Advances in Science and Technology
Research Journal
Volume 10, No. 30, June 2016, pages 32–37
DOI: 10.12913/22998624/62703

Research Article

FUZZY BASED TRUST MANAGEMENT SYSTEM FOR CLOUD ENVIRONMENT

Sunil Kumar[1], Sumit Mittal[2], Manpreet Singh[3]

[1] Department of Computer Science & Applications, Guru Nanak College for Girls, Sri Muktsar Sahib, Punjab, India, e-mail: sarora66078@yahoo.co.in

[2] M. M. Institute of Computer Technology & Business Management, Maharishi Markandeshwar University Mullana, Ambala, India, e-mail: principalmmictbm@mmumullana.org

[3] Department of Computer Science & Engineering, Maharishi Markandeshwar University, Sadopur, Ambala, India, e-mail: dr.manpreet.singh.in@gmail.com

Received: 2016.03.06
Accepted: 2016.04.25
Published: 2016.06.01

ABSTRACT
Cloud computing is a business model with high degree of flexibility, scalability in providing infrastructure, platform and software as a service over the internet. Cloud promises for easiness and reduced expense to service providers and consumers. However, a lack of trust between these two stakeholders has hindered the universal acceptance of cloud for outsourced services. In this paper, a fuzzy based trust management system is proposed to facilitate cloud consumers in identifying trustworthy providers. The performance of the proposed system is validated through a simulation using CloudAnalyst and Simulink.

Keywords: cloud computing, trust model, fuzzy logic, cloud analyst.

INTRODUCTION

Cloud computing provides many opportunities for consumers by offering a diversity of services [1]. However, consumer reluctance in adoption of cloud computing due to its data under the control of the other, unclear security assurance and lower transparency is justified to some extent. Establishing trust for successful relationship between service providers and consumers is a vital component of cloud computing [2]. Cloud clients ought to have trust that the cloud service providers will finish the submitted jobs according to the Service Level Agreements (SLA) and processed data information will be kept secured [3]. Trust management is an integral part of commercial aspect of cloud technology [4]. Organizations like Google and Amazon have actualized reputation based on Trust Management framework which helps the service consumers to find the trustworthy resource providers for doing e-business transactions in a secure and confident way.

The objective of this paper is to propose a Fuzzy based Trust Management System for the selection of Cloud Service Provider (CSP) from the available ones. A trust value for each CSP based on the four basic parameters: security, availability, cost and performance is evaluated using fuzzy logic. These input parameters to fuzzy model are calculated based on the simulation results of cloud analyst.

RELATED WORK

Security issues and trust in the area of distributed environment is always a key area of research. Various models have been proposed to resolve the issue related to trust in cloud. However, there is still a lot of scope of improvements regarding effective dynamic trust establishment in Cloud environment.

In [5], authors presented a trust model for reconfiguration and allocation of computing resources to satisfy user's requests. The reliability of each resource is collected and analyzed based on historical information of servers in a cloud data center in order to provide the best resources

to users. Experiments for reliability analysis are carried out with 4 data types, including all data set, random data set, recent data set, and the data set within a standard deviation.

A comprehensive survey focusing on the trust management of services in cloud environment is presented [6]. A generic framework is also proposed considering a logistic view of trust related issues for interactions in cloud.

In [7], authors suggested a trust model to measure the security strength and computation of trust values. CSA (Cloud Service Alliance) service challenges are used to assess security of a service and validity of the model. Adequacy of the model is also verified by evaluating trust value for existing cloud services.

A trust assessment model for cloud alliance is proposed to assess and build up bi-directional trust between various CSPs [8]. The assessment of trust depends on feedback gathered from enlisted cloud clients and Service Level Agreements of CSPs.

In [9] creators outlined a mechanism to compute trustworthiness of cloud service providers. It is calculated depending upon their compliance to promised SLA parameters. The simulation of the model is done using MATLAB. After simulation the validation of the model is completed using synthetic data set. Results demonstrate that approach is workable and can be utilized to evaluate trustworthiness of cloud service providers in a cloud.

A novel trust model which ensured the security of both cloud customers and providers in cross-clouds applications is proposed [10]. The cloud nodes are divided as customers and servers and different trust strategies for them are assigned. In this model, trust recommendation is treated as one of the cloud services. The experimental results confirm that the proposed model can efficiently and safely construct trust relationship in cross-clouds environment.

In [11], a fuzzy mathematics-based trust model is proposed for cloud services. It works on the success & failure interaction of the cloud entities so that the fuzzy direct trust relation is calculated in the light of direct experiences between clients and cloud service providers. Also, the substances can manufacture a fuzzy indirect trust relation with each other through their acquaintances. Simulation results demonstrate that the proposed model equipped for recognizing frauds and the performance of whole cloud will be improved.

A trust model based on virtual machines, with two considerations is proposed [12]. First, a timeliness strategy is introduced to ensure the response time and also to minimize the idle time of servers. Second, the linear trust chain by differentiating the trust of the platform domain and user domain is extended. Besides, a fuzzy theory based method to calculate the trust value of cloud service providers is developed.

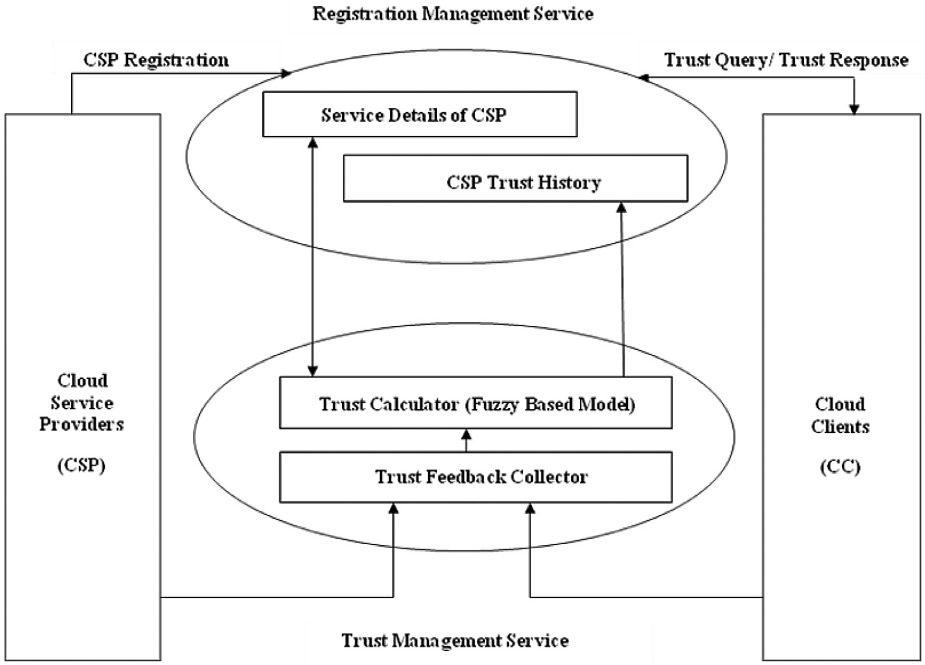

Fig. 1. Framework of Proposed Trust Management System

PROPOSED SYSTEM

In this section, a framework for trust management in cloud environment is proposed. Along with the service providers and consumers; Registration Management Service and Trust Management Service are the two main modules of the system, as shown in Figure 1.

Registration Management Service. The Registration Management Service (RMS) is responsible for the registration of cloud service providers. During registration phase; the details of all services offered by service providers are recorded to be used later in the Trust Calculator module. The RMS also publishes the updated trust values of each service provider as generated by the Trust Calculator.

Trust Management Service. The Feedback Collector module of Trust Management Service (TMS) on receiving an update (the experience of a success/ failure of a service) from a cloud client pertaining to a service provider; communicate relevant information to the Trust Calculator. The fuzzy based Trust Calculator module modify the trust value of the service provider using the feedback obtained along with the service details made available from RMS.

Fuzzy Based Trust Model

The Fuzzy model gives the degree of trust corresponding to each CSP after going through three phases as shown in Figure 2. In the first phase, all requisite details pertaining to each CSP are made input to CloudAnalyst. In the second phase, the simulation results of CloudAnalyst and customer's experience regarding security assurance of CSP are provided to Fuzzy Inference System (FIS) and in the third phase output of second phase are combined through another FIS to get the trust degree of each CSP.

The four fuzzy modules used in second phase of trust model are Efficiency and Performance, Cost, Adaptability and Security. The Efficiency and Performance module, Cost module get their inputs (Response Time, Data Center Processing Time) and(VM cost, Data Transfer Cost) respectively on the results of simulation performed through Cloud Analyst. Adaptability module is based on the direct inputs (Physical Units, Memory, Virtual Machine) provided to the CloudAnalyst and the Security module is based on the direct experience of the customers corresponding to Confidentiality, Availability and Usage Restriction, Backup and Recovery .

All these inputs are combined with the help of Simulink tool of Matlab and got the final rating based on these parameters. To design the FIS for four basic modules and final Trust rating modules Mamdani FIS is used in this proposed work.

SIMULATION AND RESULTS

The implementation has been done in three phases, first deals with implementation of simulator (Cloud Analyst) with different parameters,

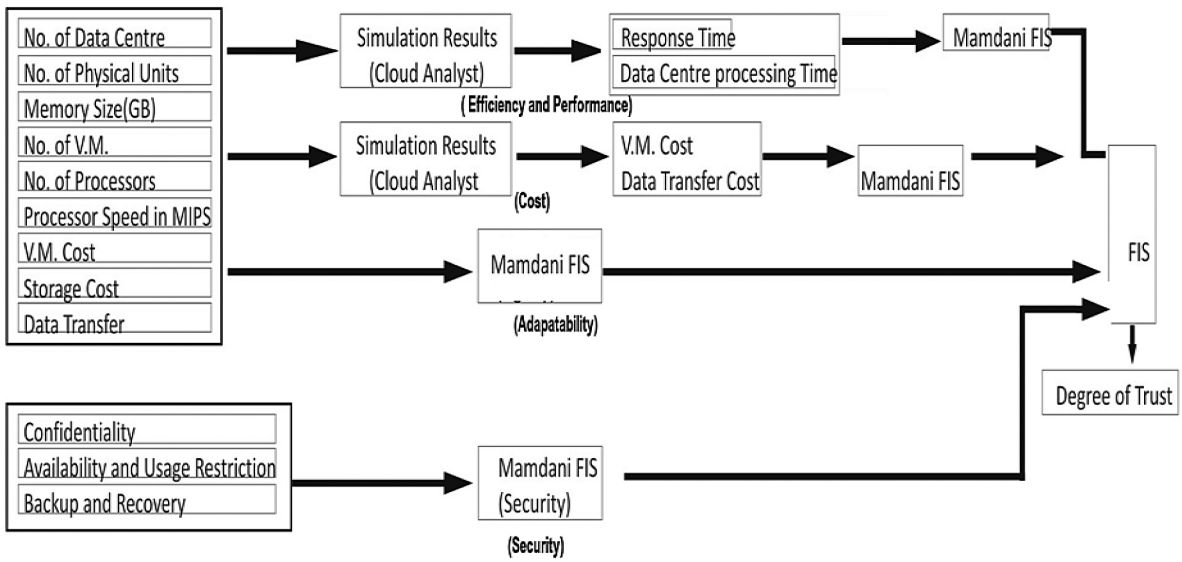

Fig. 2. Fuzzy Based Trust Model

Table 1. Simulation Parameters for CloudAnalyst

CSP	No. of datacenters	No. of physical units	Memory size [GB]	No. of V.M.s	No. of processors	Processor speed (MIPS)	Cost [$]		
							V.M.	Storage	Data transfer
A	10	10	10	50	40	100000	0.4	0.15	0.15
B	6	20	3	18	80	80000	0.2	0.2	0.12
C	3	15	3	30	45	120000	0.05	0.08	0.2
D	2	10	4	20	75	80000	0.8	0.25	0.05
E	4	40	8	80	160	160000	0.15	0.15	0.09
F	8	18	16	40	90	100000	0.45	0.28	0.12
G	7	21	7	35	63	60000	0.6	0.3	0.25
H	6	18	6	24	72	75000	0.3	0.32	0.11
I	5	20	5	25	100	10000	0.55	0.27	0.07
J	9	27	9	45	108	90000	0.37	0.21	0.14

second designed of FIS for basic four modules and last deals with the design of FIS based on the output of four modules for the final trust rating.

Simulation Setup

Simulation is carried out using CloudAnalyst configured in Eclipse and Simulink toolkit of MATLAB 7.1 on an Intel Core 2 Duo, 2.0 GHz Linux based laptop. The user base (fixed as 10 CSP) is selected in such a way that represent user all across the globe. The same amount of user load has been considered to define the performance of various CSPs.

Table 1 describes the simulation parameters for cloud Analyst. The scheduling scenarios have been executed sufficient number of times to arrive at results as shown in Table 2.

Fuzzy Module Implementation

After the results from CloudAnalyst, four rule based Fuzzy Inference System designed with different input parameter with variant range come into existence, these modules give different output values based on their inputs and applied rules.

Efficiency and Performance FIS give the results based on two inputs: response time and DC processing time received as results from the simulator and four rule base. Cost FIS gives the results based on the two inputs: total VM Cost and Total Data Transfer Cost and four rule base. On the other hand, Adaptability FIS is based on the three inputs: Physical Units, Memory, VM and nine rule base is designed to get the fuzzy based results. Security based FIS is based on the three inputs Confidentiality, Availability, Back and Recovery and twenty seven rule base.

The FIS module at third phase takes the output of last four modules as input and gives the final output based on the sixteen rule base. The output is specific to very poor, poor, good, excellent or outstanding. All FIS modules are implemented with the help of Simulink to generate the degree of trust corresponding to each CSP.

Table 2. Simulation results

CSP	Response Time [ms]	DC Processing Time [ms]	Total V.M. Cost [$]	Total Data Transfer Cost [$]
A	50.14	0.43	120.01	131.43
B	50.17	0.44	21.60	105.28
C	215.51	0.15	9.00	162.18
D	529.54	0.20	96.01	42.11
E	144.79	0.38	240.02	74.28
F	50.13	0.43	108.01	105.14
G	50.15	0.44	126.01	216.68
H	50.17	0.44	43.20	90.79
I	113.27	0.51	75.91	57.77
J	50.13	0.43	99.91	122.26

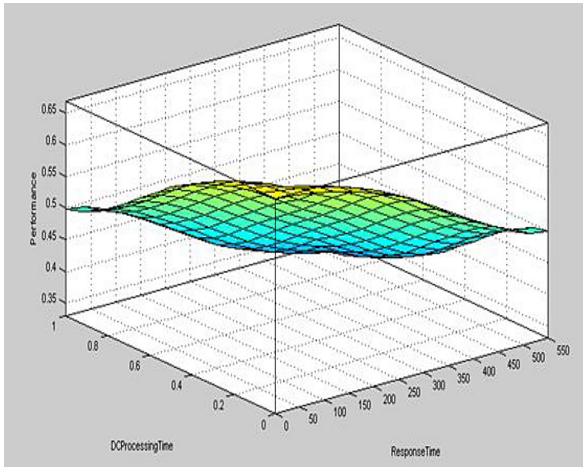

Fig. 3. Surface Value of Performance Module

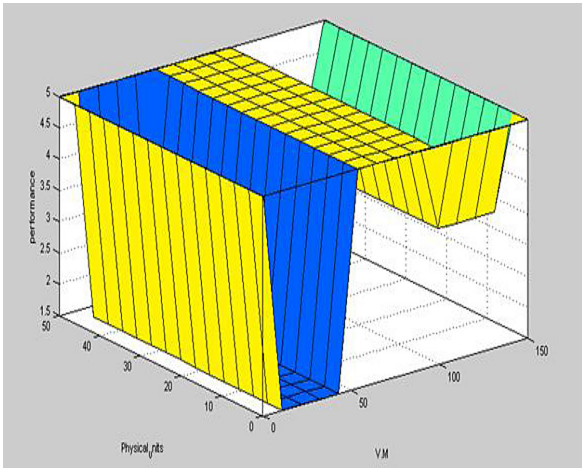

Fig. 5. Surface Values of Adaptability Module

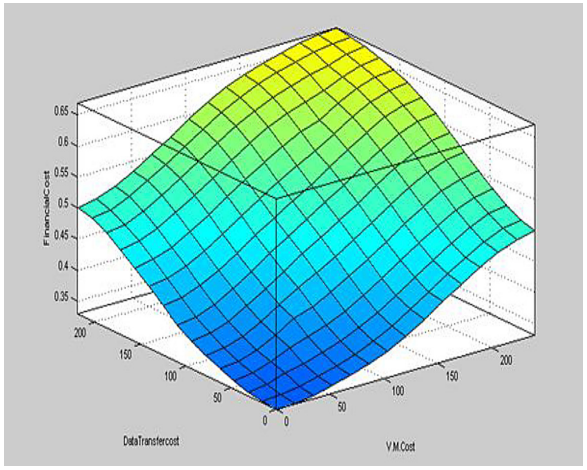

Fig. 4. Surface Value of Financial Cost Module

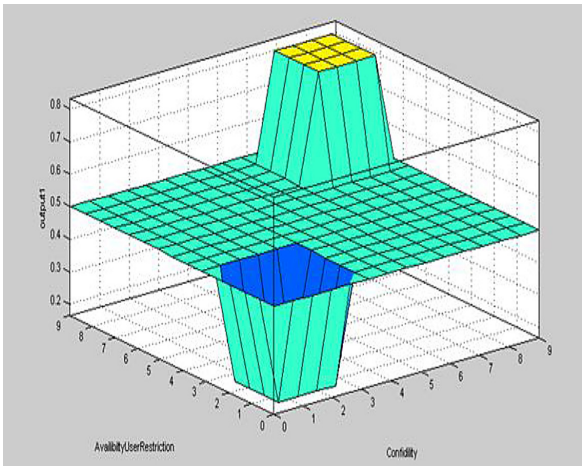

Fig. 6. Surface Values of Security Module

Here, every module has equal weight and on the basis of their values final FIS gives the trust values for each of CSP used for implementation. Figure 3 is describing the surface values of Performance Module as per its basic parameters and defined rules, same as Figures (4-6) are depicting their surface values for the module Financial, Adaptability and Security respectively. Figure 7 presents the Surface Values for the

Table 3. Degree of Trust for each CSP

CSP	Cost	Adaptability	Performance	Security	Trust
A	0.525	0.5	0.619	0.634	Good
B	0.391	0.3	0.617	0.29	Good
C	0.456	0.313	0.616	0.85	Good
D	0.394	0.25	0.471	0.6	Good
E	0.566	0.83	0.592	0.82	Best
F	0.482	0.65	0.619	0.324	Good
G	0.616	0.47	0.617	0.654	Good
H	0.394	0.38	0.617	0.345	Good
I	0.394	0.28	0.578	0.1	Poor
J	0.493	0.6	0.619	0.245	Good

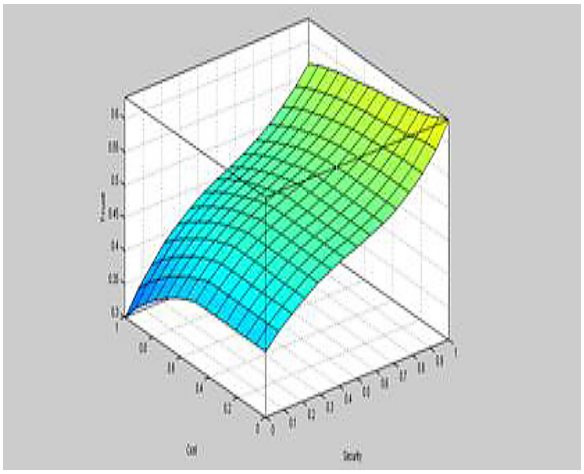

Fig. 7. Surface Values of Trust Generating FIS

Trust generating FIS after the implementation of Rule Base. This Surface figure shows the variant values with the two factors: security and cost out of four modules. This figure depicts that as the security increase and cost decrease in these modules its Trust value goes improved. Table 3 highlights the trust rating generated for CSP E is

better as compared to other CSPs. Although CSP E has more cost as compared to few other CSPs, but other factors are also contributing to improving its trust value.

CONCLUSIONS

Determining the trustworthiness of cloud service provider is of prime concern in growing confidence among customers for rapid adoption of cloud computing. An effort has been made in this research work to formalize a fuzzy based trust management system for assigning a trust value to service providers, considering their existing infrastructure and past reputation. Adequate simulation of proposed system has been carried out using CloudAnalyst and MATLAB to show that the system can be easily adopted in cloud environment.

REFERENCES

1. Buyya R., Yeo C., Venugopal S., Broberg J., Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25 (6), 2009, 599–616.
2. Manuel P. A trust model of cloud computing based on Quality of Service, Annals of Operation Research, 233 (1), 2015, 281–292.
3. Krautheim F., Phatak D., Sherman A. Introducing the Trusted Virtual Environment Module: A new Mechanism for Rooting Trust in Cloud Computing, Trust and Trustworthy Computing, Springer, LNCS, 6101, 2010, 211–227.
4. Pawar P., Rajarajan M., Nair S., Zisman A. Trust Model for Optimized Cloud Services, Trust Management VI, Springer, 374, 2012, 97–112.
5. Kim H., Lee H., Kim W., Kim Y. A Trust Evaluation Model for QoS Guarantee in Cloud Systems, 3 (1), 2010, 1–10.
6. Noor T., Sheng Q. Trust Management of Services in Cloud Environments: Obstacles and Solutions, ACM Computing Surveys, 46 (1), 2013, 1–35.
7. Shaikh R., Sasikumar M. Trust Model for Measuring Security Strength of Cloud computing Service, International Conference on Advanced Computing Technologies and Applications, Elsevier, Procedia Computer Science, 45, 2015, 380–389.
8. Kanwal A., Masood R., Shibi M. Evaluation and Establishment of Trust in Cloud Federation, ACM International Conference on Ubiquitous Information Management and Communication, 2014, 1–8.
9. Sidhu J., Singh S. Compliance Based Trustworthiness calculation mechanism in Cloud Environment, International Workshop on Intelligent Techniques in Distributed Systems Elsevier, Procedia Computer Science 37, 2014, 439–446.
10. Mohsenzadeh A., Motameni H. A Trust Model Between Cloud Entities Using Fuzzy Mathematics, Journal of Intelligent And Fuzzy Systems, 29 (5), 2015, 1795–1803.
11. Gu L., Zhong J., Wang C., Ni Z., Zhang Y. Trust Model in Cloud Computing Environment Based on Fuzzy Theory, International Journal of Computers, Communication & Control, 9 (5), 2014, 570–583.
12. Li W., Ping L. Trust Model To Enhance Security and Interoperability of Cloud Environment, Cloud Computing, Springer LNCS, 5931, 2009, 69–79.