Fault Tolerant and Risk Access Control Enabled Federated Cloud

M. Satheesh[1], M. Aramudhan[2]

[1]Department of Computer Science, Don Bosco College Arts and Science, Karaikal, Puducherry, Tamil Nadu, India

[2]Department of Information Technology, Perunthalaivar Kamarajar Institute of Engineering and Technology(PKIET), Karaikal, Puducherry, Tamil Nadu, India

ABSTRACT

Cloud Federation is a new novel collaboration paradigm where organizations share data across their private cloud infrastructures. However the adoption of cloud federation is hindered by federated organization's concerns on potential risks of data leakage and misuse. It is hard for the users to select and assign the most suitable and reliable provider to the user task in FCA. In the proposed approach, FCA shortlisted the related CSPs for the user tasks automatically and choose the optimal provider using the concept of ranking mechanism. Service Level Agreement (SLA) is an agreement that illustrates the level of performance assured by the provider to the user. The Cloud Service Measurement Index Consortium (CSMIC), identified Service Measurement Index (SMI) metrics that helps to evaluate and compare the services of different CSPs. Effective selection models offer optimal cloud service to users are high demand for the increasing number of cloud services on the cloud platform. Risk based access control framework for Federated cloud is proposed that manages user access to Federated cloud resources by quantifying and aggregating risk metrics defined in risk policies created by resource owners. This Trust based cloud selection model is proposed to discover the providers for the service and evaluate the service using the concept of Fuzzy Random Theory. Thus this Risk based access control mechanism is more flexibile to handle exceptional situations in which the access of cloud resources is maintained in the face of violation of SLA but applying the mechanism of fault tolerance to meet the requirements of the cloud user.

Keywords: Federated Cloud, Service Level Agreement (SLA), Risk Access Control, Fault Tolerant, Risk Management

I. INTRODUCTION

Federated Cloud Architecture (FCA) is defined as the interconnection of two or more Cloud Service Providers (CSP) which is accessed by particular brokers and all brokers' information are collected and updated periodically in the registry broker manager. Initially, providers are discovered for the service using broker learning algorithm, ranking all the discovered providers, and select and assign the optimal provider for the service. In the resent scenario, a single provider may not be sufficient to satisfy the requirement of the user and application. In such case, FCA is the best alternative to encounter the needs of the users. Recently, more researchers showing interest in this area and suggest lot of effective solutions to accomplish Quality of Service (QoS) based provider selection from the pool of CSPs. Cloud Service Measurement Index Consortium (CSMIC) identified Service Measurement Index (SMI) metrics that helps to evaluate and compare the services of different Cloud Service Providers [1].

CSEIT183686 | Received : 20 July 2018 | Accepted : 05 August 2018 | July-August-2018 [3 (6) : 439-448]

Effective selection models offer optimal cloud service to users are high demand for the increasing number of cloud services on the cloud platform. In this chapter, Trust based cloud selection model is proposed to discover the providers for the service and evaluate the service using the concept of Fuzzy Random Theory. The existing methods depend on the QoS ranking to select the CSP and ignore the trust relationships among users, brokers and CSP. The proposed cloud provider service selection model integrates the QoS and trust relationship.

It is hard for the users to select and assign the most suitable and reliable provider to the user task in FCA. In the proposed approach, FCA shortlisted the related CSPs for the user tasks automatically and choose the optimal provider using the concept of ranking mechanism. Service Level Agreement (SLA) is an agreement that illustrates the level of performance assured by the provider to the user at the user side [2]. In current scenario, SLA technique plays a major role that brings the confident to the user, prompts business policies and ensuring Quality of Service (QoS) at user side. SLA management provides with three phases such as SLA establishment, SLA negotiation, SLA monitoring and violation. Cloud provider commits to the user in terms of QoS is called as SLA establishment whereas the user discuss with the provider for the required level of services called as SLA negotiation. Services consumed by the user are monitored by the provider and detecting if there is any abnormality is remarked as violation. SLA is implemented between cloud member and cloud service provider for efficient processing of federated cloud [3]. SLA management is maintained in the proposed architecture by discovering and ranking the service on fuzzy random theory. A fault tolerance mechanism at the level of service such as performance and availability is managed and provided the necessary SLA using the concept of Virtual Clustered Local service Provider (VCLP).

In this paper work the Risk based Access control Framework for Federated cloud is proposed that manages user access to Federated cloud resources by quantifying and aggregating risk metrics defined in risk policies created by resource owners. The existing access controls mechanism are too rigid to handle exceptional situations in which the policy itself should be overridden in order not to stop the system,do not meet the requirements of dynamic secure information and permission sharing in collaborative environment and not exible enough to handle the changing behavior of users.The drawbacks mentioned above are addressed in the proposed framework.

The broker based fault tolerance and risk access control enabled Federated architecture is discussed in section 2. The layer architecture of the proposed federated cloud is discussed in section 3. In the section 4. the Broker Learning Algorithm is been defined and in section 5, the Fault tolerance Mechanism has been introduced for the assessment of Risk. In the following of two sections 6 and 7 the contribution is made by introducing a Risk Access control Mechanism based on the Fuzzy Random theory which does the Ranking from the available CSP and the best suitable providers are selected. In the section 8 the Simulation is done and the findings are tabulated and discussed.

II. FAULT TOLERANCE AND RISK ACCESS CONTROL IN CLOUD ARCHITECTURE

The Fault tolerance and Risk access control enabled Federated cloud architecture is.

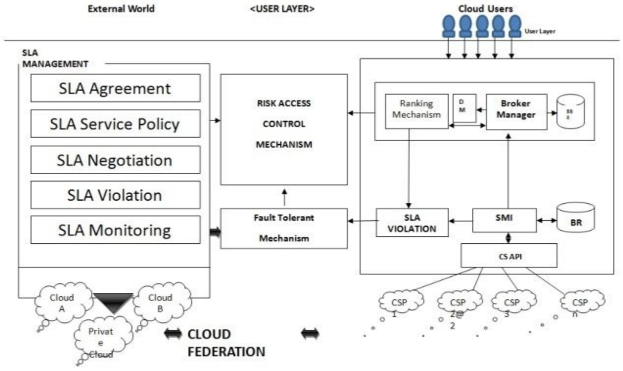


Figure 1

shown in the Figure 1 The functionality of the architecture is to maintain the life cycle of the SLA management, level permission assigned to the user as per the permission of the resource owner, shortlisted the service provider for the specific user request based on the value of the trust, ranking the selected service providers based on their trust and automatically assigning the optimal provider to the user. The trust of the provider is computed based on the Service Measurement Index (SMI) metrics suggested by the Cloud Consortium Service Measurement Index (CCSMI). In the proposed architecture, each Cloud Service Provider (CSP) interconnects with specific broker; brokers are interconnected with Broker Manager (BM). The role and responsibilities of the broker is to collect the status and availability of the resource, type of service to be supported and executed and cost. Brokers update this information in the registry of the BM periodically if there are any changes in the value of the providers. The validity of the information updated in the BM is verified using timestamp [4].

The phases in the life cycle of SLA management are design and development, service offering, service negotiation, service provisioning, service operations and service decommissioning. The life cycle of SLA brings service expectations, drive engineering decisions at design level and operational decisions at the level of usage and delivery. Users establish the agreements with one or more providers based on the requirement and importance of the service through the process of SLA negotiation. If there is any violations in the SLA life cycle, by considering the significance of SLA, fault tolerance enabled SLA service is suggested in the proposed architecture. The details of the working of fault tolerance enabled SLA is discussed in the section 3.

The trust level of the broker falls in to different categories accordance with the security of the broker. The levels of the categories are completely trusted, partially trusted, minimally trusted and not trusted. The trust of the broker is computed using the following attributes such as accreditation, competency, goodwill and integrity. Accreditation refers the Quality of Service (QoS) extended in the past performance of the broker. Accreditation assigns different grades A, B, C and D depends on the service extended by the broker to the user submitted tasks. Grade 'A' means *highly qualified Service,* Grade'B' means *medium qualified service*, Grade 'C' means *minimum qualified service* and Grade 'D' means *undefined*. Initially, broker is assigned with the Grade 'D'. Later based on its performance, it may be reassigned with any higher grade for the broker. Competency is measured by using Service Measurement Index (SMI) suggested by the Cloud Consortium. In this grade classification, Fuzzy Logic approach is used to evaluate the competency of the broker. Goodwill is computed based on the past performance of the broker [5]. Integrity is achieved based on the authentication protocol between broker and broker manager. Reputation is the computed threshold value of services by considering the available resources of the provider. Each broker provides with certain policies and standards applied in the operations of the broker that may be examined by the cloud. Self-assessment denotes the study the information about the service which is revealed by the provider.

III. LAYER ARCHITECTURE OF FAULT TOLERANCE AND RISK ENABLED FEDERATED CLOUD

To reduce the design complexity of the Fault tolerance and Risk enabled Federated Cloud, layer architecture is proposed. It consists of five layers such as Service provider Management layer, Broker Management layer, Fault Tolerant Layer, Risk access control Layer and Application layer. Broker Management layer, SLA management and Fault tolerant layer falls under the service abstraction level of the architecture where as risk access control layer deals with the security of the architecture. Broker Management layer describes the functionalities of brokers and BM. Fault tolerance layer illustrates if there is any exception occurs in the life cycle of SLA, by using the concept of Virtual Clustered Local Service Provider (VCLP) formation, brokering is possible with one or more service providers based on the agreement established by the user. Application layer performs required computing depends on availability of the resources [6]. The layer architecture of Fault Tolerance and Risk access control (FTRAC) enabled Federated cloud is shown in Figure 3.2.

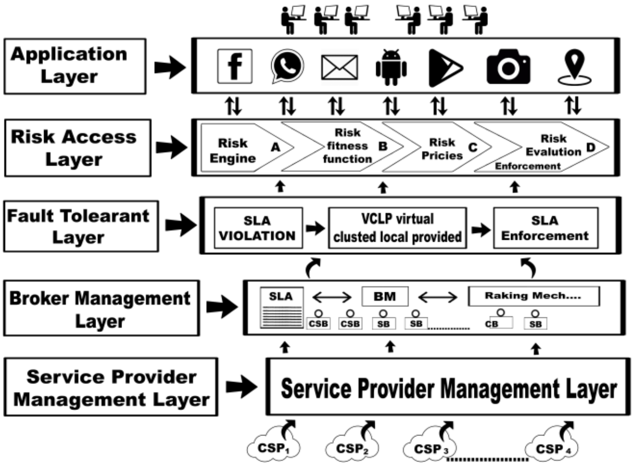


Figure 2. layer Architecture of FTRAC

IV. BROKER LEARNING ALGORITHM

Federated cloud provider selection algorithm uses the quality metrics according to the Service Measurement Index (SMI) , short list the matched providers depends on the SLA and functional requirements. Let CP= {CP1, CP_2….CP_n} are the list of cloud providers in the Federated Cloud (FC). Let CB= {CB_1, CB_2….CB_n} are the cloud brokers that connected CP to the Cloud Manager (CM) in the proposed federated cloud architecture. Cloud broker considered the list of QoS indicators Q_i = {Q1, Q2, Q3….Q_N} for the service requests submitted by the user, broker initiated the processing and short listed the providers based on the value for the quality indicators assured. Then apply ranking on the short listed providers using Fuzzy based logic sets approach. In order to normalize the value of QoS indicators, the following are considered such as QoS metrics are measured uniform, qualities of the providers are analyzed using uniform index and assign threshold for the quality indicators based on the priority of it. The matching of provider is identified by the representation of the given set

$$MP = \{QI, FA, RCP, CCP\}$$

MP denotes the Matching provider for the service. QI is the list of Quality Indicator recognized by the SMI [7] . FA discuss the functional requirements.RCP refers the resource demand by the service and released by the provider. Cloud providers are clustered based on the service referred as CCP. The functionality of provider discovery is shown in Figure 3.3 This architecture shows the user discovers the of service provider in Federated cloud architecture through the Broker Manager

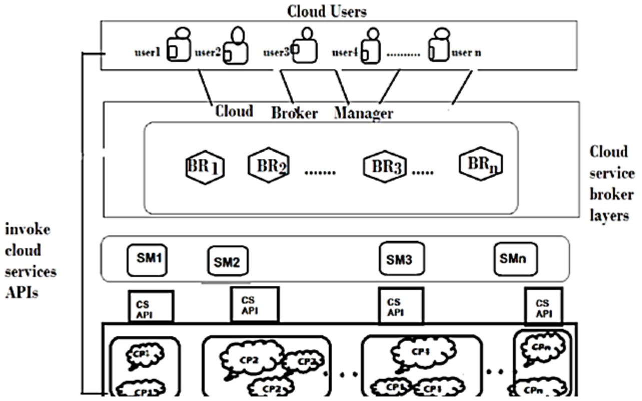


Figure: 3. Cloud Service Resource Provider

V. FAULT TOLERANCE MECHANISM

Fault Tolerance is defined as even if there is any violation in the service of life cycle of SLA management, a strategy is applied to accomplish the task as per the SLA. Two metrics such as service availability and service performance is considered and there is any violation a concept of Virtual Clustered Local service Provider (VCLP) is introduced and maintained the SLA. A clustered is development based on the establish agreements of the users with two or more providers and virtually act as a single provider. The natural inspired algorithm clustered based bee algorithm is used to form the virtual clusters and utilize whenever the SLA violations happened. Bee algorithm is combination with the concept of clustering technique is designed to solve the resource availability and performance in the federated cloud architecture[8].

The bee algorithm with clustered technique has been designed and it is given in detail as below.

1. First, each provider is virtually clustered based on the establish agreements in SLA.

2. Second, the similarity of the provider is computed based on the SMI attributes such as response time, interoperability, assurance, security and privacy and usability.

3. Service task is categorized as minimum required, maximum required

4. Initialize honeybee parameters are mapped with federated cloud

n= number of employed bees as providers

m = Number of onlooker bees (m>n) as tasks

s= number of scout bees as capacity of resources.

Iteration: Maximum iteration number α : initial value of penalty parameter

5. Construct initial provider for initial solution All tasks find suitable provider for its execution

6 . Compute the similarity of the providers by finding the fitness function of the provider

Set of tasks T = $\{T_1, T_2, T_n\}$.

Deadline of tasks D = {D1,D2,…Dn }

Let SP = $\{p_1,p_2, . . . p_m\}$

Total task completion - TCT.

Completion time of task T_i on SP_j as CT_{ij}

TCT= max $\{CT_{ij} | i \in T, i = 1, 2 . . . n$ and $j \in VM, j = 1, 2, . . . m\}$

Min $\sum_{i=1}^{n} CT_{ij}$ j= 1….m Capacity of provider's p_j

$p_j = PE_{numj} \times PE_{mipsj} + VM_{bwj}$

PE_{numj} is the number processor in $provider_j$

PE_{mipsj} is million instructions executed per second in $provider_j$

U_{bwj} is the usability of the $provider_j$

Total length of tasks that are assigned $c = \sum_{i=1}^{m} p_j$

Total length of tasks that are assigned to a provider is called usability of the provider. Usability of the provider can be calculated as the number of tasks at time t on the provider $U = \frac{N(T,t)}{S(p_j,t)}$

Processing time of a provider $PT_i = \frac{U}{p_i}$

Fitness function = $\frac{CT_{ij}}{CT_i} + \frac{1}{PT_i}$

Assign tasks to provider according to probabilities[9] .

```
For(all tasks,construct solution using tasks)
All tasks find suitable provider for each task. If fit(task)>fit(provider )

Find best provider, replace with respective task. If fit (task)<fit(provider)
Find best feasible task, replace with Best solution,
End For

Initialize scout bees

Do while{
Construct solution using tasks
If fit (resources)> fit (provider)
The resource replace provider
n=n+1
}Until (n=provider)
```

After each iteration the best fit resources and its providers are identified for the feasible task.

END

VI. RISK ACCESS CONTROL MECHANISM

This proposed work provides resource owners and Federated Service Provider (FSP) a greater control over the flexibility of authorization. This mechanism consists of Risk Engine, Risk fitness Functions, Risk Policies, and Risk evaluation unit. Risk Engine is responsible for analyzing and processing the risk policies associated to a resource and for invoking fitness functions illustrates in each policy. In existing work, Risk Engine is different for each FSP because it implements the fitness function in that provider. In the proposed work, Risk Access Control Mechanism is available in the middleware layer; act as a separate component and similar for all SP in federated architecture. Risk policy is a XML file explains how risk based access control is assigned for each resource. Risk fitness function is the computed function that implements the risk metrics that are available to be used in the risk policies. The risk evaluation unit considered the policies of the resource assigned for the user and takes decision such as permit, deny, not applicable and indeterminate[10]. The following figure shows the Risk access control Mechanism architecture.

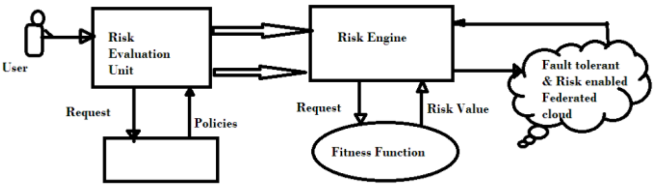


Figure 4. Risk access control Mechanism architecture.

VII. FUZZY RANDOM THEORY BASED RANKING OF PROVIDERS

The principle of fuzzy sets and fuzzy functions found useful in applications such as pattern recognition, clustering, information retrieval, and systems analysis. The notion of fuzzy random variables was introduced as a natural generalization of random set in order to represent associations between the outcomes of random experiment and non-statistical in exact data. Kwakernakk [13] introduce the concept of a fuzzy random variable as a function F:Ω→F(R) where (Ω, A, P) is a probability space and F(R) denotes all piecewise continuous functions U:R→[0, 1]. A notion of a fuzzy random variable [14] slightly different than that of Kwakernakk that it as a measurable fuzzy set valued function $x:\Omega \rightarrow F_0(R)$, where R is the real line, (Ω, A, P) is a probability space, 0(R) = {A:R→[0, 1]} and {xϵR; A(x) ≥ α} is a bounded closed interval for each α ϵ (0, 1).

Let U be a nonempty usual set, P(U) denote the set of all subsets in U and F(U) denote the set of all fuzzy subsets in U. For $A \epsilon F(U)$ we define two subsets of U as follows:

$A_\alpha = \{x \epsilon U; A(x) \geq \alpha\}$ for any $\alpha \epsilon [0, 1]$ -----(3.1)

$A\alpha = \{x \epsilon U; A(x) > \alpha\}$ for any $\alpha \epsilon [0, 1]$, ----(3.2)

Where A(x) is the membership functions of A. These are known as α-cuts of the fuzzy set A. Without loss of generality in the sequal X_α, F_α, G_α, F_α, G_α, denote the respective α-cut functions.

$A_\alpha = [A^-{}_\alpha, A^+{}_\alpha]$

Where A_α, = inf A_α, $A^+{}_\alpha$ = sup A_α

The suggested ranking model consists of three phases namely (i) Discover service providers (ii) Rank the selected service provider (iii) Choosing the best service provider. This ranking model has been working on the concept of fuzzy random variable [9].

Phase 1: Discover service providers

Cloud Broker manager selects the service providers, based on the service requirements and current status of service providers (Li, Yang, Kandula, & Zhang, 2010). CBM use the concept of fuzzy random model process, to select the service provider. A fuzzy random process satisfying the fuzzy Markov property can make predictions of the future process based on the present conditions. Consider user requirement parameters like availability, security, cost etc as Y. Broker Manager as X, service providers as P (p1, p2 ... pn) and selected service provider as SP, then the stochastic Markov property is defined as $F \{SP \leq X(P) / SP(Y) = P(Y)\}$

Selected service providers based on Markov process, are entered in the form of matrix called compatibility decision matrix. Compatibility decision matrix consists of n rows and 3 columns. Each row in a matrix gives the current status and availability of service providers. Three columns in a decision matrix represent the name of a service provider, status of service provider (eligible, ineligible) and availability of service provider. Availability of service provider is obtained from cloud table in CPM.

Phase 2: Rank the selected service providers using Fuzzy sets

CPM selects the top service provider among the number of available and eligible service provider in the compatibility decision matrix using Fuzzy set method. Classical set theory requires that each element of a set included entirely within the set. Fuzzy set theory, a generalization of classical set theory, allows set elements to have partial membership and therefore allows representation of imprecise and qualitative information in an exact manner [10]. There are numerous methods for establishing the proportion of membership between two adjoining sets. The appropriate method is determined by the context of a particular application. Sigmoid shaped membership function is used to rank the cloud providers based on the following metrics such as service response time, sustainability, suitability, interoperability, availability, reliability, stability and cost. Service response time is computed by means of how fast the service/resources can be assigned for usage. Membership function is mapped to a membership value between 0 and 1. Sustainability refers the environmental impact of the cloud service used. Suitability indicates the requirement of user met by the cloud provider. Accuracy denotes the service functionalities measures to the user's actual values when using a service compared to the expected values. Interoperability is defined as the ability of a service to interact with other services offered either by the same cloud provider or other providers. Availability refers the percentage of time a user can access the service. Reliability denotes how a service operates without failure during a given time and condition. Adaptability means the ability of the service provider to adjust changes in services based on user requests. The fuzzy random membership function provides the maximum separation between those serials in the middle of the ranking system, while those serials at either extreme are bunched together closely.

To propose ranking mechanism based on Fuzzy random approach having three general phases such as problem decomposition, judgment of priorities and aggregation of these priorities.. The following membership fuzzy random function used is given as below

$A\alpha = \{x \epsilon U; A(x) \geq \alpha\}$for any $\alpha \epsilon$ [0, 1]-------(3.1)

$A\alpha = \{x \epsilon U; A(x)\overline{>}\alpha\}$for any $\alpha \epsilon$ [0, 1]------(3.2)

To rank the service providers, the service functionality attributes are classified into three categories such as class A, class B and class C. Class A refers high level attributes such as accountability, assurance, security and privacy. Class B refers next level attributes such as usability, reliability and Interoperability. Class C denotes low level attributes such as user interest, stability, Cost, throughput and efficiency. Broker is responsible for interaction with users and understanding their request needs. Ranking system considered two aspects such as (i) the service provider ranking based on Fuzzy set and (b) the final ranking based on the cost and quality ranking. Each attributes are combined with weight functions and become easy to ensure the achievement of the best compromise solution based on the objective function.

Ranking of Cloud services is one of the most challenging tasks in the framework of cloud. The Ranking System computes the relative ranking values of various Cloud services based on the QoS requirements of the user and features of the Cloud services. To calculate the selection of ranking the service provider using two distinct threshold values, then recalculated using a fuzzy set membership function to assign the membership values for each of the individual cloud provider ranking criteria and then used fuzzy composition rules to combine these data. Finally, the overall ranking of the cloud providers are considering by the Class C level attributes[12,5].

Cloud provider selection model is based on three steps of evaluation. First step is to identify the suitability of each service provider for the service render by the user. Suitability evaluation carried out by considering to reducing the effect of any particular measure in Class A. In second step, confirms that provider can extend services to the user render service request. Third step compare the cost and list the service providers. Cloud providers are selected based on the overall and individual cut off threshold values of the attributes considered for evaluation.

VIII. SIMULATION RESULTS AND DISCUSSIONS

The Simulations were implemented on the JADE 4.3.0 platform and on a computer whose configuration was an Intel Core i5-3337UCPU 1.80 GHz, 4.0GB RAM, Windows 7 (64 bits) operating system, Service Pack 1.Average response time and throughput was computed and the performance was also analyzed. The parameters considered for the simulation are number of users, number of cloud service providers, deadline of tasks etc. The execution time for each task is assigned randomly between 0.1ms to 0.5ms. Number of users considered are 1000, 5000 and 10000 at a time. Number of service providers available is fixed as 100, and deadline for each request is fixed as 0.5ms. Every cloud service provider has 50 computing hosts and a time-shared VM scheduler. Cloud broker on behalf of user request consist of 256MB of memory, 1GB of storage, 1 CPU, and time-shared Cloudlet scheduler. The broker requests instantiation of 25 VMs and associates one Cloudlet to each VM to be executed. There are two experiments were conducted and performance is analyzed with existing approaches.

The Simulation results prove that the proposed ranking model performs better in terms of average response time compared to the without ranking model in the Federated architecture. Simulation results are shown in Table 1. Average response time is defined as the time between when user requested for a service and actually accessible.

Table 1. Average response time of selection based with and without ranking model.

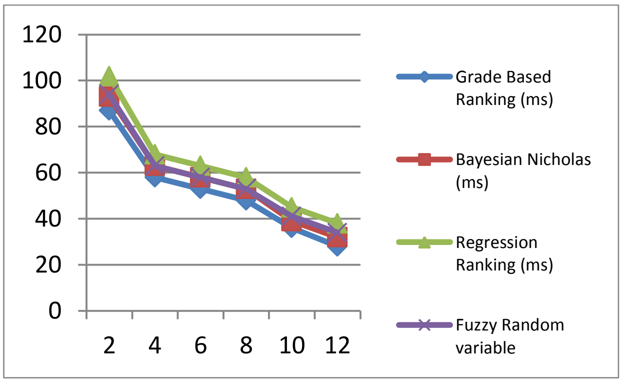
Number of users	Selection based on Ranking Model (ms)	Selection Without Ranking Model (ms)
1000	1.80	2 .08
5000	1 .93	2.24
10000	4.56	7.92

The result shows that the assigned cloud provider satisfies the requirements in terms of trust, security and performance. The overhead of the ranking mechanism depends on its implementation. The attributes in levels are assigned with constant and the execution time for performing ranking mechanism for 100 providers is 50ms.

In Simulation-2 we have conducted for the required application on the same platform for the average response time based on the number of service providers on different ranking models. We have taken the following ranking mechanism for our experiments. 1. Grade based Ranking, 2. Bayesian Nicholas ranking model 3.Regression ranking model and finally the proposed fuzzy Random variable selection Model. The Experimental results prove from the table-2 that the proposed fuzzy Random Variable based ranking model performs better in terms of average response time against other existing Ranking models in a federated cloud. The second Observation is that we can make is as the number of service providers are on the increase the minimal response time as been recorded for accessing the requested applications in the cloud.

Table 2. Average response time of selection based on different Ranking model.

Number of Service providers	Grade Based Ranking (ms)	Bayesian Nicholas (ms)	Regression Ranking (ms)	Fuzzy Random variable (ms)
2	87	93	102	94
4	58	63	68	63
6	53	58	63	58
8	48	53	58	53
10	36	39	45	41
12	28	32	38	34



Graph 1. Average Response Time

The Simulation results are tabulated and the graph is drawn on the resulted data. The graph clearly shows that among the average response time for different ranking methods, the curve drawn for fuzzy random variable deduction method covers trust, security and performance of the cloud service user in a federated cloud.

IX. CONCLUSION

Federated cloud computing has become an important technology for outsourcing various resource needs of organizations. Proposed broker based federated cloud mechanism helps to resolve the difficulties of selecting the optimal cloud provider for the service based on fuzzy random theory. The various mechanisms such as fault tolerant and risk based access control are proposed to ensure the believability of the federated cloud environment and characterizing the importance of each SMI attributes suggested by the cloud consortium. Fuzzy random theory based ranking model was simulated; the performance was compared with out ranking model and found that the proposed idea provides improved status to broker based federated cloud architecture. Future research will focus on mathematically formal frameworks for reasoning about trust, including modeling, languages, and algorithms for computing trust.

X. REFERENCES

[1]. Buyya, R., Yeo, C., Venugopal, S., Broberg, Cloud Computing and Emerging IT Platforms: Vision, Hype and Reality for Delivering Computing as the 5th UtilityFuture generation Computer Systems,(2009),pp.599-616

[2]. Garg, S., Versteeg, S.Buyya, R., SMI Cloud: A Framework for Comparing and Ranking Cloud Services2011 Fourth IEEE International Conference on Utility and Cloud Computing, (2011),pp.210-218

[3]. Buyya, R., Garg, S., Catheiros, R., SLA-Oriented Resource Provisioning for Cloud Computing: Challenges, Architecture and Solutions2011 International Conference on Cloud and Service Computing-CSC,(2011),pp.1-10

[4]. Rajarajeswari, C., Aramudhan, M., Ranking Model for SLA Resource Provisioning ManagementInternational Journal of Cloud Application and Computing,(2014)volume 4.pp.68-80

[5]. Aruna, L., Aramudhan, M., Framework for Ranking Service Providers of Federated cloud Architecture using Fuzzy SetsInternational Journal of Technology, (2016),Volume 4, pp.643-653

[6]. Kuan Lu, Ramin, Y., Fault-tolerant Service Level Agreement Lifecycle Management in Cloud using Actor systemFuture Generation Computer System.(2015)pp1-12

[7]. Aramudhan, M., Abdul Saleem, P.A., Framework for Ranking Service Providers of Federated cloud using Fuzzy Logic setInternational Journal of Technology, (2016)Volume 4, pp.643-653

[8]. Daniel, R., Carla, M., Risk-based Dynamic Access Control for a Highly Scalable Cloud FederationSECURWARE 2013: The Seventh Conference on Emerging Security Information, System and Technologies(2013), Pp.8-13

[9]. Thangaraj B., Gifta A.A.S., Complete 2-Fuzzy dual normed Liner spaces, Journal of Advanced Studies in Topology, (2013)Vol.4(2), pp.34-42

[10]. Daniel, R., Roberto, M., 2016A Framwork and Risk Assessment Approach for Risk based access Control in the cloudJournal of Network and Computer Applications.Vol 8pp.1-23

[11]. Gu, L., Wang, C., Zhang, Y., Trust Model in Cloud Computing environment based on Fuzzy theory, International Journal of Computer, Communication, control,(2014) Vol 9(5), pp.570 -573.

[12]. Vadivel, G., Arumudhan, M., 2017Priority Based Prediction Mechanism for Ranking Providers in Federated Cloud ArchitectureInternational Journal of Engineering Research and ApplicationVol(7)1, pp.81-85.

[13]. Ye Wang, Zengliang, L., 2013 Mobile Cloud Computing Network Attack and Defense Learning System Based on Fuzzy soft SetsProcedia Computer Science: Information Technology and Quantitative ManagementVol.17, pp.214-221.