A Trust Evaluation Model to Recommend a Service Provider to a Customer in Cloud Environment

Shivani Taneja
Student, M.Tech (CSE)
DCRUST, Murthal

Kavita Rathi
Assistant Professor (Computer Science Department)
DCRUST, Murthal

ABSTRACT

In this era of cloud computing, there is a need to create some sense of security in customer's mind before they can transfer their critical data on cloud. However, this trust establishment between a customer and service provider is a difficult task. Trust depends on intuitive understanding of a human being. Thus, evaluation of trust remains a major issue while making headway towards Cloud Computing. There must be a trusted third party which can help the customer to select a trustworthy service provider from a large pool of providers. In this paper, a trust evaluation model is presented that can be taken as a base to establish trust on service providers. This model recommends a service provider to customer according to his requirements. It evaluates trust from different perspectives. It considers feedbacks from customers, past experience of customer with service provider as well as results of monitoring done by third party to evaluate trust factor. The model has been simulated and the results show that the proposed model is effectual and adaptable to customers' needs and priorities.

Keywords

Cloud computing, Recommendation, Trust Evaluation, Trust Issues, Trust Model.

1. INTRODUCTION

Cloud Computing is a just like a gust of wind in this era of computing. It can be thought of as a service factory. It provides on-demand services over the internet on utility-like basis i.e. pay only for the services you are using [1]. We can relate emergence of Cloud Computing to day-to-day necessities like electricity and water. Instead of having our own generators we rely on power stations to supply electricity. Water plants provide us water so that there is no need of our own wells [2]. In the same way Cloud Computing provide us with all the resources including software and hardware that are needed to do work. User stores their data in Cloud storage. However, if individuals have no idea why their personal information is being asked, or how and by whom critical data will be processed, this lack of control over data will finally lead to doubt and will ultimately result in distrust [3]. As a result, customers may restrain themselves from using cloud services. Establishing Trust between Cloud Service Provider and Cloud Consumer is a key criterion to adoption of Cloud services. Actually in Cloud Computing there is need of mutual trust between Cloud Service Provider and Cloud Consumer. For instance there may be some malicious users who may submit malicious code which could hamper working of cloud environment. On the other hand users lack control on sensitive data as they have no idea where the data is stored and how well it is protected [4]. Also a large number of Cloud Service Providers are available in market. In order to ensure security of data, it is required to establish trust on Cloud Service Provider before using its services. Since trust is a subjective and context-sensitive term so it is very difficult to select a trustworthy Cloud Service Provider [5]. Trust is not build in a day. It is generally build based on provider's reputation in market. Cloud consumers must be willing to trust providers to store data, in the same way as they trust banks to store their money [6]. Trust plays a great role in cloud computing. Till now, enterprises are reluctant to adopt cloud because of its various security, privacy and trust issues which leads to mistrust on service provider. Cloud service providers must provide users with sufficient security levels and assurance, that their privacy is respected. Evaluating trust involves various things such as [7] defining trust parameters, handling recommendations from malicious users , managing trust values on the basis of time.

Trust Evaluation mechanisms to some extent, helps in establishing relationship between cloud consumers and service providers quickly and safely [8]. As trust is a social problem, not purely a technical issue [9] it is difficult to effectively evaluate and manage trust. So, it is important that we grasp the meaning of trust in cloud and how relationships are actually established between consumer and provider. In this paper a trust model is presented which can be adopted by any third party to recommend a service provider to customer according to his requirements. The mechanism for trust evaluation considers feedbacks from customers and third party to evaluate trustworthiness of service providers.

The remainder of this paper is organized as follows, Section 2 describes the related work, Section 3 describes the proposed model, Section 4 is regarding experimental evaluation and finally paper is concluded giving future research directions.

2. RELATED WORK

This section describes various trust models that have been proposed by various researchers to evaluate trustworthiness of service providers in cloud environment.

S. Singh et al. [10] proposed a trust evaluation mechanism which evaluates trust value on service provider by considering user's past experience with Service Provider (based on total number of past interactions with Service Provider), feedback from friends (Friends evaluate trust value based on their past interactions with the Service Provider), Third Party's Recommendation (based on compliance level between services provided actually and that of agreed in SLA i.e. Service Level Agreement). Authors have simulated the model by assigning different values of weights to different types of trust.

The model presented by X. Wua et al. [11] is based on direct trust which is evaluated on the basis of number of valid interactions in evidence information base. Only valid direct interaction between customer and service provider is considered. And the recommendation trust is calculated by the recommendation information from other entities which have ever interacted with the service provider. Here trust values are evaluated on the basis of D-S evidence theory. Simulation experiments are performed in Netlogo.

In C.Qu and Buyya's [12] model trust is evaluated based on monitored results by cloud benchmark service .The proposed system consists of various components such as- Web interface through which users can specify even their vague preferences in linguistic phrases,

Discovery service module which retrieves services based on past from repository and Trust evaluation service module which evaluates trust. It takes user requirements and the services' past benchmark results as input and then outputs a list of services with their trust values regarding each attributes. A Cloud benchmark service monitors the performance of clouds.eg Cloud Harmony website. Here, trust is evaluated using fuzzy logic.

J.Sidhu et al. [13] presented a model, in which trust is evaluated on the basis of two parameters, monitoring services are installed at user end to check whether the Service Provider behaved in conformity with SLA and then a compliance report is generated. Same kind of reports are requested from peers and aggregated to obtain final trust value.

Z. Raghebi et al. [14] considered feedbacks to evaluate trust. Here similarity in common services used by two customers is evaluated. And then all the services that the customer (friend) has rated are compared with majority of feedbacks. The trust can be evaluated based on these two parameters. Authors used real-life trust dataset of Epinions rating for simulation work.

M. Wang et al. [15] proposed a model that first checks the correlation among users' ratings and then identifies collusive users and irresponsible users from that of the large pool of users. Then these collusive and irresponsible users are removed i.e. their ratings are not considered for trust evaluation. It also proposed a multi-faceted reputation evaluation method, which evaluates cloud service reputation from several angles with multiple attributes.

X. Li et al. [16] specify an attribute based trust management scheme for SLA guarantee and an adaptive model for measuring multi-dimensional trust attributes. It presents Cloud-Trust model for evaluating various cloud service providers on the basis of multiple trusts attributes. It makes use of rough set theory to discover knowledge from trusted evidences rather than weights that are assigned subjectively. The model consists of three modules: the trust management module, the SLA management module and the resource management module.

W. Li et al. [17] proposed a domain-based trust evaluation model. Resources that belong to the same provider will be managed in the same trust domain. A trust agent is associated with each domain. Each client stores or maintains a customer trust table. Agents stores and maintains a domain trust table. Here trust recommendation is considered as a type of cloud service. The model can work in cross-clouds environment.

A. Kanwal et al. [18] proposed an assessment criterion that helps the enterprise to select which trust model to be used. It helps customers to evaluate benefits and weaknesses of trust models. Evaluation is based on various parameters such as data integrity, data control and ownership, model complexity, detection of untrusted entities, process execution control, quality of services attributes and dynamic trust update and logging.

A framework presented by S.Habib et al. [19] evaluates and verifies the security controls as published by cloud providers. Hence it helps consumers to select a trustworthy service provider. It maps *CAIQ*-based security controls to trust properties, provides taxonomy of these properties based on their semantics and identifies different authorities who can validate the properties. The framework depends on the notion of hybrid trust which is a combination of hard and soft trust. Hard trust is derived from SLA's validation whereas Soft trust is derived from past experience.

W. Fan et al. [20] presented a problem of trust management in multi-cloud environments based on a set of distributed Trust Service Providers (TSPs). These are independent third-party trust agents which are trusted by everyone. These perform the task of trust evaluation. TSPs are distributed over the clouds, and they evaluate trust on the basis of evidence information. This evidence is information regarding the adherence of a CSP to a Service Level Agreement (SLA) for a cloud-based service and the feedback sent by CSUs. Using this information, they evaluate an objective trust and a subjective trust of CSPs. TSPs communicate among themselves through a trust propagation network that permits a TSP to obtain trust information about a CSP from other TSPs.

The trust evaluation model proposed in this paper evaluates trust from three different perspectives. The task of trust evaluation is done by a trusted independent third party. The model gives customers' the chance to show their trust on recommendation systems by assigning weights to them according to their intuition and experience. The complete model is explained in next section.

3. TRUST EVALUATION MODEL

The model is designed to evaluate the trustworthiness of cloud service providers at trusted third party and recommend the best provider. The trust is evaluated on the basis of feedbacks given by customers and monitoring done by trusted third party. The database of feedbacks is also maintained by third party. The third party monitors the interaction between a customer and service provider. It records the monitored results in database. A customer or user will specify their requirements in REQUEST for recommendation of a service provider. The third party would RESPONSE by recommending a provider to a customer according to their requirements.

In our model, trust evaluation is done by considering public trust, self-trust and third party's own trust. The trust model considers three systems for evaluating the final trust factor of a provider. These are:

1. Public-Recommendation System
2. Self-Recommendation System
3. Third Party-Recommendation System

Public trust represents the trust obtained from feedbacks by customers which interacted with providers. Self-trust represents the trust obtained from the past experience of the customer with provider. Third party's own trust is evaluated on the basis of monitoring done.

Figure 1 show a hierarchy of customers who interacted with providers, providers along with their services. Services are rated on a scale of 1 to 5 by customers while giving feedbacks. At level 1, we have customers who interacted with providers. At level 2, there are providers who are providing services to customers. At level 3, there are services which are rated by customers.

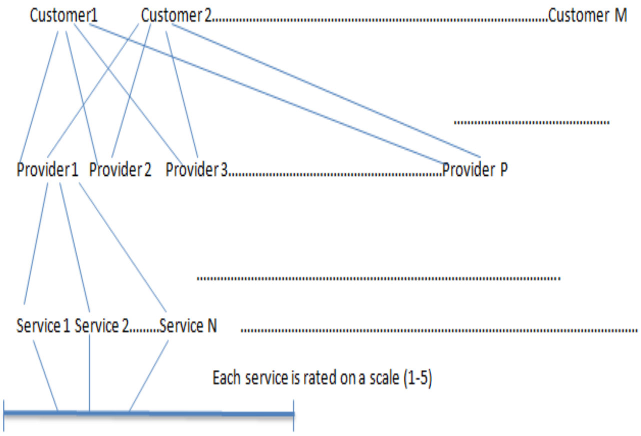

Customer1
Customer 2..........Customer M
Provider 1
Provider 2
Provider 3..........Provider P
Service 1 Service 2.........Service N
Each service is rated on a scale (1-5)

Figure 1: Hierarchy of users, providers and their services

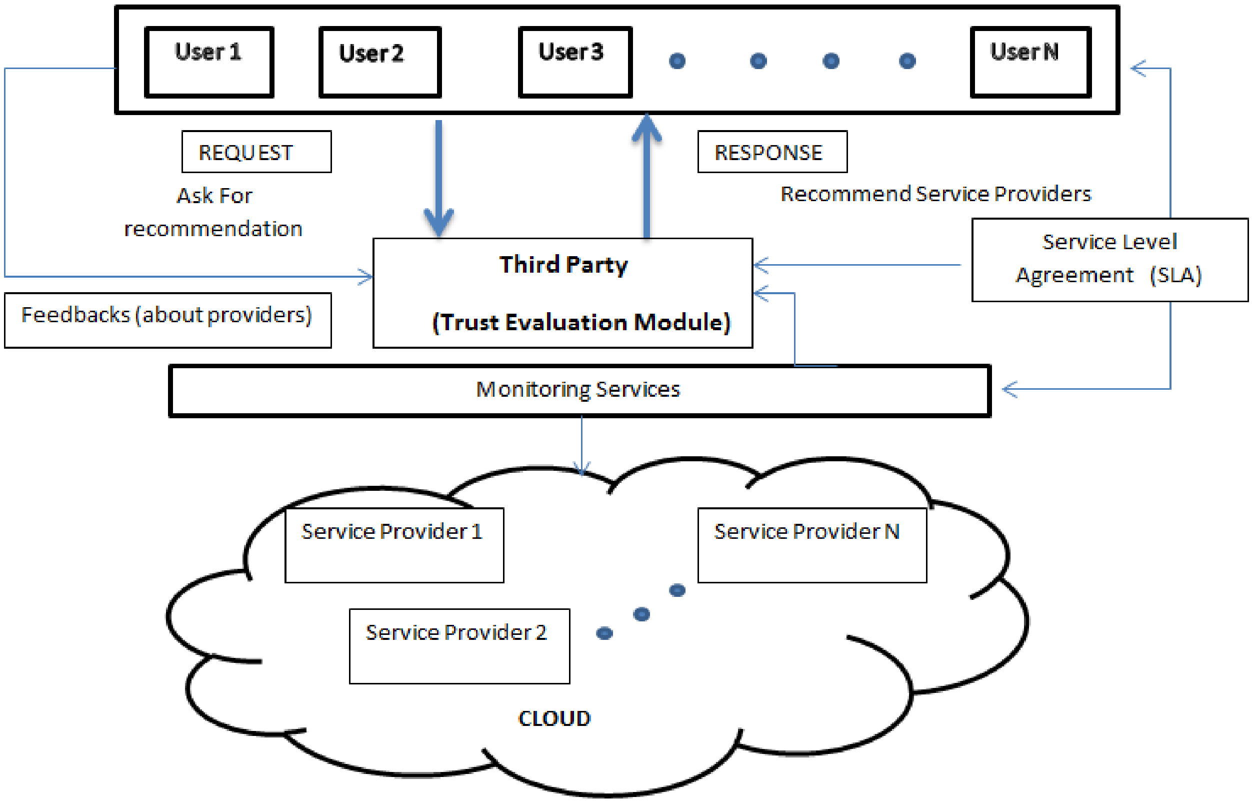


Figure 2: Cloud Computing Environment

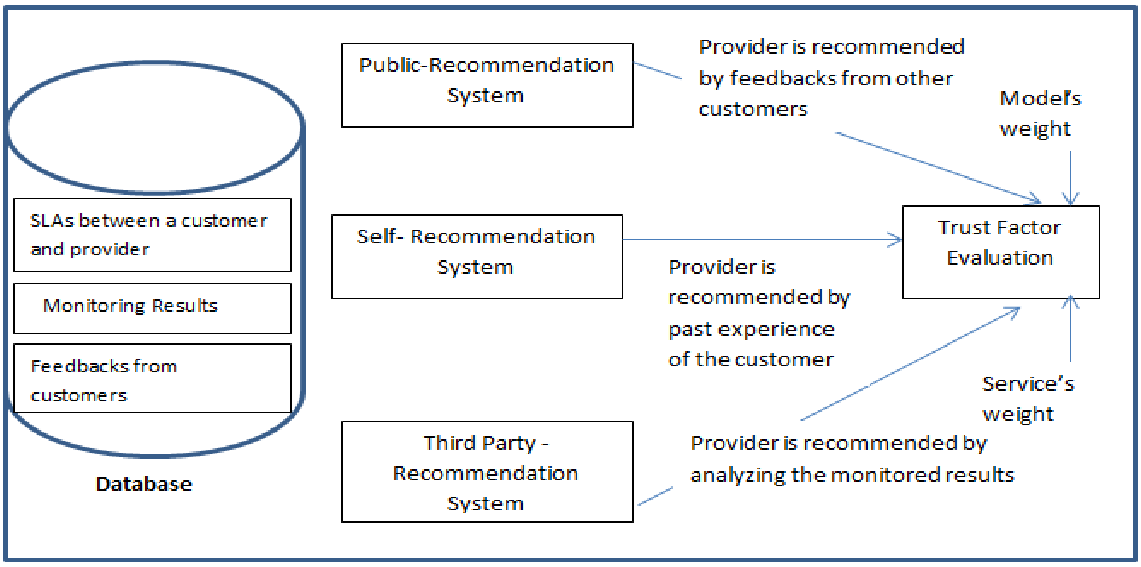

SLAs between a customer and provider
Monitoring Results
Feedbacks from customers
Database
Public-Recommendation System
Self- Recommendation System
Third Party - Recommendation System
Provider is recommended by feedbacks from other customers
Provider is recommended by past experience of the customer
Provider is recommended by analyzing the monitored results
Model's weight
Service's weight
Trust Factor Evaluation

Figure 3: Trust Model

The proposed approach for trust evaluation (in figure 3) is explained below in form of steps:

Step I: Specification of requirements, services and systems weight by a customer

a) Customers will specify their requirements in following form, say

Performance	Very High , High, Neutral, Low
Storage (RAM)	Very High, High, Neutral, Low
CPU Requirements	Very High, High, Neutral , Low
Network Requirements	Very High ,High, Neutral, Low
Security	Very High ,High, Neutral, Low

For ex: If a customer wants his system to be very secure then he must specify **'very high'** for security feature in his requirements. And if CPU requirements are low then he must specify **'low'** for CPU feature. Customer will be charged accordingly.

b) Customers are asked to give weightage to public, self and third party recommendation systems. Weights are assigned on a scale (0-1). The reasons for giving these weights is to check whose recommendations, customer trusts the most.

c) Customers are also asked to assign weight to every service according to its importance for them. Weights are assigned on a scale (0-1). The purpose of knowing the importance of services for a customer is to recommend them a provider who is able to at least provide the most important service.

Step II: Windowing (Selection of customers from database)

During this stage, a set of customers is selected from database. Since trust decays with time, so it is more efficient to consider recent feedbacks only .This is done by employing a window. A window size specifies the number of days. If a feedback lies in this window, then it is considered for trust evaluation purpose otherwise, rejected. Also, this concept of windowing is used by third party while analyzing the monitored results of interactions between customers and providers. It only analyzes the results which were stored during window size period.

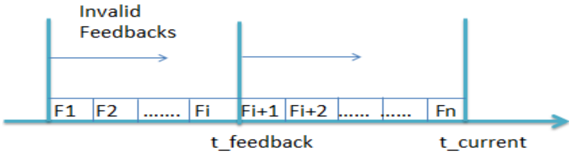


Figure 4: Windowing Concept

Total customers selected= Window (number _of_days, average_customers _per_ day) = number_of _days * average _customers _per _day

The total number of customers selected is product of number of days (window size) and average number of users present in the system per day.

Step III: Public -Recommendation System

The Public-Recommendation System works in following way:

a) Firstly, the requirements specified by the customer in REQUEST is matched with SLAs (of selected customers) stored in database to find the providers who actually provide the services which are being requested. We obtain a list of providers whose services match the customer's requirements.

b) Consider feedbacks of customers for only those providers which are present in list.

c) Now for every provider in the list and every service being provided by these providers, we take average of feedback values given by customers.

d) The output is a list of IDs of recommended providers according to services.

e) Finally, a provider is recommended by system that provides service which is most important to customer (assigned highest weight by customer).

```
For i= 1 to m    /* total users*/
  For j= 1 to p /* providers whose services customer 'i' has used in past*/
        If (REQUEST = SLA) /* SLA of user i with provider j */
            Providers_List = [Providers_List    j] /* Array of providers who provide services being requested by customer */
 L= length (Providers_List)
For k= 1 to L
            For q= 1 to n /* Total number of services */
                    Average _ Rating = mean (Customers_ Feedback (n))
                    Recommended_Provider (n) = max (Average_Rating (n))   /* Providers are  recommended service wise*/
Public _ Recommended_ Provider = Recommended_Provider ID (selected according to service with highest weight).
```

For ex:

Services	**Provider's ID**	**Service Weight**
Security	30	0.5
Performance	09	0.3
Storage	07	0.2

Here, the recommended providers' ID is 30 because customer has assigned highest weight to 'security', which means security is more important to customer than performance and storage.

Step IV: Self-Recommendation System

The Self-Recommendation System works in following way:

a) Firstly, the requirements specified by the customer 'A' in REQUEST is matched with SLAs (of selected customers) stored in database to find the providers who actually provide the services which are being requested. We obtain a list of providers whose services match the customer's requirements.

b) Consider feedbacks of customer 'A' for only those providers which are present in list, if customer 'A' has previously interacted with these providers. However if we have a new customer, then this system doesn't work.

c) Now for every provider in the list and every service being provided by these providers, we take 'MAX' of feedback values given by customer 'A'.

d) The output is a list of IDs of recommended providers according to services.

e) Finally, a provider is recommended by system that provides service which is most important to customer (assigned highest weight by customer).

```
For k= 1 to L
        For q= 1 to n /* Total number of services */
    Recommended_Provider (n) = max (A's_ Feedback (n)) /* Providers are   recommended service wise*/
Self_Recommended_ Provider = Recommended_Provider ID (selected according to service with highest weight).
```

Step V: Third Party Recommendation System

The Third Party-Recommendation System works in following way:

a) Firstly, the requirements specified by the customer in REQUEST is matched with SLAs (of selected customers) stored in database to find the providers who actually provide the services which are being requested. We obtain a list of providers whose services match the customer's requirements.

b) Compare the agreed values of services with the observed values during monitoring (for only those providers which are present in list).

c) The difference is converted into ratings on a scale (0-5). If difference is less than 20%, rating is 5. If difference is between 20-40%, rating is 4 and so on. These are stored in database as feedback values by third party.

d) Now for every provider in the list and every service being provided by these providers, we take average of these feedback values.

e) The output is a list of IDs of recommended providers according to services.

f) Finally, a provider is recommended by system that provides service which is most important to customer (assigned highest weight by customer).

```
For k= 1 to L
        For q= 1 to n /* Total number of services */
            Average _ Rating = mean (Third Party's_ Feedback (n))
                Recommended_Provider (n) = max (Average_Rating (n))  /* Providers are recommended service wise*/
ThirdParty_Recommended_Provider=Recommended_Provider ID (selected according to service with highest weight).
```

According to weightage given to public, self and third party recommendation systems by customer, a provider is recommended to customer.

Step VI: Evaluation of Trust Factor

A trust factor is evaluated for every provider, recommended by these three systems. Given below are the functions with parameters:

Public_Trust_Factor=TrustFactor(Systems_weight,Services_weight,Public_Recommended_Provider,UsersFeedback ,customer A, Third Party's _Feedback, service list)

Self_Trust_Factor=TrustFactor(System's_weight,Services_weight,Public_Recommended_Provider,UsersFeedback ,customer A, Third Party's _Feedback, service list)

ThirdParty_Trust_Factor=TrustFactor(Systems_weight,Services_weight,Public_Recommended_Provider,UsersFeedback ,customer A, Third Party's _Feedback, service list)

Trust Factor = α * Average_Rating by customers + β * Rating by customer 'A' + ϒ * Average_ Rating by third party

Here α = Weight assigned by customer to Public-Recommendation System

β = Weight assigned by customer to Self-Recommendation System

ϒ = Weight assigned by customer to Third Party-Recommendation System

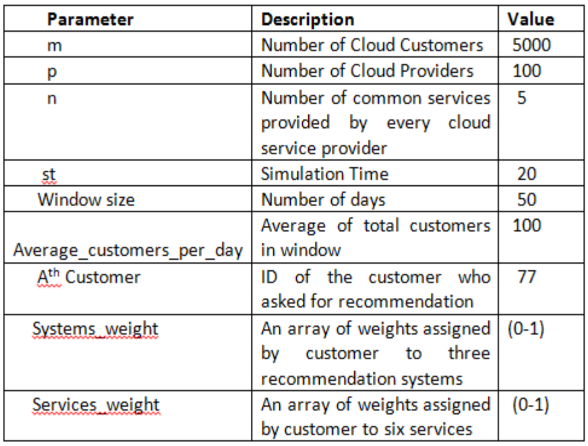
A provider whose trust factor is highest is also recommended to customer.

4. EXPERIMENTAL EVALUATION

Simulation Setup

To evaluate the performance of model, we simulate the model in MATLAB. We have used synthetic data for simulation purpose. Table 1 shows various parameters and their values that are considered for simulation purpose.

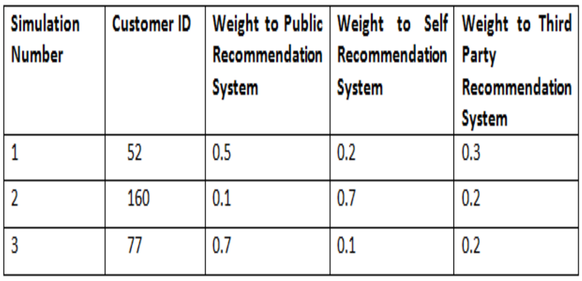
Table 1: Parameters and their values



Parameter	Description	Value
m	Number of Cloud Customers	5000
p	Number of Cloud Providers	100
n	Number of common services provided by every cloud service provider	5
st	Simulation Time	20
Window size	Number of days	50
Average_customers_per_day	Average of total customers in window	100
Ath Customer	ID of the customer who asked for recommendation	77
Systems_weight	An array of weights assigned by customer to three recommendation systems	(0-1)
Services_weight	An array of weights assigned by customer to six services	(0-1)

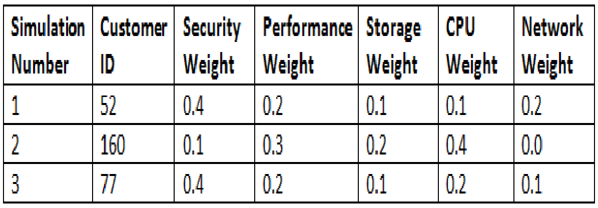
During simulation, 5000 customers interacted with 100 providers. A customer asked for recommendation while specifying his requirements and preference for recommendation system and service. Each recommendation system evaluated trust on service providers. Table 2 and Table 3 show weights assigned by different customers to recommendation systems and services.

Table 2: Example weights assigned by customers



Simulation Number	Customer ID	Weight to Public Recommendation System	Weight to Self Recommendation System	Weight to Third Party Recommendation System
1	52	0.5	0.2	0.3
2	160	0.1	0.7	0.2
3	77	0.7	0.1	0.2

Table 3: Example weights assigned by customers to services



Simulation Number	Customer ID	Security Weight	Performance Weight	Storage Weight	CPU Weight	Network Weight
1	52	0.4	0.2	0.1	0.1	0.2
2	160	0.1	0.3	0.2	0.4	0.0
3	77	0.4	0.2	0.1	0.2	0.1

A service provider was recommended by every system according to its evaluation strategy. Initially, a service provider is recommended according to output of recommendation system having highest weight (given by customer). Then, trust factor of these three providers is evaluated and a provider with highest trust factor is also recommended. Now, it's up to customer to select a provider out of these two.

Results and Discussion

Graph in figure 1 shows the trust factor obtained, for the three providers which were recommended by three systems separately. The graph is generated for recommendation request made by a customer with ID 77. Customer with ID 77 is recommended 76th provider because customer has given highest weight to public recommendation system.

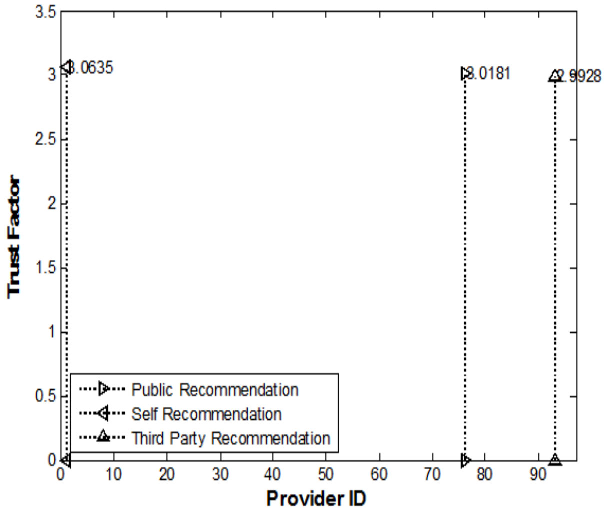


Figure 5: A graph showing trust factor of service providers recommended by three systems

However, according to graph in figure 5, the highest trust factor (3.0635) is obtained for service provider with ID 1. It is recommended by Self-Recommendation System. The lowest value of trust factor is for the provider who is recommended by Third party-Recommendation System. Figure 6 shows the recommended provider with trust factor and number of services being provided. We can generate similar graphs for different customers and their preferences for services and their trust on public, self and third party. The graph helps us to analyze the overall trust factors of all the recommended providers.

The value of trust factor is dependent on feedback values and monitoring done by third party. The proposed evaluation model evaluates trust from three perspectives i.e. customer's own experience, feedbacks from other customers and analyzing third party monitored results. The model allows the customer to specify priority of services required. Customer can show his trust over recommendation systems by assigning weight to them. Thus, we can say model is adaptable to customers' requirements.

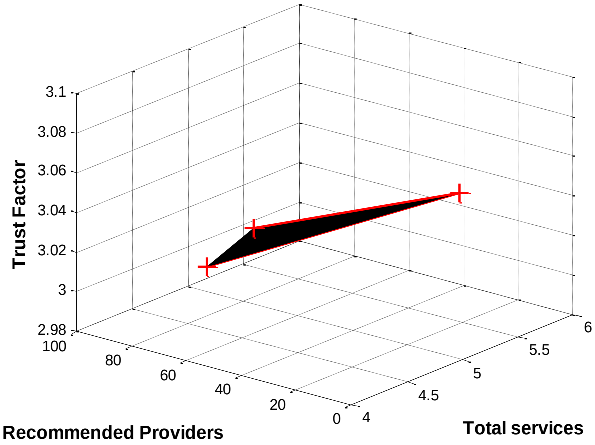


Figure 6: Recommended Provider along with trust factor and services

5. CONCLUSION AND FUTURE WORK

Trust evaluation is important as it helps the customer to select a trustworthy service provider. Before transferring customers' critical data on cloud, there is a need to establish trust between cloud customer and provider. This paper has presented a trust model which can help the customer to evaluate trustworthiness of various service providers available in market and select the best provider according to their needs and priorities. A trusted third party monitors every interaction between a customer and provider and stores the result in database. It also maintains feedbacks given by customers. It evaluates trust from three different perspectives. It considers past experience of a customer, feedbacks from other customers and its own monitoring results to find out which service provider is suitable for a customer. The model allows the customer to specify priority of services required. Customer can show his trust over recommendation systems by assigning weight to them. The model is adaptable to customers' requirements. This approach can be adopted by any third party while evaluating trust on cloud service providers. In future, we are going to use an approach to filter feedbacks from malicious customers. Also, model will be extended to work in scenario where two or more cloud service providers are inter-connected.

6. REFERENCES

[1] K. Rathi, S. Taneja, "TRUST EVALUTION IN CLOUD COMPUTING: A SURVEY", *International Journal of Innovative Research in Computer Science & Technology*, vol.3, Issue 1, 2015, pp. 48-52.

[2] S. Zhang et al., "Research on Key Technologies of Cloud Computing", *International Conference on Medical Physics and Biomedical Engineering, Procedia Physics*, 2012, pp. 1791-1797.

[3] S. Pearson, A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing", *in proceedings of 2nd IEEE International Conference on Cloud Computing Technology and Science*, pp. 696-702.

[4] Tian li-qin, LIN Chuang, “Evaluation of User Behavior Trust in Cloud Computing” *IEEE International Conference on Computer Application and System Modeling (ICCASM 2010)*, 2010, pp. 567-572.

[5] A. Kanwal et al. “Assessment Criteria for Trust Models in Cloud Computing” *in proceedings of IEEE International Conference on Green Computing and Communications*, 2013,pp. 254-261

[6] R. Bose et al., “The Roles of Security and Trust: Comparing Cloud Computing and Banking” *2nd International Conference on Integrated Information, Procedia - Social and Behavioral Sciences*, pp. 30-34, 2013.

[7] D. Sun et al., “Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments” *Advanced in Control Engineering and Information Science, Procedia Engineering*, 2011, pp. 2852- 2856.

[8] A. Sarwar et al., “A Review of Trust Aspects in Cloud Computing Security” *International Journal of Cloud Computing and Services Science*, vol.2, no.2, 2013, pp. 116-122.

[9] Kai Hwang, Deyi Li, “Trusted Cloud Computing with Secure Resources and Data Coloring”, *IEEE Internet Computing*, vol. 14 , Issue 5,2010, pp. 14-22.

[10] S. Singh, D. Chand ,“Trust Evaluation in Cloud based on Friends and Third Party’s Recommendations” *in proceedings of IEEE International Conference on Recent Advances in Engineering and Computational Sciences* , 2014.

[11] X. Wua et al., “A trust evaluation model for cloud computing”, *Information Technology and Quantitative Management*, 2013, pp. 1170-1177.

[12] C.Qu , R. Buyya , “ A Cloud Trust Evaluation System using Hierarchical Fuzzy Inference System for Service Selection” *IEEE Conference on Advanced Information Networking and Applications*, 2014,pp.850-857.

[13] J. Sidhu, S. Singh, “Compliance based trustworthiness calculation mechanism in cloud environment,” *International Workshop on Intelligent Techniques in Distributed Systems*, 2014, pp.439-446.

[14] Z. Raghebi, M. R. Hashemi, “A New Trust Evaluation Model based on Reliability of Customer Feedback for Cloud Computing”, *National CSI computer conference, Tehran, Iran*, 2013.

[15] M.Wang et al., “An Accurate and Multi-faceted Reputation Scheme for Cloud Computing” *in 11th International Conference on Mobile Systems and Pervasive Computing*, 2014, pp. 466 – 473.

[16] X. Li, J.Du, “Adaptive and attribute-based trust model for service-level agreement guarantee in cloud computing” *IET Inf. Secur.*, 2013, Vol.7, Iss. 1, pp. 39-50.

[17] W. Li, L. Ping., “Trust Model to Enhance Security and Interoperability of Cloud environment” *CloudCom2009, LNCS 5931*, 2009, pp. 69-79.

[18] Ayesha Kanwal et al. “Assessment Criteria for Trust Models in Cloud Computing” *in proceedings of IEEE International Conference on Green Computing and Communications*, 2013,pp. 254-261.

[19] S.Habib, V. Varadharajan and M. Muhlhauser , “ A Trust-aware Framework for Evaluating Security Controls of Service Providers in Cloud Marketplaces” *, in proceedings of IEEE Conference on Trust, Security and Privacy in Computing and Computations*,2013, pp.459-468

[20] W. Fan, H. Perros ,“A novel trust management framework for multi-cloud environments based on trust service providers” Knowledge-Based Systems,2014, pp. 392–406.