Regression Tree based Ranking Model in Federated Cloud

S. Mourougan¹ and M. Aramudhan²

¹Periyar University, Periyar Palkalai Naagar, Salem - 636011, Tamil Nadu, India; smourougan@yahoo.com
²Department of IT, Perunthalaivar Kamarajar Institute of Engineering and Technology Nedungadu, Karaikal - 609 603, Puducherry, India; aramudhan1973@yahoo.com

Abstract

Background/Objectives: Federated cloud architecture is heterogeneous and distributed model that provides infrastructures related to cloud by aggregating different IaaS providers. In this position, it is an exciting task to pick the optimal cloud provider for the services and deploy it in affordable cost. In this paper, an effective new methodology for establishing trust and the different cloud providers based on the trust value using SMI attributes based on regression tree model is to enrich security and privacy in the federated cloud. Methods/Statistical Analysis: The scoring is computed based on the depth of the traversals in regression tree. Policy based trust, SLA verification trust; reputation trust and Evidence based trust are proposed in the architecture to build secured federated cloud. Findings/Conclusion: Broker trust level can also be identified and classified into four different categories such as completely trusted, partially trusted, minimally trusted and not trusted. Simulation results show that the performance of the ranked based mechanism depends on its implementation and better than without rank based federated cloud. Applications/Improvements: Will focus on mathematically formal frameworks for reasoning about trust, including modeling, languages and algorithms for computing trust.

Keywords: Federated Architecture, Policy Trust, Regression Tree, SLA, SMI

1. Introduction

Cloud computing is a promised developing model that offers cost effective outsourcing services to the users on demand and on basis of pay per utilization. Federated cloud architecture is heterogeneous and distributed model that provides infrastructures related to cloud by aggregating different IaaS providers. In this situation, it is an exciting task to pick the optimal cloud provider for the services and deployed it in affordable cost. Broker based federated architecture proposed to shortlist the providers for the specific service, the concepts of fuzzy logic set and plot care method used to rank the providers and choose the best provider for the service at that time¹. In these architectures, brokers were used to evaluate the providers based on the attributes prescribed by the Cloud Service Measurement Index Consortium (CSMIC). Brokers can be audited on certain attributes such as accreditation, policy compliance audit, attributes, self-assessment and information revealing to ensure the trustworthiness.

Trust is a factor that can be assessed at any level to get safety in the architecture. Trust is calculated between two entities whereas reputation is the comprehensive estimation towards that entity. Hence, it is essential in the practice to choose the provider from many attributes as evidence to make trust decision without particular requirements. Service Level Agreement (SLA) is an agreement that illustrates the level of performance ensured by the provider at the user side².³. After establishing a trust in service, monitoring and verification are the important

¹Author for correspondence
things to manage it. The existing architecture discussed in\textsuperscript{1} is customized and various trust mechanisms are suggested between broker manager and a pool of brokers to ensure the security and privacy in federated architecture. Trust management deals with how trust information is maintained, propagated and used in proposed architecture. SLA verification based trust model brings a new dimension of describing the reliable criteria for the selection process of cloud providers. Evidence based trust of each cloud provider has evaluated based on the energy consuming of software and hardware service. Broker trust level can be identified and classified into four levels such as completely trusted, partially trusted, minimally trusted and not trusted.

In the customized architecture, Broker Manager (BM) is responsible for resource provisioning and each provider has interconnected with broker. The communication between broker and BM is authenticated by suggesting using policy based trust mechanism. The trust of the broker is assessed based on the attributes as evidence, and performance metrics are used to verify the level of SLA extended by the provider. SLA is encompassed for the user by discovering appropriate service provider, describe and define their services properly, negotiate and delivers the service as per in the agreement\textsuperscript{2,3}. It is proposed that SLA based trust is implemented between user and service provider for efficient processing in federated cloud. This paper is organized as follows; section 2 describes the related work of trust computing. Section 3 illustrates the architecture and the various trust mechanisms suggested in the architecture. Section 4 reveals the performance of the proposed architecture and section 5 concludes with a discussion.

2. Related Work

\textsuperscript{4,5}Proposed trust evaluation system using hierarchical fuzzy inference system for IaaS service selection according to user requirements and past performance. Fuzzy membership functions were computed based on different QoS attributes suggested in Service Measurement Index (SMI) and matched with the requirement of the services through trust engine component. Trust model measures the security strength and computes a trust value. A trust value comprises of various parameters prescribed in SMI that are given necessary dimensions to measure the security of cloud services. Cloud Service Alliance service challenges are used to assess security of a service and validity of the model\textsuperscript{6}. Fuzzy Analytic Network Process based Evaluation Strategy (FANP) evaluates the user behavior by combining the advantages of Analytic Network Process and Fuzzy logic sets\textsuperscript{7}. In AHP, the low-level behavior evidence affects the higher-level sub-trust, while the high-level sub-trust does not affect lower-level evidence. FANP evaluates a user behavior trust to reflect the relationship between various behaviors evidence. Bayesian Network based Trust Management (BNBTM) uses multidimensional application specific trust values and each dimension is assessed using a single Bayesian network\textsuperscript{8}. The distribution of trust values is denoted by beta probability distribution functions based on the interaction history.

\textsuperscript{1}Proposed a new framework for cloud that maintains the SLA by means of distinguished incoming requests either SLA based member or SLA based non-member. This policy brings starvation that avoids by introducing a new algorithm called Distributed Loose Priority based scheduling. In addition to that the cloud providers are ranked based on plot care method and the average response time of the requests were calculated, analyzed and compared with existing method\textsuperscript{9}. Discussed the framework which measures the quality, prioritizes and selects the cloud services based on SMI metrics and ranking the services using Analytic Hierarchy Process (AHP). It is one of the flexible ways for solving and adapted to any number of attributes with any number of sub-attributes. AHP model has three phases such as forming hierarchy structure, pair wise comparisons and find aggregated value to generate ranking of the services. The authors proposed service mapper that contains a technique called singular value decomposition which is used for ranking the services in statistical manner.

3. Proposed Trust based Mechanism for Federated Architecture

The customized architecture of federated cloud is shown in Figure 1. The functionality of the architecture falls in three phases such as (i) Discovery of service providers (ii) Rank the selected service provider (iii) assigning the service to the best service provider. Broker Managers (BM) both primary and secondary collect the levels of services offered by cloud service providers based on their performance through broker learning algorithms. BM
communicates with brokers and short list the providers. Incoming requests are differentiated, based on the category, requests forwarded to either primary or secondary BM. Broker based Learning Algorithm (BLA) is used to study the workload of the providers, necessity tasks of users and requirement of resources. Cloud provider selection algorithm uses the quality metrics according to the Service Measurement Index (SMI)\(^6\), short lists the matched providers depending on the SLA and functional requirements. Let \( CP = \{ CP_1, CP_2, \ldots, CP_n \} \) be the list of cloud providers in the Federated Cloud (FC). Let \( CB = \{ CB_1, CB_2, \ldots, CB_n \} \) be the cloud brokers that connect CP to the Cloud Manager (CM) in the proposed federated cloud architecture. Cloud broker considered the list of QoS indicators \( Q_i = \{ Q_1, Q_2, Q_3, \ldots, Q_N \} \) 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. The matching of provider is identified by the representation of the given set
\[
MP = \{ QI, FA, RCP, CCP, SLAF \}
\]
(1)

MP denotes Matching provider for the service. QI is the list of Quality Indicator recognized by the SMI. FA discuss the functional requirements. RCP refers the resource demand by the service and released by the provider. SLAF means Service Level Agreement Factor, which is computed from the RCP. Cloud providers are clustered based on the type of service referred as Clustered Cloud Providers (CCP). Service Level Agreement (SLA) is measured as a trust between the user and a specific broker that is connected with the provider. Initially, SLA verification trust is established by the measuring metrics of the broker and later the qualified brokers connected providers are considered for the selection. Trust Authority (TA) is a centralized mechanism that manages security of cloud providers by computing the level of trust extended by the broker. The metrics such as accreditations, policy compliance audit, broker attributes, reputation and self-assessment are used to evaluate the level of the trust in each broker that connects with the providers.

Broker trust level can be classified into four different categories in accordance with the security of the broker. The levels are completely trusted, partially trusted, minimally trusted and not trusted. Accreditation is a status that denotes the Quality of Service (QoS) extended by the particular broker. Accreditation is classified into different grades A, B, C and D depending on the quality of service extended to the user. 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 Grade ‘D’. Later based on its performance, it may be reassigned with any higher grade for the broker. Broker attributes are used to justify the trust that includes competency, goodwill and integrity. Competency is measured by using Service Measurement Index (SMI) suggested by the Cloud Consortium. In this paper, Fuzzy Logic approach is used to evaluate the competency of the broker. Goodwill is computed based on the past performance of the broker. 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. It is very useful for the new user to know the maximum quality of the service promised by the broker. 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 of information about the service which is revealed by the provider.

### 3.1 Policy based Trust

Broker Manager (BM) plays an important role that manages the performance, selection and delivery of cloud services. Trust Authority (TA) performs issuing and maintaining valid public key certificates based on certain certificate policies to evaluate communication between broker, TA and BM. Any broker considered for assign-
ing service after evaluating the trust. Trust is computed by using the third party certificate authentication protocol. TA performs the functions such as validates the broker’s identity, issues certificates, maintains certificate status information regarding certificates and issues certificate withdrawal list. The following phases are performed to evaluate the trust of the broker such as registration, distribution and confirmation.

Step 1: Initially, brokers send its detail to TA along with identity number.

Step 2: TA generates a certificate, sends to broker and broker manager for authentication.

\[
C_iB_i = E(B_iid, certi(private key, SNO),\text{Cname}) \quad (1)
\]

\[
T_i = cert_i(B_iid,Pname,SNO) \quad (2)
\]

‘\(C_iB_i\)’ denotes the certificate for the broker that is issued by the TA. ‘\(B_iid\)’ refers the unique identity number of the broker and ‘\(\text{Cname}\)’ refers the name of the cloud provider. ‘\(\text{Cert}_i(\text{private key, SNO})\)’ is the certificate that must be kept by the broker to decrypt the subsequent messages from the number by the TA. If there is any uncertainty on the transactions of the broker, BM requests to change the ‘certificate by referring the ‘\(\text{SNO}\)’. Subsequently, message \(T_i\) forwards to the BM.

Step 3: Later, Broker sends its detail to the BM with ‘\(\text{SNO}\)’ for registration and it is verified by the BM and TA. Once it is verified successfully, registration is successfully completed.

Step 4: Authenticated trust is classified into different levels based on the SLA verification based trust. It is referred in section 3.2.

Step 5: Users look for the service from the federated cloud. Registrated Brokers at BM are distribute and based on the requirement of the user, brokers are selected, ranked and optimal one is confirmed for the service.

### 3.2 SLA Verification based Trust

SLA verification based trust model brings a new solution of defining the reliable criteria for the selection process of cloud providers. After establishing the policy based trust among the brokers and BM, the cloud user needs to verify, recalculate and evaluate the SLA to ensure QoS. Cloud resources released by different providers have different SLA and difficult to predict it at selection time can reduce overall application cost and risk. Evidence based trust of each cloud provider has evaluated based on the energy consuming of software and hardware service. In real-time management, it creates more communication overheads and increases execution time. Different services need different observation on software and hardware such as execution efficiency of VM (e), price for the utilization (p), trustiness of service (t) which is defined as the ratio between the execution time of successful tasks and the total execution time, average energy consumption of hardware service (ae) and performance in terms of speed (p) and number of transmission messages (m).

Total execution time of software services
\[
(Te) = \text{Number of submitted tasks (n)/e.}
\]

Total Cost of software services
\[
(\text{Tc}) = p*n/e.\]

Total execution time of hardware service
\[
(\text{He}) = Te + n*m/e.\]

Total cost of hardware service
\[
(\text{Hc}) = \text{Tc} \times \text{He}.\]

Energy consumption
\[
(\text{ec}) = t \times \text{ae} \times \text{Hc}.\]

Let user application have ‘\(n\)’ tasks, and submitted to run on ‘\(m\)’ machines from the cloud provider. Let ‘\(\text{He}\)’ be the execution time of \(n\) tasks on ‘\(m\)’ machine. Let \(\text{To}\) be the overhead caused due to infrastructure initiation delays and communication delays. Therefore, the throughput (t) of the provider is indicated as

\[
T = \frac{n}{\text{He} + \text{To}}
\]

### 3.3 Evidence based Trust

Service Measurement Index (SMI) attributes are designed based on the International Organization for Standardization (ISO) by the cloud consortium for the evaluation of the provider. Accountability, cost, performance and security are the major types of attributes that must be verified to ensure QoS. Accountability refers the group of QoS attributes such as auditability, compliance, data ownership, provider ethically, sustainability that used to measure the trust of the cloud provider. Performance denotes the functionality, response time and accuracy of the applications on the provider. Security maintains the confidentiality, privacy, data integrity and availability.

The expected behavior of application is based on the evidence about the SMI attributes of competency, good will and integrity with respect to that expectation. The general form of evidence based trust as follows
In equation (3), if an individual application believes an event ‘e’ has attributes ‘attr’, ‘with value ‘v’ …. ‘attrn’ with value, then app, trust in performance, e with respect to z, the performance of e or information created or believed by e, in a specific condition c. A belief in an attribute assessment is dependent on the value of entity and who makes the attribute assessment. The general form of trust in performance based on attribute performance is given as below

\[
\text{Trust(app}, TA, \text{attr(e,v)}, S) \land \text{madeBy(attr(e,v),TA,S)} \land \text{inSituation(S)} \Rightarrow \text{Believe (app}^i \text{, attr(e,v))}
\] (3)

In equation (4), if an application trusts Trust Authority TA to make assertions about the event e has attribute attr with the value v in specific situation S.

### 3.4 Reputation based Trust

Broker Manager plays a vital role as intermediaries between the providers and users with the aim of discharging the user from evaluating trust and risk of the provider has been used in the cloud environments. In the proposed architecture, brokers are interconnected with providers, collect the information periodically from the broker and update in the registry of the broker manager for decision making in selection of the optimal performance provider for the user. It is also very important to review the reputation of the provider in terms of successful project delivered, stability and available time for service. Generally, trustworthiness of the providers are calculated based on the past behaviors, broker manager and user ratings. The past behaviors of the providers are related to the Service Measurement Index (SMI) that provides a standardized method for measuring and comparing the services\(^1\). SMI suggests that user can select the provider based on accountability, assurance, cost, performance, security and privacy. Past behaviors can be identified either by the provider and sent to the broker or the analysis of the broker manager itself. The number of tasks executed by the provider within a time window ‘t’ is considered and the performance of the SMI attributes for the submitted tasks within a time window are evaluated in analyzing the behaviors of providers. Based on the values of the SMI, broker manager categorizes the status of the providers. There are n number of cloud users \{cu,cu2, cu3,…….cu_n\} and m number of cloud providers \{cp1,cp2,cp3,…….cm\} interacting with the help of broker manager. Broker manager interface is intermediary between providers and users. Broker Manager interface updates the interaction amongst their resources, provide feedback and calculate the rating of these interactions for establishing trust in an open dynamic environment. Broker maintains tables to check the credibility of resources and register the feedback score of each transaction of an entity. User rating denotes the satisfaction of the SMI attributes provided by the CSP corresponding to the requirements seeking by the user initially. The formal definition of the reputation trust is given as below

\[
R= \{CP, CU, B_T, SMI, T, U_r\}
\]

Let CP be the list of cloud providers in the federated cloud, CU denote the list of cloud users. B\(_T\) denotes the assessment of the broker which is connected with cloud provider. SMI\(_r\) refers to the level of performance on service measurement index attributes considered for the evaluation of provider reputation. Let T be the window time and U\(_r\) refers the ratings of the user registered for the service of the provider. Let SMI\(_r\)=\{SA\(_r\),SA\(_2\),…….SA\(_n\)\} be the QoS attributes, W\(_m\)=(m=1,2……M) be the weights, FV\(_i\)=\{fv\(_1\),fv\(_2\),…….fv\(_n\)\} be the threshold value to distinguish the levels of the reputation, EV\(_i\)=\{Ev\(_1\),Ev\(_2\),…….Ev\(_i\)\} be the actual value, the output falls on the category as \{C\(_r\),P\(_r\), M\(_r\),N\(_r\)\}. C\(_r\) refers as completely reputation it is highly rated by the user. P\(_r\) denotes the level as partial, M\(_r\) denotes as minimum reputation and N\(_r\) denotes as not reputation.

### 4. Trust based Ranking of Service Provider Model

The proposed trust based ranking model helps the user to find the most suitable cloud provider based on the past behaviors of provider and performance of service. Broker Manager is responsible for interaction with users and understanding their application needs. Broker Manager short lists the brokers that are connected with the provider. Ranking model ranks the short listed providers and finds the best which is more appropriate for the needs of the user. The past behaviors afford incidents related with the response time failure, stability, cost, elasticity and usability. Response time failure denotes how many times providers were not able to satisfy their capacity. Stability refers the variability in the performance of a service. Elasticity denotes how much a cloud service can be scaled during peak time. Usability means the average time...
experienced by the previous users of the cloud service to operate, learn, install and understand it. In this paper, classification and Regression trees methodology is used to rank the cloud providers based on the depth traversals. The constructing regression tree as ranking model is a challenging task but it includes the rules for splitting values at a node as attributes based on the value, stopping rules for deciding when it is terminated and can be split no more and prediction for the target SMI attribute. The first level refers the incidence related with past behaviors of the provider. The second level discusses the SMI of the service on the basis of priority. Third level relates with the level of trust. The provider score is defined based on the level of traversals and the list is prepared. The regression tree model for ranking the cloud provider is shown in Figure 2.

5. Simulation Results and Discussions

Simulation experiments were implemented on the JADE 4.3.0 platform\textsuperscript{12,13} and on a computer whose configuration was an Intel Core i5-3337U CPU 1.80 GHz, 4.0GB RAM, Windows 7 (64 bits) operating system, Service Pack 1. Average response time and throughput were 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 consists 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 were two experiments conducted and performance is analyzed with existing approaches.

The experimental 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.

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.

6. Conclusion and Future Work

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 regression tree. The various trust mechanisms are proposed to ensure the believability of the cloud environment and characterizing the importance of each SMI attributes suggested by the cloud consortium. Regression tree 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 architec-

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

<table>
<thead>
<tr>
<th>Number of users</th>
<th>Selection based on Ranking Model (ms)</th>
<th>Selection Without Ranking Model (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>1.80</td>
<td>2.08</td>
</tr>
<tr>
<td>5000</td>
<td>1.93</td>
<td>2.24</td>
</tr>
<tr>
<td>10000</td>
<td>4.56</td>
<td>7.92</td>
</tr>
</tbody>
</table>
ture. Future research will focus on mathematically formal frameworks for reasoning about trust, including modeling, languages, and algorithms for computing trust.

Reference