International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7 Issue-5, January 2019

An Uncertain Trust and Prediction Model in Federated Cloud using Machine Learning Approach

A. Mary OdilyaTeena, M. Aaramuthan

Abstract**:** ***Federated Cloud Model referred as the interconnection of two or more providers with some guidelines prescribed in Service Level Agreement to address the uncertainty such as SLA Violation for the specific service. Most well-known models use the concept of either probability or fuzzy set theory in managing the Quality of Service (QoS) required by the Cloud user, application and tool. In this paper, Deep Learning is applied to predict the SLA Violation and manage the uncertainty. SLA violation is defined as the failure to meet the requirement prescribed for the user and application. In addition to that, banker's algorithm is modified and used as prediction algorithm to find the possible safe state computation of the tasks and avoid wastage of resources in federated cloud. Random forest data mining technique is applied to rank the trust based provider and top provider may be considered for the service. The simulation results reveal that the proposed model helps to avoid uncertainty to about 78% and recognized that it is one of the most appropriate model needed in federated cloud architecture.***

Index Terms**:** ***About four key words or phrases in alphabetical order, separated by commas.***

I. INTRODUCTION

To satisfy the requirement of business needs, Federated Cloud Model is the deployment and management of multiple cloud providers Resource allocation is the most challenging area in federated cloud. The prediction of resource required for upcoming computational tasks are necessary to bring QoS under any constraints. Resources Provision Strategies falls on either Predictive or Relative[1]. Predictive strategy leads to better resource performance and reaction time whereas relative strategy measures the system state. In this paper, Banker's algorithm also known as the detection algorithm is used to predict the resources required for computation and also find the possible order of execution of tasks. This algorithm predicts the safe and non-safe state of computation of tasks which helps to avoid wastage of resources in federated cloud. Service Level Agreement (SLA) is an contract between the user and provider to define the stage of the service and its related cost[2,4,6]. SLA Violation is the failure of providing the agreed service to the cloud user. In this paper, Deep Learning is helps to predict Violations, Reallocate the resources before the occurrence of Violations. To examine the performance of the providers Service Measurement Index (SMI) attributes are applied[3].

This paper is arranged as follows. Existing work discusses in Section 2 which is related to SLA Violation and Prediction, Section 3 discusses Proposed Model and banker's algorithm, Section 4 illustrates deep learning, Section 5 shows simulation results of the proposed work. Finally, Future work and conclusion discusses in Section 6.

Revised Manuscript Received on 30 January 2019.
***** Correspondence Author

A. Mary OdilyaTeena* , Assistant Professor, Department of Computer Science, St. Joseph's College of Arts &Science (Autonomous), Cuddalore& Ph.D. (Category-B), Research Scholar, Bharathiyar University, Coimbatore.

Dr. M. Aaramuthan , Associate Professor &Head of the Department of Information Technology, PerunthalaivarKamarajar Institute of Engineering and Technology, Nedungadu, Karaikal.

II. EXISTING WORK

A lot research has been conducted to deal with the SLA issues in Federated cloud. The researches in[5] proposed as SLA based trust model and a conceptual SLA framework to evaluate cloud services. Chakraborty and Roy[7] defined an SLA based quantitative trust model to estimate the trustworthiness of a cloud service. The researchers in[8] proposed a quality of service mechanism on cloud computing based on SLA model. In this research, they defined a new language to illustrate QoS oriented SLA associated with cloud services. L.Wu., S.K.Garg and RajkumarBuya[9] joined together proposed a new resource allocation technique for SaaS providers, helps to reduce infrastructure cost and SLA Violations. Y. Xiaoyong and other researchers[10] presented a cloud SLA availability commitment framework together with availability calculation and fine calculation methods. Secure management and trustworthy[11,12,13,14] in the federated cloud is the most challenging problems in the federated clouds. So, cloud user should prefer a big level of trust to a CSP of federated cloud applications. Every time CSP deploys its application and services on federated cloud to establish trustworthiness of their services deployed is very difficult compare to a single cloud. Our earlier research work shows that deep learning be able to help create context aware trust evaluation and aggregation in a coherent, intuitive and strong way[15]. We propose an uncertainty of trust based on Cloud Model and deep learning to evaluate the trustworthy and untrustworthy in a federated cloud more accurately and efficiently in this paper. Deep Learning methods gives high performance and provides accurate results in big data applications.

III. TRUST BASED SERVICE SELECTION ARCHITECTURE FOR FEDERATED CLOUD

In the Figure 1 depicts the proposed architecture for selection of the trust provider. In this proposal, Quality of Service (QoS) and trustworthiness of services are calculated such level of provider is assigned to the user.

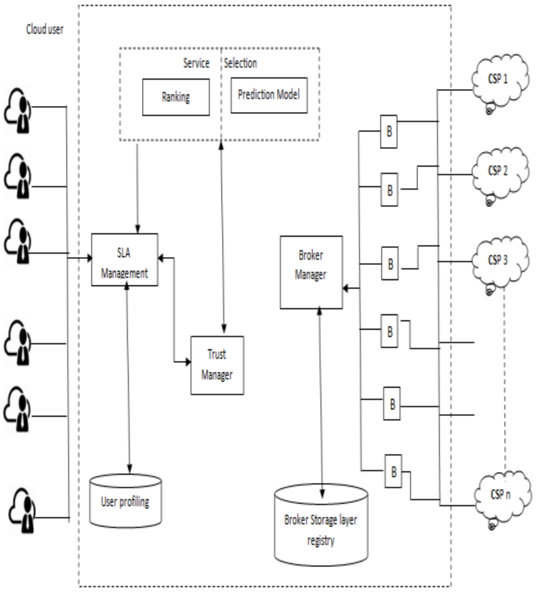

Figure 1 Proposed Architecture

In this paper, trust is defined as an expectation that user accomplish the specific service with the guidelines of SLA. The failure of unaccomplished service with the guidelines of SLA is called SLA Violation. SLA violations are managed and predicted using banker's algorithm that helps to know the safe state and unsafe state of the providers. Trust manager formulates trust relationship of the provider based on SMI attributes and suggests recommendation to the Prediction and Service Selection. The proposed architecture selects the best provider based on the QoS values of cloud services and QoS requirements of the cloud user.

Trust Manager (TM) is responsible for computing the trust based on QoS monitoring and prescribed guidelines in SLA for specific user. QoS represents a set of non-functional characteristics of services such as Scalability, Reliability, Performance, Response time, Usability Throughput, Security, etc.The resources in the federated cloud are estimated in prediction model, apply banker's algorithm and find the deployment is either safe or unsafe state. Ranking model helps to identify the top priority of the provider at that time suitable for the deployment of service.

Cloud Service Provider is interconnected with broker and the broker collects and updates the resource information in the broker registry. Broker Manager is in charge for selecting and assigning the trustworthiness providers. The following are the interaction performed for selecting the trustworthiness provider for the specific user service.

1) loud Service Provider exchanged their service information including SLA to the broker and updated in the BM registry.
2) Prediction component computes the actual QoS performance of service required and reports to the Broker Manager.
3) Broker Manager Registry matches the QoS requirements on services with all registered cloud providers which SLA meet with the user requirements.
4) Trust Manager evaluates the trustworthiness of the provider and updates the Broker Registry.
5) Cloud Provider is assigned to the specific service, performance level is updated in the broker registry and it will be considered to compute trust level of the providers.

3.1 Prediction Model

A resource allocation and deadlock avoidance algorithms also known as Banker's algorithm, predicts the security of the cloud service providers by simulating the allocation for Predetermined maximum feasible amount of all resources and decide the allocation should be either continue or not.

Algorithm

Consider the number of cloud service providers 'p' and number of resources types available in federated cloud 'q'.

The number of available resources denoted as avail [j] = a, there are 'a' instances of resource type T_j. The maximum request of each resources denoted as maximum [i,j] = a, user Ui may request at most 'a' instances of resource type T_j.

The number of resources currently allocated to the user Ui denoted as alloc [i,j] = a, then user Ui currently allocated 'a' instances of resource type Tj.

The remaining resource want for the process is denoted as wanted [i,j] = a, user U_i is currently wanted 'a' instances of resource type T_j.

wanted [i,j] = maximum [i,j] – alloc [i,j]

Allocation specifies the resources currently allocated to user U_i, Wanted specifies the additional resources that user U_i may still request to complete its task. In this algorithm for finding out if the user service is executable or not can be described as follows.

Step 1: Consider progress and complete be vectors of length 'p' and 'q' respectively.

Step 2: Assign Progress = avail, Finish [u] = False, where u=1,2,…q.

Step 3: Compute u such that Finish [u] = False, wanted [u] <= Progress if no such u exists go to Step(5)

Step 4: Compute Progress = Progress + alloc
Finish [u] =True go to Step(3)

Step 5: If Finish[u] = True, for all u then the enough resources are available for execution.

3.2 Trust Manager

TM is an intermediary between Cloud Providers (CSP) and Cloud Users (CU), an idea inherited from the Trust Brokers. Trust Manager are spread above the clouds and represented by various Cloud Providers in federated clouds to provide trust based services[16]. TMs are called when Cloud User request cloud services and also Cloud Provider response to the cloud user with the guidelines of SLA and QoS functioning. TMs are independently maintained and operated like search engines, portals, etc. Cloud C Users can use the services (such as SaaS, IaaS or PaaS) either free or able to be used through a paid membership[17]. Trust Manager collects information about CSP and this evidence information is sent to SLA. SLA monitoring the Cloud based services and Cloud Users sent the feedback to TM through SLA.

With the help of this information we can evaluate the trustworthiness of CSP.

3.3 Deep Learning

This module will explain how to combine the trust cloud with deep learning to predict SLA Violations and manage uncertainty. Here, trust value is the root node and resource type corresponds to leaves. A new resource type is added in the leaf node and existing conditional possibility tables (CPTs) are still accepted. To remove a resource type doesn't have any cause to left nodes either.

Deep Learning Algorithm for Trust Based Service Selection

Input: The group of Cloud Blobs *Y*, contains set of resources R (Response time, throughput, reliability, scalability, usability, SLA Violations)

Output: Trust cloud's three parameters *Ex*, *En*, *He* and each ranking's truth degree $\mu T(r)$

```
Steps:
Step1: Declare all the CPTs to be uniform distribution
Step2: Assign initial= 1
    repeat
        Fetch a rank $r_i$ , associated resource type C from Y
        Do time decay process as in (4) if needed
        Update the CPTs with the new rank $r_i$
        Increment initial= initial+1
    untilfetch in all ranks
Step3: Assume the possibility that an cloud user's service quality is on level k in each various resource C
        (i.e., P(Trust = level $_k$ |C), k∈{1, 2,…, n})
Step4: Compute Ex in each various resource C as the expectation of node "Trust" in resource C holding
    $Ex = \sum_{k=1}^{n} P(Trust = level_k |C) *k$
Step5: For various resource C compute Enas in (1)
Step6: For various resource C compute He as in (2)
Step7: do
        j=1
        compute$\mu T(rj)$ in the linked resource C as in (3)
    while(j < i-1)
```

To select best cloud provider for the cloud services uncertainty (calculated by En+He) of trust must be taken for consideration and it is compared with trust value (i.e Ex). So we conclude that, if trust value is high and uncertainty is low then the trustworthy is fair. If trust value is low uncertainty is high then the trustworthy is not fair.

IV. RESULTS & DISCUSSION

In this section, we exhibit the experimental evaluation and validation of trust. The proposed mechanism is implemented in CloudSim using Java. The number of submitted requests is 100. The average response time of the proposed work is shown in Table – 1.

The proposed work provides better performance in average response time because it combines Prediction, trustworthiness and ranking components in the architecture. Prediction model ensures that the sufficient resources are available as per the need of the serving the requests. Table – 2explains the average throughput of the proposed model.

Table 1 Average Response Time of the Proposed Work

Number of Cloud Providers	Grade based ranking(ms)	Bayesian network (ms)	Regression (ms)	Proposed Model(ms)
2	78	93	102	64
4	58	68	78	52
6	53	58	63	46
8	48	53	58	41
10	28	38	48	23
12	18	29	38	12

Table 2 Average Throughput of the Proposed Work

Number of Cloud Providers	Grade based ranking(ms)	Bayesian network (ms)	Regression (ms)	Proposed Model(ms)
2	20	15	13	24
4	30	25	18	36
6	40	32	27	48
8	60	50	40	70
10	65	56	52	76
12	70	63	57	88

Table 3 SLA Violations of the Proposed Work

Number of Cloud Providers	Grade based ranking(ms)	Bayesian network (ms)	Regression (ms)	Proposed Model(ms)
2	12	16	18	3
4	8	11	15	2
6	4	6	8	2
8	3	5	6	2
10	2	4	5	1
12	2	3	4	1

The average response time of the proposed model compared with other mechanism depicted in Figure2, and the average throughput of the proposed model shown in Figure 3.

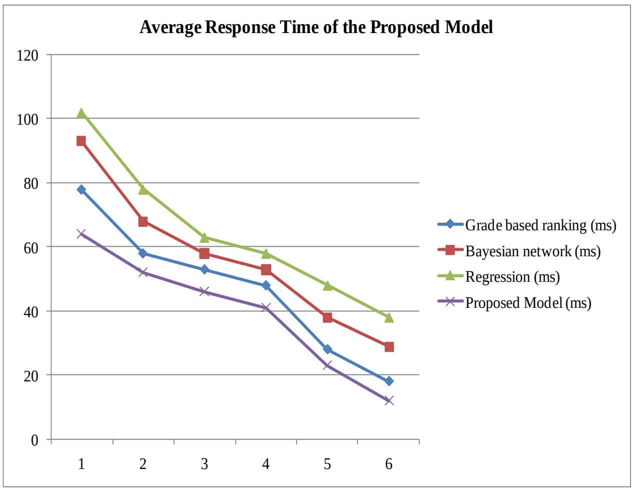

Figure 2 Average Response Time

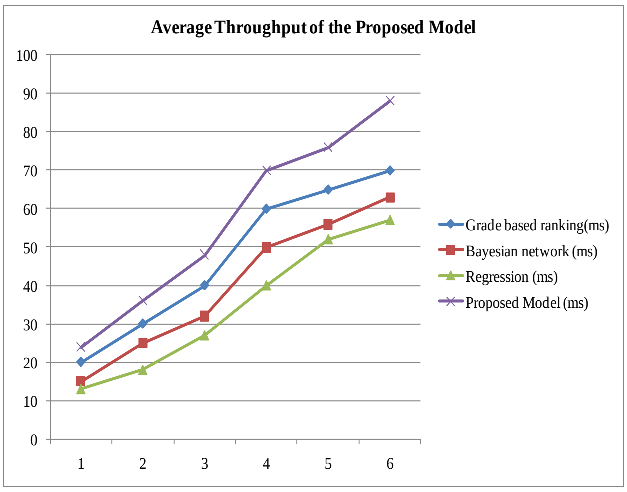

Figure 3 Average Throughput

The number of SLA violations observed in the considered scenario is shown in Table – 3and depicted in Figure 4.

The proposed model almost eliminates SLA violations are observed from the simulation results due to the inclusion of Trust and Prediction model in the architecture.

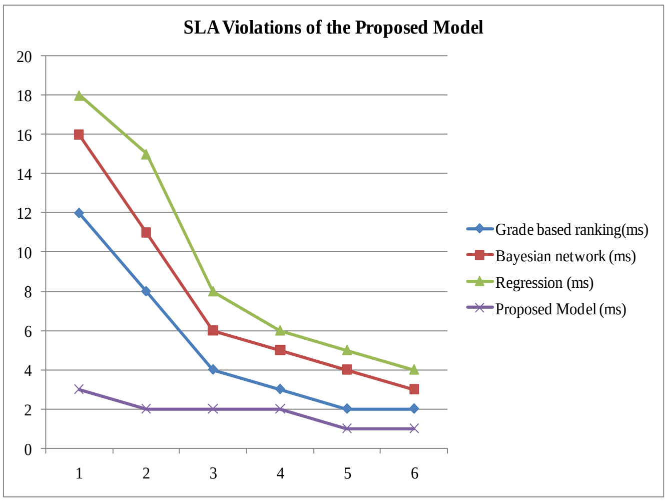

Figure 4 SLA Violations

V. CONCLUSION

In this paper, trust based service selection model is proposed which comprises of evaluating trust based on SMI attributes, predicting the required resources using banker's algorithm and ranking based on Random Forest data mining technique. This combination yields better performance and minimum SLA violations compared to the existingmethods.In the future, social trust relation among users to infer the trust worthiness of the provider is to be addressed.

REFERENCES

1. Rodrigo N. Calheiros, Rajiv Ranjan , Anton Beloglazov , César A. F. De Rose and RajkumarBuyya, "CloudSim: a toolkit for modelling and simulation of cloud computing environments and evaluation of resource provisioning algorithms", 24 August 2010, https://doi.org/10.1002/spe.995.
2. RajkumarBuyya ;Saurabh Kumar Garg ; Rodrigo N. Calheiros, "SLA-oriented resource provisioning for cloud computing: Challenges, architecture, and solutions" in: 2011 IEEE International Conference on Cloud and Service Computing, 12-14 Dec. 2011
3. 3.Saurabh Kumar Garg, Steve Versteeg and RajkumarBuyya," SMICloud: A Framework for Comparing and Ranking Cloud Services" in 2011 Fourth IEEE International Conference on Utility and Cloud Computing, 5-8 Dec 2011.
4. J. Udayakumar, M. Manikkam, and A. Arun, "Cloud-SLA: Service Level Agreement for Cloud Computing."
5. Mohammed, T. Dillon, E. Chang, SLA-based trust model for cloud computing, in: Proceedings of 2010 13th International Conference on Network-Based Information Systems (NBiS), 2010, pp. 321–324.
6. Maheswari, R. Sanjana, S. Sowmiya, SudhirShenai& G. Prabhakaran, "An Efficient Cloud Security System Using Double Secret Key Decryption Process for Secure Cloud Environments", International Journal of Advanced Scientific Research & Development (IJASRD), 3 (1/II), pp. 134 – 139.
7. Sudip Chakraborty, Krishnendu Roy, An SLA-based framework for estimating trustworthiness of a cloud, in: Proceedings of 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2012, pp. 937–942.
8. D. Serrano, S. Bouchenak, Y. Kouki, T. Ledoux, J. Lejeune, J. Sopena, L. Arantes, and P. Sens, "Towards QoS-oriented SLA guarantees for online cloud services," in Cluster, Cloud and Grid Computing (CCGrid), 2013 13th IEEE/ACM International Symposium on, 2013, pp. 50-57.
9. L. Wu, S. K. Garg, and R. Buyya, "SLA-based resource allocation for software as a service provider (SaaS) in cloud computing environments," in Cluster, Cloud and Grid Computing (CCGrid), 2011 11th IEEE/ACM International Symposium on, 2011, pp. 195-204.
10. Y. Xiaoyong, L. Ying, J. Tong, L. Tiancheng, and W. Zhonghai, "An Analysis on Availability Commitment and Penalty in Cloud SLA," in Computer Software and Applications Conference (COMPSAC), 2015 IEEE 39th Annual, 2015, pp. 914-919.
11. J. Abawajy, Determining service trustworthiness in inter-cloud computing environments, in: Proceedings of 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN), 2009, pp. 784–788.
12. J. Abawajy, Establishing trust in hybrid cloud computing environments, in: Proceedings of 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2011, pp. 118–125.
13. D. Bernstein, D. Vij, Inter-cloud security considerations, in: Proceedings of 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), 2010, pp.
14. MukeshSinghal, Chandrasekhar Santosh, GeTingjian, Sandhu Ravi, Krishnan Ram, Ahn Gail-Joon, Bertino Elisa, Collaboration in multi cloud computing environments: framework and security issues, Computer 46 (2) (2013).

15. F. Lu, H.Z. Wu, “Research of Trust Valuation and Decision-making Based on Cloud Model in Grid Environment,” Journal of System Simulation, Vol. 21, Jan. 2009, pp. 421 – 426.
16. J.Y.J. Hsu, K.J. Lin, T.H. Chang, C.J. Ho, H.S. Huang, W.R. Jih, Parameter learning of personalized trust models in broker-based distributed trust management, Inform. Syst. Front. 8 (4) (2010) 321–333.
17. K.J. Lin, H. Lu, T. Yu, C.E. Tai, A reputation and trust management broker framework for web applications, in: Proceedings of the IEEE International Conference on e-Technology, e-Commerce, and e-Service, 2005, pp. 262–269.

AUTHORS PROFILE

Mrs. Mary OdilyaTeena is working as an Assistant Professor in Department of Computer Applications,St. Joseph’s College(Autonomous), Cuddalore, currently she pursuing her Ph.D., (Part Time) in Bharathiyar University, Coimbatore under the guidance of Dr. M. Aramudhan. She has more than 10 years of experience in teaching in industry. She has published three research articles in the field of cloud computing and her research is focused on a security in Cloud Computing. She has participated more than 15 seminars and workshops.

Dr. M. Aramudhan, Ph.D., is a Head & Associate Professor in Information Technology at PerunthalaivarKamarajar Institute of Engineering and Technology (PKIET), Karaikal. He received his Ph.D., from Anna University, Chennai. He is an academician, a Research Supervisor in Computer Science, with more than 20 years of accomplished experience in teaching. He has published over 49 articles in national and international referred journals and one text book for the college students. He has received Young Teacher Award from AICTE and also received best paper award 3 times.