International Journal of Database Theory and Application
Vol.8, No.5 (2015), pp.161-170
http://dx.doi.org/10.14257/ijdta.2015.8.5.13

A Trust Model Based on Quality of Service in Cloud Computing Environment

Atoosa Gholami and Mostafa Ghobaei Arani

Desectionment of Computer Engineering, Islamic Azad University of Mahallat, Mahallat, Iran
Desectionment of Computer Engineering, Islamic Azad University of Parand, Tehran, Iran
atoosa.gholami@gmail.com, mostafaghobaei@piau.ac.ir

Abstract

In recent years, the popularity of cloud computing technology is widely grown and most organizations want to use this technology in their business processes. But on the other hand, the use of this technology is not easy and many organizations are concerned about storing their sensitive data in their data centers instead of storing them in the cloud storage centers. In the cloud computing environment, trust, as a solution to enhance the security, has attracted the attention of researchers. Trust is one of the most important ways to improve the reliability of cloud computing resources provided in the cloud environment and has an important role in the business environments. Trusting the user to select the appropriate source helps in heterogeneous cloud infrastructure. In this paper, we present the trust model based on standards of appropriate service quality and speed of implementation for cloud resources. Simulation results show that the proposed model compared with similar models, in addition to taking into account measures of the quality of service, selects the most reliable source in a cloud environment by taking into account the speed of things.

Keywords: *Cloud Computing; Trust Model; Reliability; Availability; Quality of Service*

1. Introduction

Cloud computing is one of the newest and most challenging emerging technologies, because of various advantages such as the availability of computing resources and software services when required. With significant advances in IT infrastructure this technology has had a greater impact on the business world. Also the latest emerging trend in distributed computing that delivers hardware infrastructure and software applications as services [1-2]. In cloud computing, computing resources are hosted in the Internet and delivered to customers as services. Although consumers do not have control over the underlying computing resources, they do need to ensure that the quality, availability, reliability and performance of these resources are provided [3-4].

Prior to the commencement of services, the customers and cloud providers negotiate and enter into an agreement named service level agreement. The Service level agreements clarify the roles, set charges and expectations and provide mechanisms for resolving service problems within a specified and agreed upon time period. The service level agreements also cover performance, reliability conditions in terms of quality of service guarantees [5]. These guarantees define required quality of service parameters such as reliability, availability, response time and data integrity on a pay-per-use model.

Besides several advantages of cloud computing, there are security and privacy issues that hinder the adoption of cloud services by various organizations and IT industry. Data confidentiality, data privacy and trust establishment are considered to be the main security concerns for an organization moving its data to the cloud platform. Uncertainty about data

ISSN: 2005-4270 IJDTA

protection and loss of data control are the major reasons for reducing level of trust on cloud providers. Therefore, it is required to establish trust on cloud provider for assuring the data security and obtaining the guarantee about cloud performance [6]. Today, one of the most important factors for the success of cloud computing is to create trust and security. Cloud computing will face a lot of challenges when the key element trust is absent. In cloud computing, trust as a solution to enhance security, has attracted the attention of researchers [7]. Cloud computing has a lot of research focus in recent years and it provides a virtual framework for sharing of resources. In such a geographically distributed environment, an entity has the privilege of using collection of resources. The idea of virtual framework such as cloud is not appealing to some entities because of the risk of being associated with the notion of sharing resources or services. Because of the sensitivity and the vitality of the data or information, such entities prefer to use their own closed box resources. This is not just costly for the individual entities but also an inefficient way to utilize resources. To make cloud computing more attractive, trust must be addressed and trustworthy domains must exist where an entity can use resources or deploy services safely. In such a scenario, the user/consumer and the resource provider does not have complete control over each other. The user/consumer expects good Quality of Service from a trustworthy service provider. The Service providers expect that cloud resources to be protected and it allows the cloud resources to be utilized by a trustworthy consumer [8].

Still there are many challenging issues such as security, encryption of data stored in the cloud and lack of trust in providers. Choosing a reliable service provider is a challenging problem in cloud environment. For commercialization of cloud computing technology, users must trust cloud providers; this means that providers of resources end assigned work on the basis of service level agreement and the information about processed data is secure.

When an enterprise needs to transfer its business critical data on cloud, it prefers to evaluate the trustworthiness of cloud service provider. The different mechanisms, techniques and protocols have been proposed in cloud computing to preferably evaluate the trust score for different cloud services. All these aspects of trust establishment and evaluation methodologies are commonly known as the "Trust Models" in literature. A trust model can be defined as a coded implementation that relay on concepts of trust in order to assign a trust value for a cloud entity on the basis of which the interactions with that specific entity are restricted and controlled. Trust models are used to calculate the trust numerical value for data centers as well as reliable and secure increased schedule in distributed, cloud environments and grid networks [9-10].

The rest of this article is organized as follows: The second section is devoted to the related works and the proposed model is presented in Section III. Evaluation and simulation results of the proposed model are presented in the fourth section and then at the fifth and final section the conclusions and future work are discussed.

2. Related Works

Various studies have been carried out on models of trust in cloud computing environment, which usually are based on agreement, certificate/secret keys, feedback, domain and subjective trust models that they have advantages and disadvantages. We will introduce some of these models:

Ahmad *et al.* [11], have proposed a Trust Model between users and cloud providers establishing trust in three turns and when cloud users are satisfied at first two turns then at third turn they can rely on cloud provider. In first turn user must be satisfied with previous experience of cloud provider, and at second turn user must have knowledge about SLAs (Service Level Agreements) security issues at different levels. User or Organization can trust on reliable cloud provider at third turn.

Caedo *et al.* [12], proposed a trust calculation process and trust model to ensure a reliable files exchange among nodes, in a private cloud, in accordance with the established metrics on basis of history interactions/queries between the nodes. These values are similar to weights in [13] and ranging between [0-1]. The trustworthiness evaluation is based on node storage space, operating system, Network bandwidth and processing capacity. The simulations are done using CloudSim framework to show the efficiency of the model in selecting more reliable node in private cloud. The model has scope of evaluating it further with weights of SLA parameters and other performance indicators. In this trust model, each node has two trust tables containing direct trust table and a recommendation list. To calculate value of trust, first the trust table is checked and the numerical value of trust is used and if the value of trust is not available, the requesting node would review the recommendation list.

Kumar Garg *et al.* [14], offered a framework for measuring the quality and priority of cloud services. This framework has a significant effect on healthy competition among cloud providers to meet service level agreement and improve the quality of their service. They suggested Analytical Hierarchy Process [15] on the basis of a ranking mechanism in which cloud services can be assessed based on the various applications related to quality of service requirements. This proposed method is only used for measurable features of the quality of service such as: accountability, skills, service reliability, cost, performance, security, privacy and usability.

Kumar Goyal *et al.* [16], proposed a trust management model and a trust based on an efficient cost algorithm to "improve the quality of service" for parameters in cloud infrastructure as a service. In this trust model, trust is calculated based on data center parameters (start time, price, processing speed, failure rate, bandwidth) that based on the trust values obtained, trust values of the data is created in two lists of reliable and unreliable data centers. Making use of these lists of reliable and unreliable data centers, scheduling is done. With this schedule, reliable sources are allocated to a user with a higher trust value and unreliable resources are allocated to an untrustworthy user.

Zafar *et al.* [17], offered a model that help users of cloud service to find reliable and efficient suppliers of cloud service based on data taken from the official legislation and the performance of suppliers of cloud service in the past year, and feedback of the customers. It provides a choice for the user to assess providers of various services available based on their reputation in the market based on the quality of their service and selects the most reliable service provider. The main features of this model are, Down Time (inactive time), Up Time, Customer Support Experience, Fault Tolerance Capability and response time. These options are given to customers to select cloud service providers based on their needs.

Manual *et al.* in [15], proposed a trust model based on the previous certification and current potentials of cloud service providers, and called the proposed model as model of trust for the quality of service level. In this model, the trust value is calculated by combining four parameters of availability, reliability, data integrity and Turnaround Efficiency and finally, for each action a cloud source with the highest value of trust will be chosen from list.

Li *et al.* [18], has introduced a Multi-tenant Trusted Computing Environment Model. This model was designed for IaaS layer to secure a reliable cloud computing environment to users. Reliable multi-user computing model has two hierarchical levels in variable trust model (indirectly) that supports the separation of interest between efficiency and security. This model has three identity currents: A) consumers that rent the cloud computing service of cloud service provider B) cloud service provider, which provides IaaS services C) auditor (optional) is recommended that from the user's side is responsible for confirming the fact that the infrastructure provided by cloud service provider is trustworthy. In reliable multi-user computing model, cloud service providers and users cooperate to create and maintain a reliable cloud computing environment.

Zhimin *et al.* [19], for the firewalls in the cloud, offered a collaborative trust model in the domain level. In their proposed trust model, trust is a numerical value that depends on the nature of the entities, past behaviour, *etc.* and its value is not constant. The cloud is divided into several independent domains and trust relationships between nodes are divided into two types: intra-domain trust relationships and inter-domain trust relationships. Inter-domain trust relationships are based on transactions operated within the domain. This model has three advantages: First, it uses different security policies for different domains. Secondly, this model considers transactions nature, old data of entities and their effect on the dynamic measurement of trust value; third, this trust model is consistent with the firewall and does not violate its local control policy.

3. The Proposed Model

The proposed model is a development of trust model in [17]. We call the proposed model Turnaround_Trust trust model; In this model, the cloud resources will be selected according to equation 1:

$$Turnaround\_Trust = w_1 * trust + w_2 * runspeed \quad (1)$$

In which w_1 and w_2 are positive values of trust parameters so that: w_1+w_2=1. In the proposed equation, we also considered two factors of trust and run speed.

The first is trust:

$$Trust \text{ Value of a resource } = w_1 * AV + w_2 * RE + w_3 * DI + w_4 * TE \quad (2)$$

In Equation 2, w_1, w_2, w_3 and w_4 are weights of each parameter so that: w_1+ w_2+ w_3 + w_4=1; the values of these parameters are determined based on their priorities and trust evaluation criteria, including: AV represents accessible and RE represents reliability and DI is data integrity and TE is response time performance).

The second measure is run speed according to the equation 3:

$$RunSpeed\ Value = \frac{CPU_{job}}{CPU_{resource}} \quad (3)$$

The implementation of this trust model by using of the proposed trust management system is shown in Figure 1.

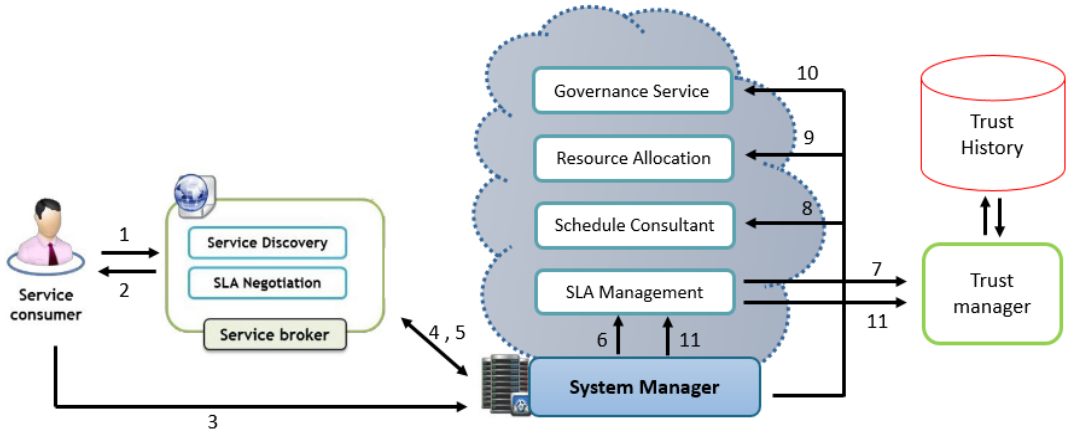

Figure 1. The Trust Model of Proposed

The algorithm of trust model of Proposed is as follows:

Steps 1, 2: The cloud user provides a list of its quality of service requirements reviews Service Discovery and selects a set of cloud resources according to quality of service criteria.

Step 3: User sends requirements list of quality of service and the list of cloud sources selected from the Service Discovery to System Manager.

Step 4, 5: The System Manager reviews accessibility of requested cloud resources through the Service Discovery.

Step 6: System Manager refers requirements of quality of Service and a list of potential cloud resource to the director of the service level agreement.

Step 7: at the same, the reliability and speed of execution of work in each candidate provider is calculated. The SLA Manager collects the trust values of the cloud resources from Trust Manager. Cloud resources are sorted out based on trust and speed of execution of works. After negotiation and agreement with the cloud user through the System Manager, agreement of service is provided. And agreement of the service is given to the System Manager.

Step 8: After selecting the best source, the System Manager consults with Scheduling adviser for scheduling of resources. The proposed policy for the timing of the proposed Trust Model is that we consider the best timing for execute of requests, and a request that has the least Turnaround Time and is executed first.

Step 9: The System Manager provides service level agreement to service allocator. Requested cloud resources are provided and marked. A working environment is virtualized for the user. They also create, customize, manage and expand the needed virtual systems.

Step 10: Concurrently the System Manager provides a service level agreement to Governance Service. Governance Service manages and controls allocated and used resources. It also carries out measurement and billing of cloud services. System Manager delivers given processed data and the bill to the user.

Step 11: The System Manager also forwards the trust attributes AV, RE, and TE regarding the execution of the job to SLA Manager. The SLA Manager updates the Trust Manager with these values AV, RE, and TE. The Trust Manager in turn stores the data in the Trust History. After receiving the processed data from the System Manager, the user tests data and evaluates the service provided by the cloud provider. User evaluates data integrity and updates trust manager with data integrity values. The Trust Manager in turn stores the data in the Trust History.

4. Performance Evaluation

In this section, the toolkit of Cloudsim [20] has been used for the simulation of the proposed method. A user can record several works in which each work with different facilities from calculation parameters such as the different speeds of the processor, memory, hard drive, memory, RAM and network parameters such as latency and bandwidth is to blend the heterogeneous concepts. To evaluate the proposed model we compare it with trust models, FIFO [8], QoS_Trust [17] in metrics of Turnaround Efficiency (TE), Reliability (RE) and Availability (AV) and since our proposed model is based on the criteria of reliability measurements and service quality standards.

Experiment 1: Turnaround Efficiency Metric

Experiment 1 is a sequence of 10 posts. Each post is with 500 developed works. During each post all works are sent together. Posts are distinct in terms of the different number of tasks and different processes of database. The larger the number of jobs, the test results in Figure 2 shows the better performance of the model *Turnaround_Trust* compared with the other two models. In the first experiment it was proved that trust model

Turnaround_Trust has a better performance than models *Turnaround_Trust*, Qos_Trust, FIFO, in the response time.

Performance of response time: the actual response time, is the exact time between requested time of work and the delivery time of work to the user. Promised response time is delivery time by source provider between request time and delivery of done work.

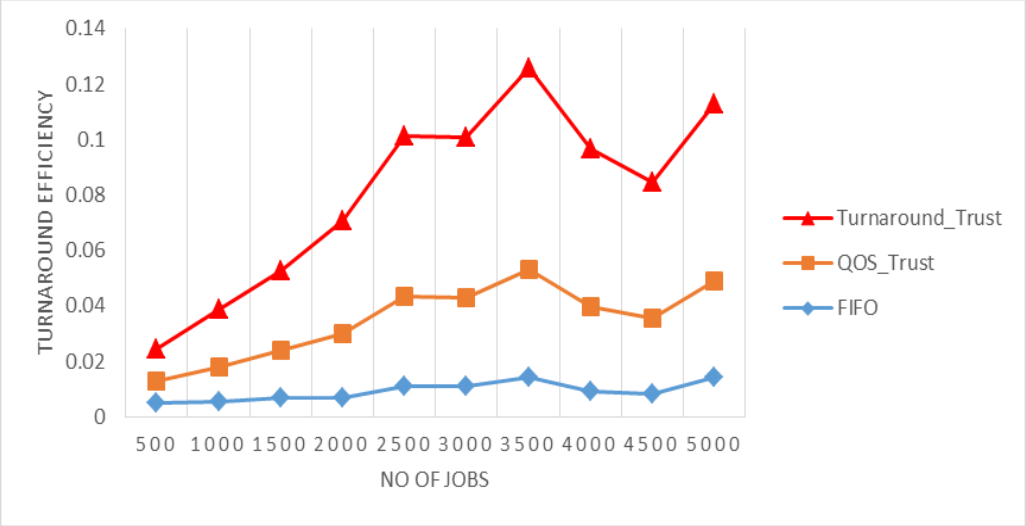

Figure 2. Evaluation of Turnaround Efficiency with Varying Number of Jobs

Figure 3 show the comparison of response time performance of the number of increased jobs and the average based on each trust model on features of response time performance.

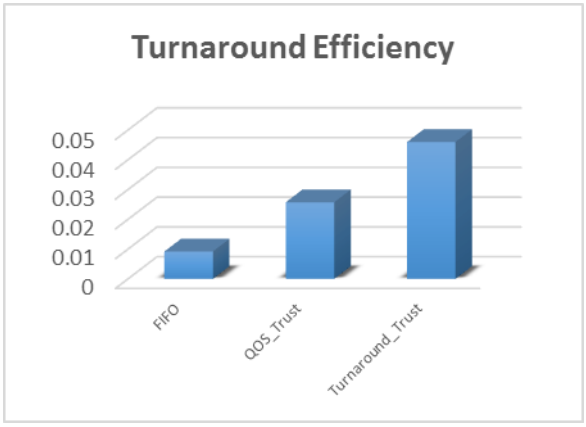

Figure 3. Comparison of Turnaround Efficiency Metric

Experiment 2: Reliability Metric

In the second experiment it was proved that success rate of trust model *Turnaround_Trust* is better than the other two models. The second test consists of a sequence of 10 posts. Post 1 is a collection of 500 works. Post 3 has 1000 works and Post 4 has 1500 and so on. The results of this experiment are shown in Figure 4; so that trust model *Turnaround_Trust* is better than the other two with significant facilities. Reliability is an important component of trust is also called the success rate.

Reliability is the ability of a system or a component required for operation under steady-state conditions for a specific time period. The reliability of a cloud source is a measure of success of a work accepted by the cloud supplier. If A_k is the number of works

accepted by R_K source and C_K is the number of works completed by R_K source in T time limit so reliability is obtained according to equation 4:

$$Reliability\ (RE)\ R_k = \frac{C_k}{A_k} \quad (4)$$

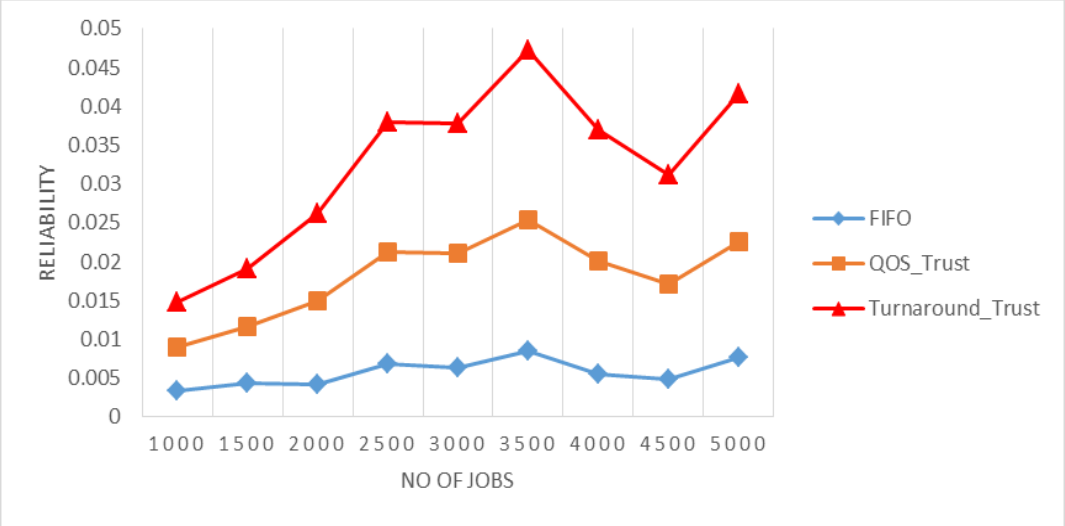

Figure 4. Evaluation of Reliability with Varying Number of Jobs

Figure 5 show the comparison of reliability capability is checking on the number of increased works based on each of trust models over reliability capability.

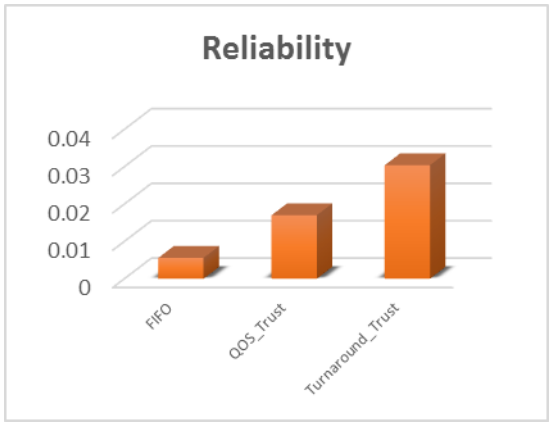

Figure 5. Comparison of Reliability Metric

Experiment 3: Availability Metric

Experiment 1 show evaluation of availability with varying number of jobs. Availability is the degree to which a system or a component is achievable or usable when needed to be used [21]. Resources are called Inaccessible in one of the following conditions: 1. section of the source service is unavailable for users, 2. Resources are idle (OFF), 3. The source is very busy for processing the request.

Suppose R_1, R_2,...R_n are cloud sources, for each K=1,2,...,n, N_k is as the recorded works and A_k is the number of works accepted for cloud sources of R_k in T time limit; so availability is obtained according to Equation 5:

$$Availability\ (AV)\ R_k = \frac{A_k}{N_k} \quad (5)$$

Figure 6 shows how the trust model *Turnaround_Trust* is better than other two models.

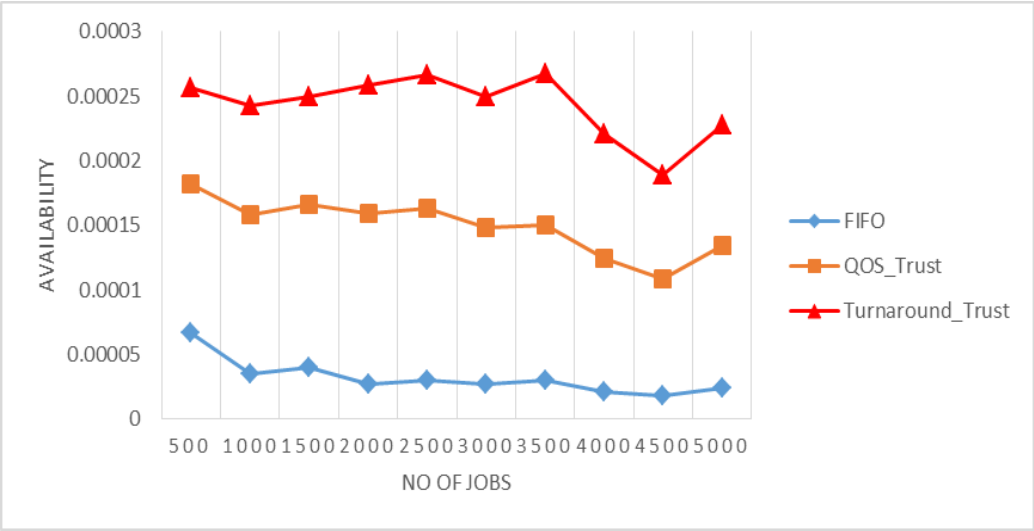

Figure 6. Evaluation of Availability with Varying Number of Jobs

Figure 7 show the comparison of availability is checking on the number of increased works based on each of trust models over availability capability.

Figure 7. Comparison of Availability Metric

5. Conclusion and Further Work

Cloud computing is a very broad term is used for recent development Internet-based computing. General characteristics and reliable security of cloud computing helps development and adoption of this growing technology. Creating Confidence to suppliers of cloud services is a challenging issue, so that many large companies are hesitant to transfer their business to cloud data centers. Currently, many cloud providers that offer cloud services, their service quality and service level agreements are different. One of the challenges being faced by the cloud client is that how to find cloud service that can satisfy them based on the requirements of quality of service with regard to parameters. Now, there is nothing that could help large companies choose a model of trust in accordance with the appropriate security features and data control. In this paper, we presented a trust model to choose the best source. The proposed model, in addition to taking into account criteria of quality of service such as cost, response time, bandwidth, and processor speed, and so on it considers the speed of implementation of works. The proposed model (trust Model *Turnaround_Trust*) has better performance compared to the trust model of the first input, the first output (FIFO) and trust model of quality of service (QoS_Trust) and similar models. The proposed model, in addition to taking into account the measures of

quality of service, selects the most reliable source in the cloud environment by taking into account the speed of things. Using rating mechanism by using the analytic hierarchy process model to select the best cloud source and the development of trust model based on cost efficient algorithm are among the things that can be done in the continuation of this study.

References

[1] B. S. Taheri, M. G. Arani and M. Maeen, "ACCFLA: Access Control in Cloud Federation using Learning Automata", International Journal of Computer Applications, vol. 107, no. 6, December **(2014)**, pp. 30-40.
[2] M. Fallah, M. G. Arani and M. Maeen, "NASLA: Novel Auto Scaling Approach based on Learning Automata for Web Application in Cloud Computing Environment", International Journal of Computer Applications, vol. 113, no. 2, March **(2015)**, pp. 18-23.
[3] Z. Qi, L. Cheng and R. Boutaba, "Cloud computing: state-of-the-art and research challenges", Journal of internet services and applications, vol. 1, no. 1, **(2010)**, pp. 7-18.
[4] A. Ghazi, M. G. Arani, and H. Babaei "A New Framework for the Evaluation of QoS in Cloud Federation", International Journal of Computer Applications, vol. 107, no. 1, December **(2014)**, pp. 44-49.
[5] F. Mohamed, S. Hassan and O. Ghazali, "A Comprehensive Survey on Quality of Service Implementations in Cloud Computing", International Journal of Scientific & Engineering Research, vol. 4, no. 5, **(2013)**, pp. 118-123.
[6] K. Ayesha, R. Masood, U. E. Ghazia, M. A. Shibli and A. G. Abbasi, "Assessment Criteria for Trust Models in Cloud Computing", In Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, IEEE, **(2013)**, pp. 254-261.
[7] G. Qiang, D. Sun, G. Chang, L. Sun and X. Wang, "Modeling and evaluation of trust in cloud computing environments", In Advanced Computer Control (ICACC), 2011 3rd International Conference on. IEEE, **(2011)**, pp. 112-116.
[8] Manuel, Paul D., M. I. A. El Barr and S. T. Selvi, "A Novel Trust Management System for Cloud Computing IaaS Providers", JCMCC-Journal of Combinatorial Mathematic sand Combinatorial Computing, vol. 79, **(2011)**.
[9] K. Shyamlal and D. Tomar, "SLA-Aware Trust Model for Cloud Service Deployment", International Journal of Computer Applications, vol. 90, no. 10, **(2014)**.
[10] P. I. Bhosle and S. A. Kasurkar PADM. DR. V B KOLTE COE Malkapur, "Trust in Cloud Computing", International Journal of Advanced Research in Computer Engineering & Technology, vol. 2, no. 4, April **(2013)**.
[11] A. Shakeel, B. Ahmad, S. M. Saqib and R. M. Khattak, "Trust model: Cloud's provider and cloud's user", International Journal of Advanced Science and Technology, vol. 44, **(2012)**, pp. 69-80.
[12] C. E. Dias, R. T. de Sousa Junior, R. de Oliveira Albuquerque and F. L. L. De Mendonça, "File Exchange in a Private Cloud supported by a Trust Model", In Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2012 International Conference on, IEEE, **(2012)**, pp. 89-96.
[13] G. S. Kumar, S. Versteeg and R. Buyya, "A framework for ranking of cloud computing services", Future Generation Computer Systems, vol. 29, no. 4, **(2013)**, pp. 1012-1023.
[14] G. M. Kumar, P. Gupta, A. Aggarwal and P. Kumar, "QoS based trust management model for Cloud IaaS", In Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on, IEEE, **(2012)**, pp. 843-847.
[15] Saaty T. L., "Theory and applications of the analytic network process: decision making with benefits, opportunities, costs, and risks", RWS publications, **(2005)**.
[16] N. M. Kashif, S. Jabbar and Irfan Zafar, "A novel trust model for selection of Cloud Service Provider", In Computer Applications & Research (WSCAR), 2014 World Symposium on, IEEE, **(2014)**, pp. 1-6.
[17] M. Paul, "A trust model of cloud computing based on Quality of Service", Annals of Operations Research, **(2013)**, pp. 1-12.
[18] L. X. Yong, L. T. Zhou, Y. Shi and Y. Guo, "A trusted computing environment model in cloud architecture", In Machine Learning and Cybernetics (ICMLC), 2010 International Conference on, IEEE, vol. 6, **(2010)**, pp. 2843-2848.
[19] Y. Zhimin, L. Qiao, C. Liu, C. Yang and G. Wan, "A collaborative trust model of firewall-through based on Cloud Computing", In Computer Supported Cooperative Work in Design (CSCWD), 2010 14th International Conference on, IEEE, **(2010)**, pp. 329-334.
[20] Calheiros R. N., R. Ranjan, A. Beloglazov, C. AF De Rose and R. Buyya, "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms", Software: Practice and Experience, vol. 41, no. 1, **(2011)**, pp. 23-50.

[21] G. Punit, M. K. Goyal, P. Kumar and A. Aggarwal, "Trust and reliability based scheduling algorithm for cloud IaaS", In Proceedings of the third international conference on trends in information, telecommunication and computing, Springer New York, **(2013)**, pp. 603-607.

Authors

Atoosa Gholami received the B.S.C degree in Software Engineering from University Mashhad, Iran in 2007, and M.S.C degree from Azad University of mahallat, Iran in 2015, respectively. Her research interests include Cloud Computing.

Mostafa Ghobaei Arani received the B.S.C degree in Software Engineering from IAU Kashan, Iran in 2009, and M.S.C degree from Azad University of Tehran, Iran in 2011, respectively. He's Currently a PhD Candidate in Islamic Azad University, Science and Research Branch, Tehran, Iran. His research interests include Grid Computing, Cloud Computing, Pervasive Computing, Distributed Systems and Software Development.

