ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 12, December 2016

A Recommender System for Trust as a Service Layer in Cloud

E. GunaSekhar
M. Tech, Dept. of CSE
JNTUA College of Engineering
Anantapur, Andhra Pradesh, India

K. Madhavi
Assoc. Professor, Dept. of CSE
JNTUA College of Engineering
Anantapur, Andhra Pradesh, India

***Abstract*-Cloud computing provides many services such as Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS). These services are rendered along with other services in cloud. They are characterized by distributed, dynamic and non-transparent nature and cause challenges such as availability, security, and privacy. It is not easy to preserve privacy of consumers as the transactions between the consumers, so that the cloud services involve sensitive information. In this context it is very challenging to have a trust management service which provide another service layer known as Trust as a Service (TaaS). This layer when added to service stack of cloud, this cloud services wiil be rendered with in more secure environment. However it is an open issue to be addressed. The existing system proposed by Noor et all. has the design and also implementation of TaaS that provides set of services. These services are rendered based on the reputation and also will be based-on the Trust Management Framework. It has features like credibility of the Trust Feedbacks along with Robust Credibility Model, and Availability Model will ensure clock service. However, the TaaS can be improved further by combining with other Trust Management Techniques. The proposed system combines Reputation Based Trust Management System with recommendation model so as to improve the trust results accuracy. Such system can improve the decision making process with in the security of the system. Thus the TaaS service layer gets an improved means of delivering services in secure environment.**

Keywords **–Cloud computing, trust, reputation, recommender system**

I. INTRODUCTION

Now a days the Cloud computing has been emerged in order to provide valuable services to people and organizations across the globe. Cloud is nothing but a shared pool of resources which will be used by users in pay per use fashion. There are many services existed in cloud computing. However, Trust as a Service (TaaS) can help it to ensure that cloud services are provided with genuine intentions. This paper mainly focuses on the recommendations provided to cloud users for making well informed decisions on cloud services. General cloud computing phenomenon is as shown in the Figure.1

Figure 1: Cloud Computing Scenario

In the literature there was sufficient research on trust management in real world applications including cloud based ones. The Trust Management is most important topic pertaining to cloud computing and security [1], [2], [3]. For instance policy-based trust management techniques are among them. A trust cloud framework was proposed in [4] for trust and accountability in cloud based applications. There are five layers in the cloud trust framework. They include regulations, policies, system, data and workflow. These layers are meant for improving accountability in cloud based systems. They maintain cloud accountability life cycle which has many phases. They are known as policy planning, sensing and tracing, logging, safe-keep of logs, reporting, auditing, optimizing and rectifying. A compliance management approach was proposed in [5] for establishing trust between two parties.

A centralized architecture is used for achieving compliance management technique in order to establish trust among different factors such as service providers, service users and other stakeholders of cloud. Earlier policy-based trust management techniques were used. Of late trustworthiness of cloud service is assessed by using trust and reputation based mechanisms. Reputation does mean that high influence on the service users that is part of trust management system [6]. Especially cloud service users can influence the trust management systems. Te influence is either positive or negative. There are some research efforts that focused on trust based and reputation based security systems. A multi-faceted trust management is explored in [7] for the identification Trustworthy Cloud Service Providers.

The architecture models focused on trust models and Quality of Service (QoS) attributes such as customer support, availability, latency, and security. The architectures combine two kinds of techniques known as reputation and trust. The combination is made using different operations such as CONSENSUS, FUSION, NOT, AND, DISCOUNTING and OR. Secure aware cloud architecture was proposed in [8] assessing trust for the cloud services users and cloud service providers. Trust negotiation is used for establishing trustworthiness of the cloud service providers while Distributed Hash Table (DHT) is used for assessing trustworthiness of cloud service users. There is a problem with unpredictable reputation of the attacks which will mislead the trust feedbacks that are to be handled. The attacks are known as Sybil and the collusion attacks. Ability to provide secure and detect malicious activities is very important for many reasons. In [9] security issues like privacy, trust pertaining to cloud computing are explored. In [10] there was focus on digital identity management in privacy preserving fashion. In [11] a game theory was explored to protect the systems. With respect to public cloud, the security and privacy challenges which are presented in [12] while in [13] more focus was on trust based management in cloud computing. It advocates trusting strangers and also provides efficient trust mechanism in the cloud computing. Our work has being influenced by the work in [14] where reputation based trust management is explored for cloud computing. In this paper we proposed a framework that takes care of reputation based trust for cloud services.

II. PROPOSED SYSTEM

The main aim of proposed system is to build a recommender system on top of trust and reputation models in order to improvise the transparency in the system. The recommender system can help the subscribers of cloud services to provide honest recommendations. These recommendations help users to have quick decisions besides enabling them in taking well informed decisions. Recommender system is the sub system of a real world application. It is responsible to provide recommendations which are based on the study historical data. The data reveals the collaborative filtering of multiple users' transactions to provide useful insights. Thus recommender system plays an important role in the reality world and also in the online applications like e-commerce, education and healthcare domains to mention few.

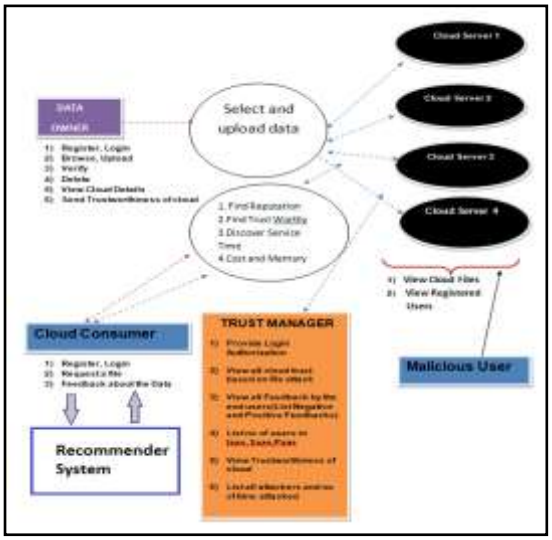

Figure 2: Shows Overview of the Proposed System
As shown in the Figure 2, there is quiet enough evidence which proves there are different roles which are involved in the system. Data owner,

cloud consumer, trust manager and malicious user. For the further demonstration the proof of concept, these roles support respective activities. The data owner can perform uploading data, viewing and manipulating it besides viewing cloud details and trustworthiness of cloud. The uploaded data goes to different cloud servers. The cloud consumer can view reputation, trust worthiness, discover service time, cost and memory. Malicious user can provide Attack Model so they could verify the resiliency with respect towards the proposed system. On top of this system recommender system is implemented which provides suitable recommendations pertaining to trust in cloud computing.

III. Algorithm Implemented for Recommender System

In order to have a recommender system, the data associated with the system is mined to extract trends in the system. The trends or patterns can help in understanding the hidden information. The trends and patterns are interpreted and converted into recommendations. Frequent Pattern Mining is used to obtain patterns from dataset.

Algorithm: Recommendations Algorithm
Inputs: Dataset ***D***, minimum support ***minSup***
Outputs: Recommendations

```
01    Initialize FIS for candidate frequent item sets
02    Initialize FIS' for final frequent item sets
03    Initialize recommendations R
04    Initialize trust t
05    Initialize reputation r
06    Initialize trust threshold tt
07    Initialize reputation threshold rt
08    FIS = extract candidate item sets from D
Find Candidate Frequent Item Sets
09    For each fis in FIS
10      Find count of fis
11      Associate count with fis
12    End For
Find Final Frequent Item Sets
13    For each fis in FIS
14      IF count>= minSup THEN
15        Add fis to FIS'
16      END IF
17    End For
Generate Recommendations
18    For each fis' in FIS'
19      IF t>= tt and r>= rt THEN
20        Add fis' to R
21      END IF
22    End For
23    Return R
```

Algorithm 1: Recommendations Algorithm

As shown above, the Algorithm 1 extracts frequent item sets that reflect the most used applications by the subscribers. The frequent item sets knowledge can help the application to have required business intelligence (BI).The BI can be used along with the knowhow of reputation and trust values in order to generate recommendations. Minimum support is the measure used to improve quality of patterns obtained for recommendations.

IV.IMPLEMENTATION

We implemented the proposed system as a prototype application using Java/J2EE platform. The implementation has different roles involves. They are data owner, cloud consumer and trust manager. Different cloud servers are involved in the system. They can store files view files and allow view file content.

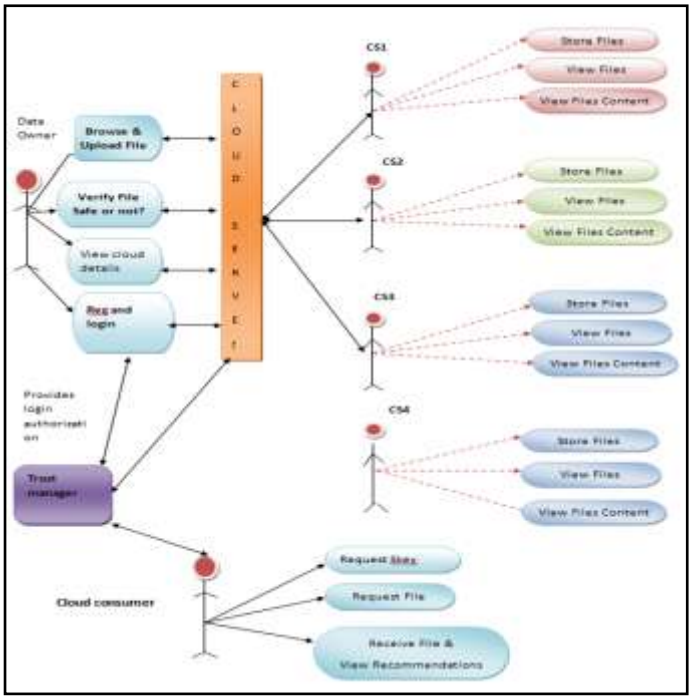

Figure 3: Overview of the Proposed Implementation

As shown in Figure 3, the cloud consumer has provision to have secure access to data besides viewing recommendations. The recommender system implemented as part of the proposed application can provide trust related recommendations to cloud consumers so as to help them to make well informed decisions.

V. EXPERIMENTAL RESULTS

The prototype application is evaluated with different performance measures such asavailability, reallocation, workload, and caching error.

Time Step	Estimated Availability	Actual Availability
1	0.1	0.5
2	0.75	0.75
3	0.8	0.82
4	0.72	0.7
5	0.73	0.73
6	0.73	0.73
7	0.72	0.7
8	0.73	0.73
9	0.7	0.7
10	0.74	0.73
11	0.75	0.74
12	0.74	0.73
13	0.7	0.58
14	0.74	0.73
15	0.74	0.73
16	0.71	0.71
17	0.73	0.73
18	0.73	0.73
19	0.67	0.67
20	0.69	0.78
21	0.69	0.8

Table1: Actual Availability vs. Estimated Availability

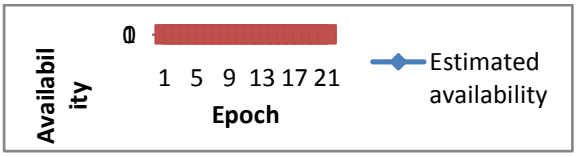

Figure 4: Actual Availability VS. Estimated

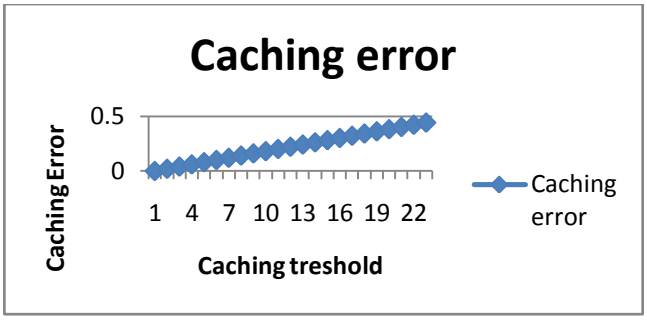

Figure 5: Trust Results Caching Error Rate

No. of Feedbacks	No Reallocation	Reallocation
1	1	3
2	3	3
3	3	3
4	4	3
5	4	3.8
6	5	3.8
7	5	3.8
8	6	3.8
9	6	3.8
10	6	3.8
11	7	3.8
12	7	3.8
13	7	3.8
14	8	3.8

Table3: Number of Feedbacks vs. Reallocations

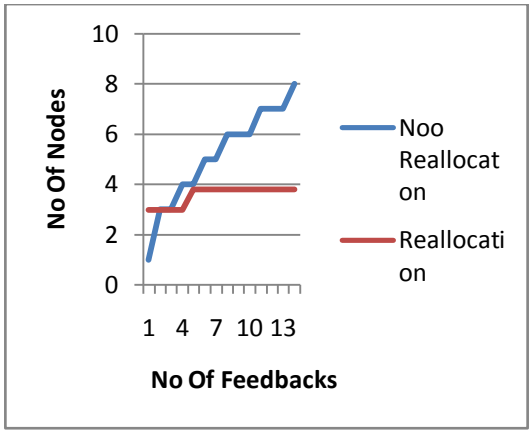

Figure 6:Number of Nodes Vs Feedback

No Reallocation	Reallocation
70	58
20	20
18	10
17	5
16	5
15	5
9	5
7	5
5	5
0	5

Table4: Number of Nodes Vs Workload Threshold

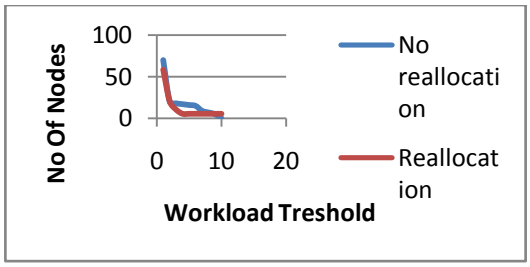

Figure 7: Number of Nodes vs. Workload Threshold

As shown in Figure 4, 5, 6, and 7, it is evident that the system is evaluated with different measures. The difference between estimated availably and actual availability is presented. Caching error for different caching thresholds is presented. Number of nodes vs. feed back in terms of reallocation and workload are presented.

VI. CONCLUSIONS AND FUTURE WORK

In this paper we studied cloud computing and its trust and reputation based approaches for making Trust as a Service (TaaS) which can be reused by people across the globe. We proposed an algorithm for recommendations which are based on the trust and reputation values. The reputation based trust management can help users to understand the credibility of different cloud services. Thus they can make well informed decisions. In this paper we implemented a prototype application that has implemented an algorithm for recommendations. Recommendations in the real world can help making decisions faster besides improving accuracy. The recommendations algorithm proposed in this paper is implemented for mining collaborative data and produce suitable recommendations. The empirical results revealed that the proposed system is very useful. In future we improve it further for various kinds of recommendations besides trust based services.

REFERENCES

[1] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A Survey of Attack and Defense Techniques for Reputation Systems," *ACM ComputingSurveys*, vol. 42, no. 1, pp. 1–31, 2009.

[2] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[3] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, "Trust Management of Services in Cloud Environments: Obstacles and Solutions," *ACM Computing Surveys*, vol. 46, no. 1, pp. 12:1–12:30, 2013.

[4] R. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. Lee, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," in *Proc. SERVICES'11*, 2011.

[5] I. Brandic, S. Dustdar, T. Anstett, D. Schumm, F. Leymann, and R. Konrad, "Compliant Cloud Computing (C3): Architecture and Language Support for User-Driven Compliance Management in Clouds," in *Proc. of CLOUD'10*, 2010.

[6] C. Dellarocas, "The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms," *ManagementScience*, vol. 49, no. 10, pp. 1407–1424, 2003.

[7] S. Habib, S. Ries, and M. Muhlhauser, "Towards a Trust Management System for Cloud Computing," in *Proc. of TrustCom'11*, 2011.

[8] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," *IEEE Internet Computing*, vol. 14, no. 5, pp. 14–22, 2010.

[9] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising From Cloud Computing," in Proc. CloudCom'10, 2010.

[10] E. Bertino, F. Paci, R. Ferrini, and N. Shang, "Privacy-preserving Digital Identity Management for Cloud Computing," IEEE Data Eng. Bull, vol. 32, no. 1, pp. 21–27, 2009.

[11] E. Friedman, P. Resnick, and R. Sami, Algorithmic Game Theory. New York, USA: Cambridge University Press, 2007, ch. Manipulation-Resistant Reputation Systems, pp. 677–697.

[12] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[13] F. Skopik, D. Schall, and S. Dustdar, "Start Trusting Strangers? Bootstrapping and Prediction of Trust," in Proc. of WISE'09, 2009.

[14] Noor, T. H., Sheng, Q. Z., Yao, L., Dustdar, S., and Ngu A. H. H. (2015). CloudArmor: Supporting Reputation-based Trust Management for Cloud Services. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, p1-14.