International Journal of Engineering & Technology, 7 (3.29) (2018) 405-408

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A quality feed trust model for data transactions at cloud

Usvir Kaur [1] *, Manish Mahajan [2], Dheerendra Singh [3]

[1] Research Scholar, I. K. G. Punjab Technical University,Jalandhar, Punjab, India
[2] Department of Computer Science & Engineering, CGC Landran, Punjab, India
[3] Department of Computer Science & Engineering, CCET, Punjab, India
**Corresponding author E-mail: usvirkaur@gmail.com*

Abstract

The cloud is one of the most emerging platforms of the modern world. Although the complete cloud model is going to take a while to act practically the research industry has started focusing on the data storage and futuristic transaction problems.This paper focuses on developing a trust model based on the user authentication and feedbacks.The proposed work combines the authentication structures with a job scheduling models which looks into the partition of the job. The proposed model utilized a feedback solution model to maintain the trust model of the cloud executioner. The evaluation of the proposed work is done on the base of Quality of Service (QoS) parameters. The evaluated parameters are also compared with previous QOS trust model.

Keywords: *Trust Model; QOS; Feedback .*

1. Introduction

The Cloud Computing is an emerging platform. Future applications of the cloud may result into super computation and presentation structure [1].The present proposed structure of cloud model contains three layers:

a) Infrastructure as a Service
b) Platform as a Service
c) Software as a Service

As for now the cloud is not completely implemented everywhere, most companies like Google, Apple, Microsoft and other major vendors of cloud use Database as a Service(DAAS) only [2].The structure of the cloud contains the following elements

a) The storage model
b) The execution model
c) The security model

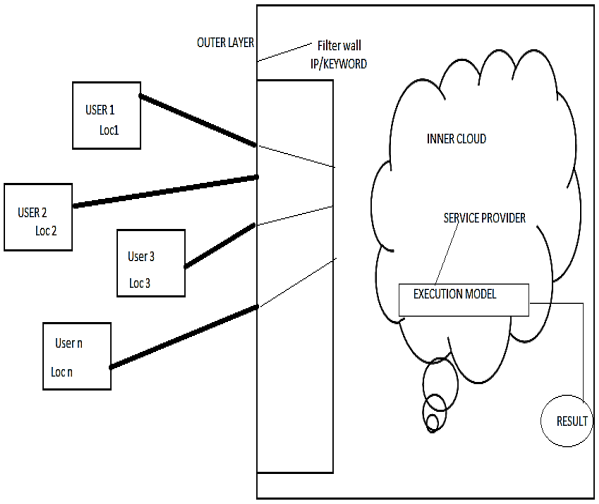

Fig. 1: Execution Model.

The user sends the request to the cloud. There is two layers in the cloud namely outer-layer and inner-layer [3].First of all the user is verified at the outerlayer.The request is filtered and then sent to the innerlayer. The inner-layer has the service execution model and resources to complete the demand of the user requirement [4].The user may or may not lie in the same region as per the location of the user and service provider.

The proposed work model has worked out on both inner and outer layer of cloud.

2. Proposed work model

The proposed work model is divided into three sections.

a) User authentication at the outer layer of Cloud

b) Job Execution at the Intermediate inner layer of Cloud
c) User Feedback update to enhance the trust factor at innermost layer of Cloud

2.1. User authentication

The user authentication system is divided into two subsections [5].
Password Validation
Captcha Authentication

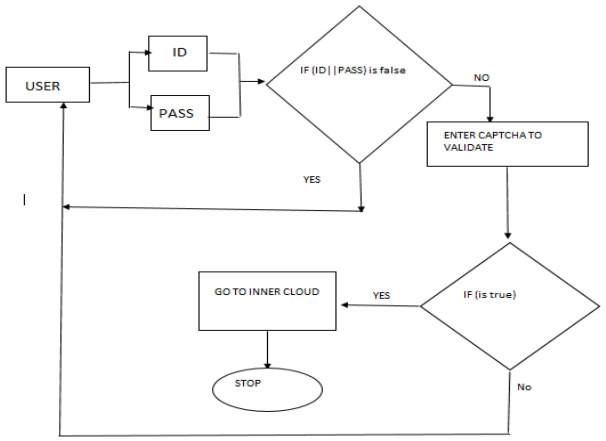

Fig. 2: Validation and Authen0074ication.

The user applies the user id and password.If both the credentials are correct, then the user fills a captcha to authorize that the user is not a robot [6]. If the captcha is correct then the user's request is forwarded to the cloud filter.The cloud filter dumps the unwanted requests [7]. To check whether a request is valid or not, the proposed model applies two types of filter.

a) IP-Filter
b) Keyword Filter

Algorithm 1 demonstrates the working of a filter at the cloud layer.

Algorithm 1: Filter_User_Request(User_Query)	
1.	Extract Keywords(User_Query);
2.	Load Stop_Words_Cloud( );
3.	Flag_found=0;
4.	Foreachkw in keywords // For each keyword in the list
5.	If kw is same as that of spam_words_cloud
6.	Found=1;
7.	End If
8.	End For
9.	If found==1
10.	Dump keyword();
11.	End if
12.	Search IP in the Banned list of IPs
13.	If found then dump the request and issue warning to the user.
End Algorithm	

The filter design looks for spam keywords in the query.If any keyword is found from the spam list, it is dumped and then the filtered list is forwarded [8]. If the IP of the user does not fall under the banned IPs of Cloud then the request is forwarded to the inner cloud else the request is dumped and a warning message is issued to the user.

2.2. Job execution model

The most interesting section of the proposed model is the execution model.This section checks the execution pattern based on the significance of the following elements [9].

a) User Location
b) Available Resources
c) Feedbacks

2.2.1. User location

The user sends its request to the cloud server. The server, first of all, checks the user x and y co-ordinates and then checks that which executioner is closest to the user demand [10].

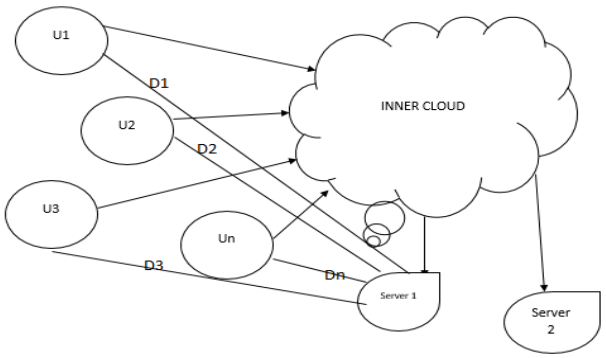

Fig. 3: User Location Service Selection.

A direct co-ordinate geometry distance formula is applied.Algorithm 2 demonstrate the working of Algorithm 2.

Algorithm 2: Location Verifier (User_x,User_y,Ex,Ey)	
//Input: Ex→Executioner_x, Ey→Executioner_y , User_x, User_y	
//Output: Executioner	
1.	Alld=[ ] // All distance values from the executioner to the user
2.	Foreach v in the executioner
3.	Exi=Ex(v)
4.	Eyi=Ey(v)
5.	D=sqrt(User_x-Exi)^2+(User_y-Eyi)^2);
6.	Alld[v]=D;
7.	End for
8.	Find Min[Alld];
9.	Return Executioner
End Algo	

For all the distance values, the proposed structure identifies the minimum distance value. Getting a minimum distance value-doesnot ensure the execution of the job. The nearest executioner may not have all the resources [11]. Hence the nearest executioner will be checked for the resources and if it is satisfied then the job will be allocated to the executioner. If the condition is not satisfied then a 30% distance margin from user to executioner will be applied. This will reduce to the energy consumption of the proposed model.

2.3. Feedback up-dation and trust assignment

When so ever, a job is executed, the proposed model updates the executioner feedback so that it can be referred for the next time.The feedback and the distance model develops the trust of the execution of the user demands [12].

3. Results and evaluation

The following QoS parameters are evaluated:
Turn Around Time: Time to respond to a job
Delay: The total delay in executing the job
Reliability: The trust model is based on the reliability.If it is reliable, it will produce quick results.
Energy Consumption: Total Consumed energy in the execution of user demandss
The results obtained after the simulation are defined below in tabular and graphical form:

Table 1: Turnaround Time Evaluation

No. of jobs	Turnaround time	
	Proposed work	QoS Trust model
100	3	4
200	5	7

500	8	10
1000	7	9
10000	10	13

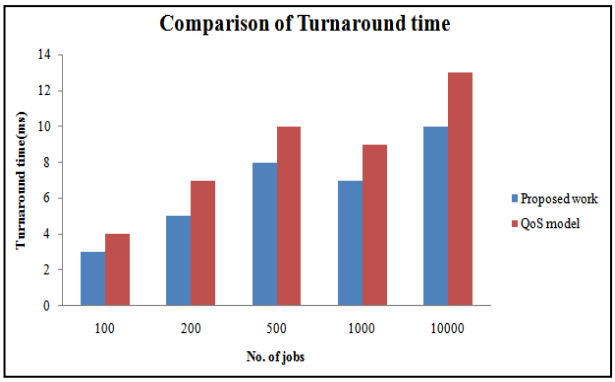

Fig. 4: Comparison of Turnaround Time W.R.T Number of Jobs.

Table 1 and figure 4 describes the outcome of turnaround time by means of number of jobs. As depicted, X-axis defines the number of jobs (100, 200, 500, 1000 and 10,000) whereas Y-axis defines the values depicting the result of turnaround time. The average value for turnaround time to respond the jobs measured for proposed work and existing QoS trust model are 6.6 and 8.6 respectively.

Table 2: Delay Evaluation

No. of jobs	Delay (ms)	
	Proposed work	QoS Trust model
100	35	37
200	39	40
500	32	35
1000	37	39
10000	40	42

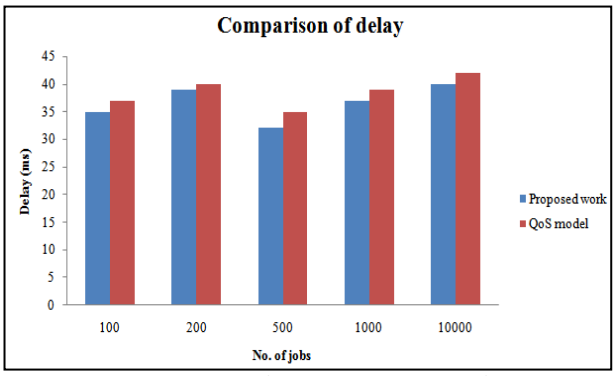

Fig. 5: Comparison of Delay W.R.T Number of Jobs.

The computation of delay is depicted in above figure 5 and table 2. X-axis is defining the number of jobs taken to execute the work and Y-axis defines the delay values obtained after the execution. The main aim of cloud computing is to have less delay that is the time it takes to obtain the outcome.The obtained delay in executing the jobs for proposed and QoS trust model are 36.6 ms and 38.6 ms respectively.

Table 3: Reliability Evaluation

No. of jobs	Reliability	
	Proposed work	QoS Trust model
100	0.12	0.10
200	0.35	0.32
500	0.49	0.42
1000	0.59	0.48
10000	0.89	0.72

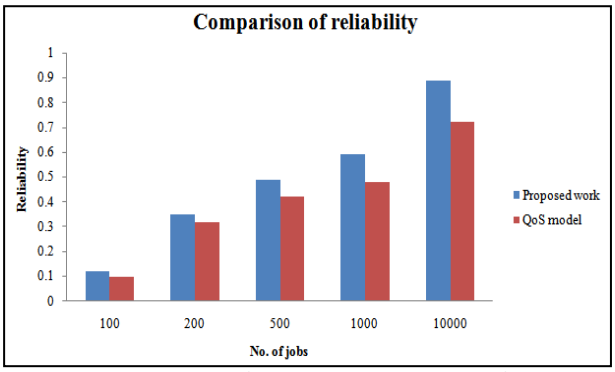

Fig. 6: Comparison of Reliability W.R.T Number of Jobs.

Reliability is the ability to produce the results quickly. As shown in figure, X-axis is for number of jobs and Y-axis is for the values obtained for reliability by means of number of jobs. The average values of reliability measured for proposed and existing work are .488 and 0408 respectively. So, it can be concluded from the obtained value that the proposed work is more reliable to produce quicker and accurate results as compared to the existing work.

Table 4: Energy Evaluation

No. of jobs	Energy Consumption (mJ)	
	Proposed work	QoS Trust model
100	62	67
200	65	66
500	61	62
1000	67	69
10000	70	72

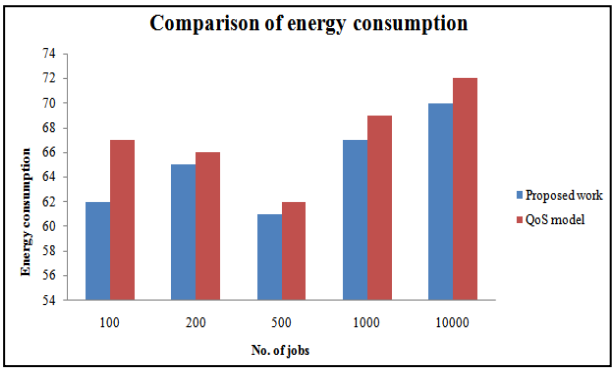

Fig. 7: Comparison of Energy Consumption W.R.T Number of Jobs.

Above figure 7 and table 4 defines the simulation of energy consumption measured for proposed work as well as for existing work. Usually, sever consumes more amount of energy in cloud and energy consumption differs with utilization. Energy efficient cloud generally improves the sustainability of data centers. In this research work, the energy consumption is 65 mJ approximately which is less as compared to the energy consumed by the QoS trust model (67.2mJ), therefore, it can be concluded that the proposed work is more energy efficient than the existing QoS model.

4. Conclusion

This research work has dealt with the cloud computing layers; such as inner layer and outer layer. The aim of this research is to authenticate the user at cloud's outer layer by password validation and Captcha authentication. An execution model has been designed that validates the execution pattern on the basis of user location, feedbacks and available resources. After the execution of the jobs, the executioner feedback is updated that helps in the development of trust model for user demands execution. To check the effectiveness of the proposed work, parameters such as turnaround time, delay, reliability and energy consumption are considered. The average value for turnaround time to respond the jobs is 6.6. The obtained delay in executing the jobs is 36.6 ms. The average value is 0.488

for reliability and the energy consumption is 65 mJ approximately which is less. It has been concluded from the research work that the proposed trust model is reliable and energy efficient.

Acknowledgement

Authors are highly thankful to the department of RIC, IKG, Punjab Technical University, Kapurthala, Punjab, India for providing the opportunity to conduct this research work.

References

[1] M. Ali, S. U. Khan and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges", Information sciences, vol. 305, pp. 357-383, 2015.
[2] M. N.Sadiku, S. M. Musa and O. D. Momoh, "Cloud computing: opportunities and challenges", IEEE potentials, vol. 33, no.1, pp. 34-36, 2014.
[3] N. H.Hussein and A. Khalid, "A survey of Cloud Computing Security challenges and solutions", International Journal of Computer Science and Information Security, vol.14, no. 1, 52-56 , Jan, 2016.
[4] V. Chang and M. Ramachandran, "Towards achieving data security with the cloud computing adoption framework", IEEE Transactions Services Computing, vol.9, no.1, pp. 138-151, 2016.
[5] T. Oliveira, M. Thomas and M. Espadanal, "Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors", Information & Management, vol. 51, no. 5, pp. 497-510, 2014.
[6] J. A. González-Martínez, M. L. Bote-Lorenzo, E. Gómez-Sánchez, and R. Cano-Parra, "Cloud computing and education: A state-of-the-art survey", Computers & Education, vol.80, pp. 132-151, 2015.
[7] A. Hameed, A. Khoshkbarforoushha, R. Ranjan, P. P. Jayaraman, J. Kolodziej, P Balaji, and S. U. Khan, "A survey and taxonomy on energy efficient resource allocation techniques for cloud computing systems", Computing, vol. 98, no. 7, pp. 751-774. 2016.
[8] D. Y. Chang, M. Benantar, J. Y. C. Chang, and V. Venkataramappa, U.S. Patent No. 8,769,622. Washington, DC: U.S. Patent and Trademark Office, 2014.
[9] R. V Auradkar, and R. P. D'souza, U.S. Patent No. 9,165,154. Washington, DC: U.S. Patent and Trademark Office, 2015.
[10] S. S. Manvi, and G. K. Shyam, "Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey", Journal of Network and Computer Applications, vol. 41, pp.424-440, 2014.
[11] C. Colman-Meixner, C. Develder, M. Tornatore and B. Mukherjee, "A survey on resiliency techniques in cloud computing infrastructures and applications", IEEE Communications Surveys & Tutorials, vol. 18, no.3, pp. 2244-2281, 2016.
[12] C. Fehling, F. Leymann, R. Retter, W. Schupeck, and P. Arbitter, Cloud computing patterns: fundamentals to design, build, and manage cloud applications, Springer Science & Business Media, 2014.
[13] M. A. Khan, "A survey of security issues for cloud computing", Journal of network and computer applications, vol. 71, pp. 11-29, 2016.
[14] A. Shawish and M. Salama, "Cloud computing: paradigms and technologies", In Inter-cooperative collective intelligence: Techniques and applications Springer, Berlin, Heidelberg, pp. 39-67, 2014.
[15] S. Singh, Y. S Jeong and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions", Journal of Network and Computer Applications, vol. 75, pp. 200-222, 2016.
[16] R. N. Calheiros, R. Ranjan and R. Buyya, "Virtual machine provisioning based on analytical performance and QoS in cloud computing environments", In 2011 international conference on Parallel processing, IEEE, Taiwan, pp. 295-304. Sept. 2011.
[17] P. Manuel, "A trust model of cloud computing based on Quality of Service", Annals of Operations Research, vol. 233 , no.1, pp. 281-292, 2015.
[18] D. Bruneo, "A stochastic model to investigate data center performance and QoS in IaaS cloud computing systems", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no.3, pp.560-569, 2014.