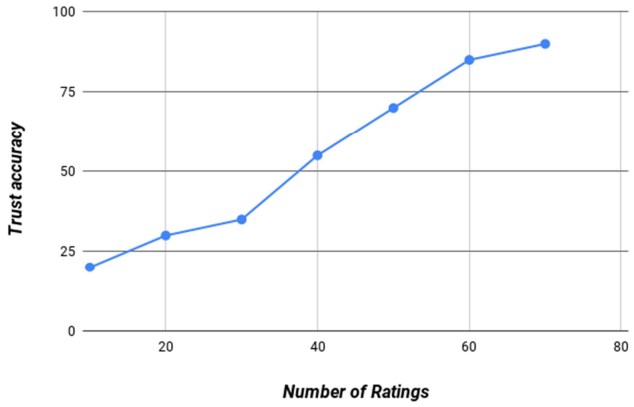

Figure 8. *Trust accuracy.*

5. Conclusion

In recent years, cloud computing has become exciting and fast expanding area of research and development. But, the problem of trusting cloud computing is a foremost concern for most cloud customer's in such a way that trust is widely regarded as one of the top obstacles for the adoption and growth of cloud computing. In order to evaluate trust management systems, trust model needs to be developed. In this paper, a reputation based algorithm for evaluating trust is discussed by considering the feedback from the user, queue load and rejection rates of the server in detail. The experimental results show that the proposed algorithm is efficient for building trust between customers and service providers.

References

[1] Mahantesh N. Birje, Praveen S. Challagidad et al., "Cloud computing review: concepts, technology, challenges and security", *International Journal of Cloud Computing*, Volume 6, Issue 1, 2017.

[2] P. S. Challagidad, M. N. Birje, "Hierarchical Attribute-based Access Control with Delegation Approach in Cloud", *Proceedings of the 11th INDIACom; INDIACom-2017; IEEE Conference ID: 40353 2017 4th International Conference on Computing for Sustainable Global Development*, 2017.

[3] Manisha Sinha et al., "Trust based Mechanism for Secure Cloud Computing Environment: A Survey", *International Journal of Engineering Science Invention*, 2016.

[4] LI Jun-Jian et al., "User's Behavior Trust Evaluate Algorithm Based On Cloud Model", *Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control*, 2015.

[5] Akinwale et al., "Trust: A Requirement for Cloud Technology Adoption", (IJACSA) *International Journal of Advanced Computer Science and Applications*, Vol. 6, No. 8, 2015.

[6] Shivani Taneja, Kavita Rathi, "A Trust Evaluation Model to Recommend a Service Provider to a Customer in Cloud Environment", *International Journal of Computer Applications,* Volume 121 – No. 2, 2015.

[7] Talal H. Noor et al., "Cloud Armor: Supporting Reputation-based Trust Management for Cloud Services", *IEEE Transactions on Parallel and Distributed Systems,* Vol. 0, No. 0, 2015.

[8] Xiaolan Xie et al., "Trust Management Model of Cloud Computing Based on Multi-agent", *International Conference on Network and Information Systems for Computers*, 2015.

[9] Ali. Mohsenzadeh, "Trust Model to Enhance Security of Cloud Computing", *Journal of mathematics and computer science 14*, 2015.

[10] M. N. Birje, P. S. Challagidad, "Security Issues and Countermeasures in Cloud Computing", *International Journal of Applied Engineering Research*, ISSN 0973-4562 Vol. 10, No. 86, 2015.

[11] Shyamlal Kumawat, Deepak Tomar, "SLA-Aware Trust Model Cloud Service Deployment", *International Journal of Computer Applications,* Volume 90 – No 10, 2014.

[12] Qingtao Wu et al., "Reputation Revision Method for Selecting Cloud Services Based on Prior Knowledge and a Market Mechanism", *Scientific World Journal Volume 2014, Article ID 617087*, 2014.

[13] Wanga et al., "An Accurate and Multi-faceted Reputation Scheme for Cloud Computing", *The 11th International Conference on Mobile Systems and Pervasive Computing*, 2014.

[14] Syed Rizvi et al., "A Centralized Trust Model Approach for Cloud Computing", *978-1-4799-5249-6/14/$31.00 © IEEE,* 2014.

[15] Rama Krishna Kalluri, Dr. C. V. Guru Rao, "Addressing the Security, Privacy and Trust Challenges of Cloud Computing", *International Journal of Computer Science and Information Technologies,* Vol. 5, 2014.

[16] Shakeel Ahmad et al., "Trust Model: Cloud's Provider and Cloud's User" *International Journal of Advanced Science and Technology,* Vol. 44, 2012.

[17] Jemal Abawajy, "Establishing Trust in Hybrid Cloud Computing Environments", *International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11*, 2011.