A REPUTATION BASED TRUSTWORTHY SYSTEM FOR CLOUD ENVIRONMENT

Priya G*1, N.Jaisankar2
Assistant professor (senior)1, professor 2
School of Computing Science and Engineering VIT University Vellore -632014.
Email: gpriya@vit.ac.in

Received on 10-08-2016

Accepted on 30-08-2016

Abstract

Cloud computing is one of the most prominent word of today’s promising technology. The main reason for the success of cloud computing is to create trust between cloud provider and cloud consumer. Trust is the important factor in cloud computing and it is mostly depending on observation of reputation and the self assessment by cloud providers. There are various actors involved in cloud environment such as cloud service provider, cloud consumer, cloud broker, cloud auditor and cloud carrier. Every service provider has their own features and behaviors. In this paper we propose an architecture for reputation based trustworthy system which provides the trust between customer and provider. It contains a trust evaluator which calculates the trust on various service providers based on the customer feedback and quality of service such as data handling. The calculated trust value is updated dynamically on database and finally the ratings of service providers will be displayed based on customer’s feedback.

Keywords: Cloud computing, Trust, Cloud service provider, Cloud Consumer, Reputation.

I. Introduction

The advancement of cloud computing in various fields is enormous. Even though it became an essential like water and electricity in our life but still security is the major concern. The cloud consumer, the owner of the data does not know where exactly the data is stored and whether the data is safe? How the user will believe the cloud providers? Who are the authorities to monitor, assess or validate cloud attributes? To answer the above questions we have to adopt Trust in cloud environment. According to NIST’s cloud computing definition, it has three service models software as a service, platform as a service and infrastructure as service and four deployment models private cloud, public cloud, hybrid and community cloud. If a customer needs any service first he has to send a request to a service provider. The request may
be processed by different service providers [5]. In that private scenario the trust plays the most vital role between the provider and customer.

The assurance level of Cloud service provider alone does not satisfy the customers because they are looking for other QOS parameters. In trust management there are two entities involved, they are trustor who creates the trust and trustee who manages the trust. Jingwei Huang[1] proposed two types of trust based on trustors expectancy. Trust in performance is the trust about what the trustee executes. Trust in belief is a trust about what the trustee believes.

Huang J.Nicol et.al., [4] proposed the following definition “Trust is a intellectual state which contains expectancy in which the trustor expects an exact behavior from the trustee, Belief in which the trustor trust that the predictable behavior occurs based on the proof of trustee’s ability, reliability and support and the trustor is keen to acquire the risk for that trust.

In order to make trust on CSP, the following elements to be considered the original feedback, reviews, Quality of service, deployment models, portability and security to convince the customers [6]. Most of the above elements are not satisfied by the service providers, so they have high chances of losing the trust in the system.[7]. Trust is based on customer feedback which prevents the risks[10].

This paper propose a reputation based trustworthy system which takes the feedback from various customers and then the trust is calculated by the trust evaluator and it is stored cloud database.[3]. This paper is organized as the following sections (i) Related Work (ii) Architecture for reputation based trustworthy system (iii) Conclusion.

II. Related Works

There were various researches have done on trust in order to improve the trust management in the cloud environment. Habib[8] proposed a comprehensive trust management system which tells the most excellent provider based on security, performance and compliance attributes. But he had not implemented trusted ratings dynamically.

Xiaoqi li [11] has proposed a architecture for trust management which uses Service level agreement based trust that afford the model to choose the most trust worthy provider among several service providers. Zhang et al., proposed trust as a service in which he describes adaptive trustworthy model and he differentiate trustworthy and malicious feedback [2]. Jingwei Huang et al., has projected various trust mechanisms [1]. We present those trust mechanisms and limitations in tabular format.
Table 1. Trust Mechanisms.

<table>
<thead>
<tr>
<th>Trust mechanisms</th>
<th>Main Idea</th>
<th>Limitations</th>
</tr>
</thead>
</table>
| Reputation based trust         | • Reputation of an entity is the collective opinion of a community towards an entity.  
                                  | • Reputation is the score reflecting the overall belief.                     | • Reputation is useful when we are choosing the service at the initial stage but it is inadequate afterwards.  
                                  |                                                                           | • The complexity is high because of more number of cloud users to rate a cloud service |
| SLA Verification based trust   | • The cloud user wants to verify and reevaluate the trust after establishing the initial trust.  
                                  | • Service level Agreement is contract between user and the provider.        | • It cannot deal with security and privacy.  
                                  |                                                                           | • Cloud users cannot evaluate on their own. They require a professional third party such as cloud broker or cloud trust authority. |
| Cloud Transparency trust       | • Cloud service provider gives self assessments in either a Consensus Assessments Initiative Questionnaire (CAIQ) or a cloud controls matrix. | • Dishonest service provider can strain out or modify the data               |
| Trust as a service             | • Introduce third-party professionals (commercial trust brokers)            | • Difficult to build the trust relation between cloud users and               |
                                  | • Cloud Trust Authority treat trust as a service to offer a single end for organizing and maintaining security of cloud services from several providers. | • Commercial trust brokers.                                                    |

III. Proposed Work

In this paper we propose an idea for reputation based trustworthy system, where the trust evaluator calculates the trust based on the customer feedback, number of customers and the quality of service provided by the particular cloud service provider. The dynamic display monitor shows the trusted system based on the above metrics.
The display monitor displays the trusted system based on the comparative result of previous and current input stored on the database. The monitor displays the updated content dynamically with respect to time. The cloud repository plays the role of database which stores the relevant information of the trusted service provider and it will be updated based on the current input. It has the collection of all related data of the system which calculates the trust towards the system. 

Figure 1 explains the detailed architecture of the proposed system which calculates the trust based on the customer feedback.

3.1 Cloud Consumer

The cloud consumer is the customer who gets the services from the cloud service provider based on their needs. The customer may be an individual or an organization. The cloud service consumer plays an important role in the proposed reputation based trustworthy system, in which they can give the feedback based on provider’s services and the trust evaluator calculates the trust based on the customer feedback.

3.2 Trust Evaluator

The trust evaluator calculates the trust based on the customers feedback, Quality of service and number of customers for the specific cloud service provider. The calculated trust value is displayed on the display pane that shows the trusty provider based on the previous and current value stored in the cloud store. The rating for the customer feedback is ranged between 0 and 5. According to their satisfaction on a particular service provider, the customer provides the feedback. The quality of cloud service provider can be ranged from 1 to 5 based on the parameters such as speed and data storage.
Trust value = \( \frac{(R_{cf} + R_{qs} + N)}{3} \)

Where \( R_{cf} \) is the feedback which is given by the customer for a particular service provider rating from 0 to 5. \( R_{qs} \) is the rating for quality of service by the consumer which is between 1 and 5. \( N \) is the total number of customers given feedback for the particular service provider. Finally the calculated trust value is stored in the cloud store.

### 3.3 Cloud Store

The cloud database stores the information about the service provider based on the customer’s feedback and the quality of service. Here the cloud store is the database which takes the trust value from the trust evaluator which is calculated after giving the ratings by the customer. It contains the list of values for each and every service provider offered by the customer. Cloud repository contains the current trust value \( T_c \) and the previous value \( T_p \) provided by the customer.

### 3.4 Display Pane

The display pane is a user interface which will display the result to the user. It shows the result of all service providers.

It gets the input from cloud repository where the values are updated based on the user data. It will check the current trust value with the previous trust value and it is updated in the cloud store and displays the service provider with highest trust value. It will also show the complete trust worthy system of the individual service provider. The performance is checked by comparing \( T_c \) and \( T_p \). If the current trust value is greater than the previous trust value then it is enough to prove that the service provider is trust worthy. Otherwise the service provider will be given the least preference in the list.

### 3.5 Cloud Service Provider

The cloud service provider provides the services to the cloud consumer based on their needs. There are various types of service providers with their unique characteristics and other several features. The user rate the cloud service provider based on the feedback given to the trust evaluator. The number of customers is high for the good service provider which makes that service provider is the best in the market.

**Algorithm for the Proposed Work**

**step1:** Cloud customer gives the feedback on particular cloud service provider and ratings on Quality of service provided by the service provider.

**Step 2:** Then it will be given to trust evaluator who calculates the trust value based on the customer feedback i.e \( \frac{(R_{cf} + R_{qs} + N)}{3} \) where \( R_{cf}, R_{qs} \) are ratings on customer feedback and Quality of service, and \( N \) is the total no of customers.
Step 3: The cloud store is the database which takes the trust value from the trust evaluator which is calculated after giving the ratings by the customer.

Step 4: Cloud repository contains the current trust value $T_c$ and the previous value $T_p$ provided by the customer.

Step 5: Display Pane gets the input from cloud repository where the values are updated based on the user data.

Step 6: It will check the current trust value with the previous trust value and it is updated in the cloud store.

6a. If the current value is greater than the previous value then the service provider is trustworthy.

6b. Else that service provider will be in the least preference list.

IV Conclusion

The cloud computing is one of the most extensively used technology in current trend. In this paper we introduce the reputation based trustworthy system to recognize the trusty cloud service provider among various service providers. The system calculates the trust for the cloud service provider based on the customer feedback and quality of service. The present system shows the trust value for the entire service providers on the display screen. Though we have several advantages on cloud computing but still security is the major concern. This problem can be recognized with the help of reputation based trustworthy system which is based on customer feedback.

References


3. S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, Volume 34, Issue 1, January 2011, Pages 1-11, ISSN 1084-8045


Corresponding Author:
Priya G*,
Email: gpriya@vit.ac.in