ISSN: 0976-3104
SPECIAL ISSUE (SCMDSA)
Mohan et al.

ARTICLE OPEN ACCESS

F-TEM: A FUZZY BASED TRUST EVALUATION MODEL FOR HEALTHCARE APPLICATIONS IN CLOUD

K Mohan[1*], M Aramudhan[2], Sasikala Ramasamy[3], Swarnalatha P[3]
[1,] *Department of Computer Science and Engineering, Sathyabama University, Chennai, INDIA*
[2]*PKIET, Karaikal, INDIA*
[3]*School of Computer Science and Engineering, VIT University, Vellore, INDIA*

ABSTRACT

Healthcare organizations are beginning to move cloud services in recent years to enhance services and quality without spending much investment for IT infrastructure. Medical records are very sensitive and private to any individuals. Hence, Trust in the relationship among Cloud Service Providers (CSP) and Cloud Service Users (CSU) is very important prerequisite before any service interaction. Hence effective mechanisms are required to identify trustworthy CSP. It is very difficult to evaluate trust level in an open and dynamic environment like cloud. In this paper we have proposed F-TEM: A Fuzzy based Trust Evaluation Model, which filters suitable CSP for any CSU based on their input parameters. Experiments were conducted with several parameters like security, capability and behavior of CSP and the results were compared with conventional method.

Received on: 30th-Nov-2015
Revised on: 22nd-March -2016
Accepted on: 13th– April-2016
Published on: 10th –June-2016

KEY WORDS

Fuzzy; trust; cloud computing; healthcare system

***Corresponding author: Email:** meetmohan.k@gmail.com

INTRODUCTION

In the past few years, Health care is moving to digital and particularly Cloud services are becoming patient focused and data driven. By using cloud computing facility, medical data sharing among doctors and patients, accessing and storage becomes easier. Responsibilities of health care service providers and choosing the best service provider by the user becomes the important part of digital health care systems [1,2].

Health Care System

Healthcare and the quality of Health care service are playing significant roles in any country. The responsibilities of Health care include prevention of disease, diagnosis, treatment, report preparation and analysis. Accessing Health care by common people across countries varies by economic conditions of individuals [3]. Technologies can create major impact in health care includes Robotic surgery, Health care web service, Decision support system. As like above technologies, Cloud computing is also emerging technology, which can create major impact on health care. In future, Cloud Computing will play major role in modernizing Health care service. The proposed system integrates the decision making system, Health care web services and cloud computing to make health care service more authoritative.

Health Care Service Providers Responsibilities

Healthcare providers are expected to provide a quality improved patient care with limiting cost. Cloud Computing service model is to enable convenient, on -demand software as a service (SaaS) and Storage as a Service to Hospitals and patients through Health Care Cloud Service Providers. Cloud Computing Service model rapidly reduce Management efforts and services. Cloud Computing services initiated in Health care have the following features:

THE IIOAB JOURNAL ISSN: 0976-3104

- Elastically increase the infrastructure such as servers and storage
- Moving huge data such as radiology images, clinical data from Health care IT department to Cloud reduces troublesome task
- Software and Patient record are on demand and 24 x 7
- Maintenance risks are substantially reduced
- Single point of failure is totally avoided
- Web based easy access to Patients and Doctors
- Improves the skill to analyze and track patient information
- Provides facility to sharing lifesaving information quickly among doctors in various geographical areas during emergency and reduces the need for duplicate testing

Hence health care cloud service providers provide preventive, curative health care services through storage, service request, report generation and Analysis during emergency and for out-patients (OP). However, during the integration of Cloud service to Health care service providers, two properties need to be considered: Expectations of users from Service providers and Trust value of Cloud Service Providers [4]. Hence, Qualifying criteria need to be chosen carefully to choose appropriate cloud service providers.

Qualifying Health Care Service Providers

Hospitals and patients wanted to use service providers have all authority to choose the best providers. Hence, CSPs are responsible to get trust certificates from some centralized authority called Trust Managers. The role of Trust Manager is to match the expectations of users and trust value of CSPs.

Expectation of Users from Cloud Service Providers

Users or Doctors use cloud services 24 x 7 to access patient health records, medicine details and Doctors can access other doctor's assistance through these services. Hence users expect from cloud service providers that the service should be available 24 x 7, the records need to be available where ever they go, their records should be maintained securely and hence privacy of patients health records is playing significant role. It is the responsibility of cloud service users to choose cloud service provider with high reputation value. It provides the facility to the patients to utilize their database when they move from one Health Service Organization to another.

Trust Value of Cloud Service Providers

Trust value of cloud service provider is calculated based on the parameters considering Security, Capability and Behaviour of Cloud Service Providers. The criteria Security, Capability and Behaviour are chosen from the user's feedback, which we have taken manually by giving the forms to various hospitals and patients who are all interested to go for external service and for keeping their records in cloud. The parameters are assigned with weightage value to differentiate the significance of each parameter.

Security: The service provider has to maintain the privacy of patient's record, be accessed only by the authorized patient and doctors and data should be recovered immediately in case of failure. Hence, the attribute security is highly deciding parameter for health service cases. Therefore, 50% of weightage is assigned to security parameter alone.

Capability: Health care service is a basic responsibility of any Government to treat the world population without considering their financial background. Web services and cloud services makes the total system simple, economic and easy accessible. To provide cloud service to every patient, who need service from anywhere, the capacity is the next important factor of CSP. To make the system highly elasticity, the high capacity server, storage and RAM are vital factors. Server and Storage makes the system to store more patient data. The RAM capacity makes the system quick access.

THE IIOAB JOURNAL
ISSN: 0976-3104

Behaviour: Service level agreement advises the possibilities of services the provider can offer to users. Hence, the cloud service users need to decide the level of CSP based on their SLAs. Also the user has to obtain the feedback from other cloud users to choose the best service provider. Hence, every cloud users have to register their feedback in particular time interval about CSPs. The Trust value calculation is based on Fuzzy logic for cloud service providers. The proposed system uses Fuzzy based model which takes input from the user's feedback and SLAs of individual CSPs and the model gives the Trust rating as output. The fuzzy model chosen is Mamdani FIS, Mamdani FIS and Defuzzifier generates the output as a crisp value. The implementation consists of two stages: Fuzzy based calculation for Trust expectations of users and Fuzzy based weightage calculation of CSPs based on three criteria Security, Capability and Behaviour.

The rest of the paper is organized as follows. Section 2 presents the related works to cloud based health care service in the literature. Section 3 describes Fuzzy based trust evaluation model (F-TEM) used in this paper; In Section 4 the results achieved in this work are discussed. Finally Section 5 is conclusion and future enhancements to be carried out. The list of references to build the work is furnished at the end.

RELATED WORK

There is no comprehensive trust mechanism existing among leading cloud service providers like Amazon, Google and Microsoft. So cloud service users are really struggling to identify suitable service providers. [5] proposed Feedback rating based reputation to evaluate trust. Feedback collector module is developed for collecting feedback from users about cloud service provider. But, more detailed classification of context is missing in this paper. [6] proposed credibility based trust model which evaluated the credibility of trust feedbacks given by cloud service users also this model identifies malicious trust feedback from hackers. [7] proposed SLA based trust model to help cloud service users to identify trustworthy cloud service providers based on their SLA agreement. However some important parameters outside SLA agreement cannot be monitored and evaluated which reduces the overall effectiveness. [8,9] proposed user behavior based trust evaluation. The author divided the user behavior into four categories and under each category users behavior is monitored and evidences are maintained. Based on some formula the level of deviation with normal behavior is computed and trust decision is made. [10] proposed game theory based trust model which helps cloud user applications to map appropriate service providers. However this model failed to answer uncertain nature of applications and resources. The proposed game theoretic based approach for trust evaluation model can be applied only for the first time user and provider; it could not be used for evaluation of HSP with continuous evaluation model. [11] proposed trust based mechanisms for the integration of cloud and sensor network, but the technique considers few attacks on trust such as good mouthing, bad muting, collusion and white washing. Fuzzy inference system is used for trust evaluation in [12-16], but dynamically changing behavior is not considered by those authors.

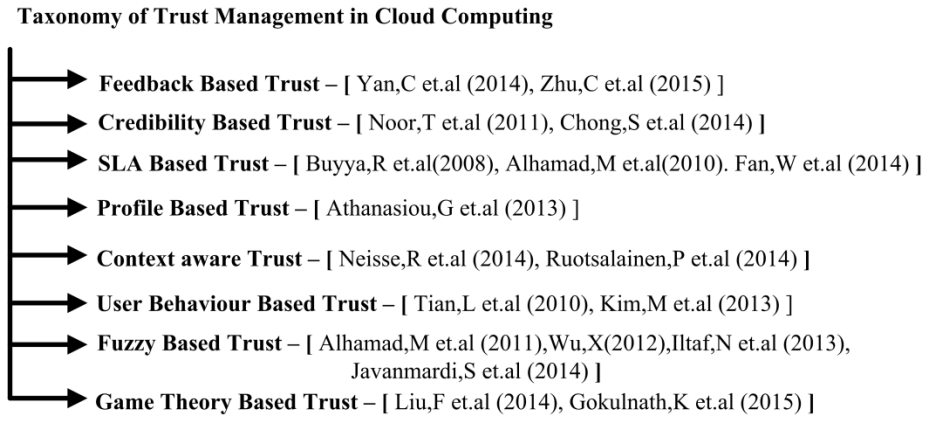

Fig: 1. Taxonomy of Trust Management in Cloud Computing

[17] developed a hierarchical fuzzy inference system for service selection process. In hierarchical inference system output of low level are given to input of high level models. It helps the system to compute partial solutions. The proposed system uses min-max structure of Mamdani model to forward output of one level to other level in same category. [18] used fuzzy comprehensive evaluation method to validate trust evaluation

THE IIOAB JOURNAL
ISSN: 0976-3104

value is close to trust level or not. The model works well only the granularity of trusted value is great. The fuzzy comprehensive evaluation model is a decision making method. And the developed model is not applied on any real time experiments. But Fuzzy inference system is proposed method is the process of formulating the mapping process from input values to the output using fuzzy rules.

PROPOSED FUZZY BASED TRUST EVALUATION MODEL

Figure- 2 illustrates the general overview of our proposed system. There are three major level of input steps involved in the usage of F-TEM Engine: The first step, Users requirements submission to F-TEM Engine, Second, Service Catalogues and SLA Submission by Service providers and finally dynamic feedback collection from Users.

F-TEM overview

A software framework of F-TEM consists of three functional units: F-TEM Engine, Cloud based HSP Layer and HSU layer. The CSU and CSPs are mentioned as HSU and HSP layers. The F-TEM makes final decisions based on the inputs such as Cloud user's feedback, SLA and Service catalogue. It provides its resultant decisions to HSU layer as Service advertisements. The F-TEM is responsible to check the identity of Cloud users and Cloud service provider users from Identity Provider (IdP). The F-TEM engine contacts Knowledge base to retrieve and store details of HSU layer feedbacks, Service catalogue and SLA of individual Cloud service providers. The Knowledge Base is a storage engine to store complex unstructured information used by the F-TEM Engine. It is a centralized repository for information: details of HSU and HSP layer. This knowledge base assists the F-TEM to analyse and take decisions on Trust requirements of Cloud users. The trust decisions about Cloud providers will also be stored by Knowledge base for later retrieval.

The HSU layer is a set of cloud users who need health care services through online during emergency and for report generation. Initially, The HSU layer communicate its requirements to F-TEM Engine. The HSU layer expectation is to identify a quality service provider based on its requirements. The service advertisements from F-TEM help out users to identify a competent provider who matches the requirement of cloud users. After identifying the Cloud service provider, HSU layer directly interact with the service provider for all its Health care issues and decisions.

The Cloud Based HSP layer is a set of cloud providers who have different SLAs, models, performance rates in terms of security, capability and behaviour. It provides its service catalogues and capability list through SLA. The Cloud providers are assigned with trust value by the F-TEM. The trust values are assisting the users to choose its provider. The proposed work focuses only the F-TEM Engine Role.

F-TEM Architecture

The components of F-TEM as shown in **Figure- 3** are Input Layer, Fuzzifier, F-TEM Inference Engine, Knowledge Base, COG defuzzifier and Trust Result. The Input layer considers three parameters: Security, Capability and Behaviour. For example, the input values of attributes namely authentication, access control, Data security and Data recovery of Security are given as in terms of Low, Medium and High to Fuzzifier.

The steps of Fuzzy Inference Engine are : Compare the input variables with the membership function to obtain the membership values. This is done by Fuzzifier. Fuzzy Inference Engine generate the qualified resultant value either crisp value or fuzzy based. Aggregate the resultant value to produce a crisp output. This step is done by defuzzifier. A rule base containing number of IF-THEN rules and Database jointly called as knowledge base.

THE IIOAB JOURNAL
ISSN: 0976-3104

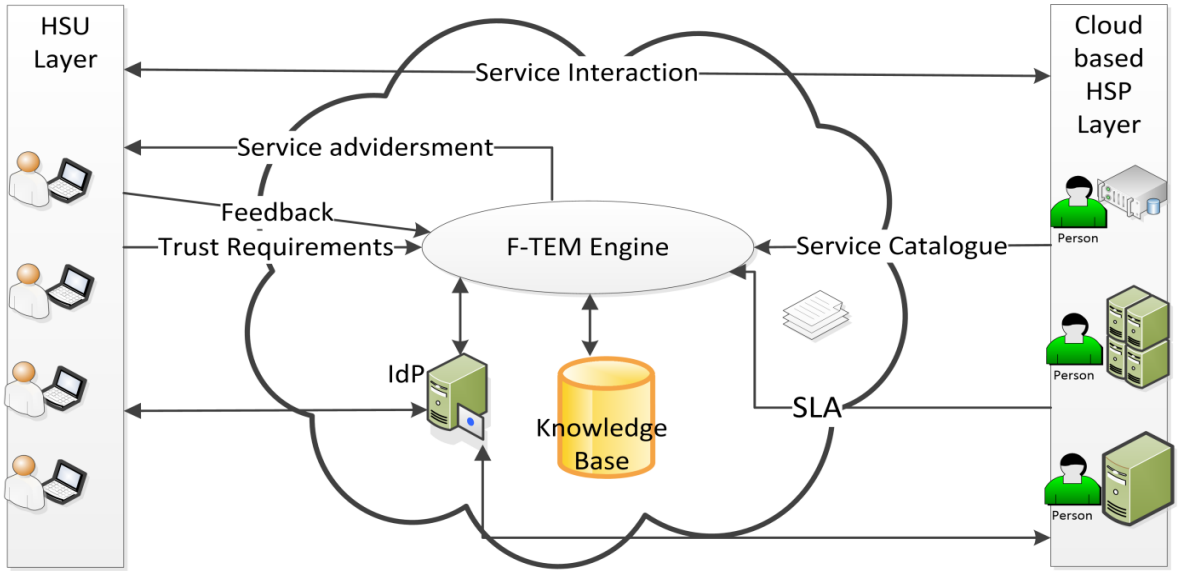

Fig: 2. F-TEM Overview in Cloud Environment

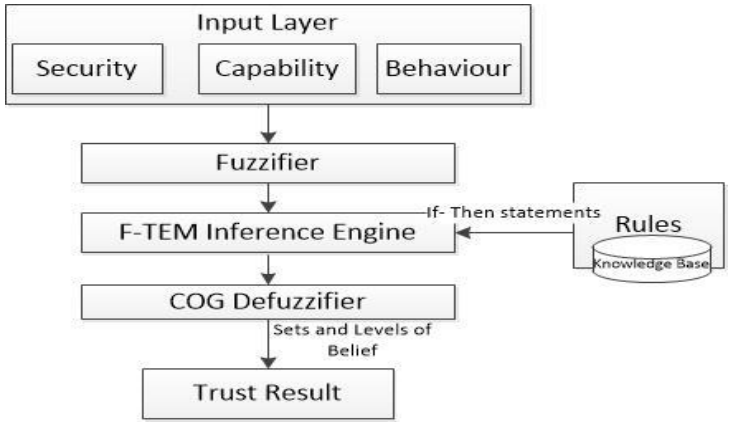

Fig: 3. F-TEM Architecture

Fuzzy based Trust Evaluation Model

The evaluation of the trust value for CSP and user expectation for cloud computing users, comprises of two stages: trust value for CSP and Trust Expectation from Users. Fuzzy inference system is classified into direct Fuzzy inference system and Indirect fuzzy inference system. Mamdani and Sugeno-type are direct method and direct methods are easy to implement, but indirect methods are complex in nature. In this paper, the model based on Mamdani is used to calculate trust value dynamically for cloud service provider. Mamdani method and Sugeno methods are widely accepted fuzzy models for capturing expert knowledge. The most fundamental difference between Mamdani-type FIS and Sugeno-type FIS is the way the crisp output is generated from the fuzzy inputs. The Mamdani-type FIS uses the technique of defuzzification of a fuzzy output. Due to the interpretable and intuitive nature of the rule base, Mamdani-type FIS is widely used in particular for decision support application [19]. Also the Mamdani type is most suitable for human input. The purpose to choose mamdani model is it simple min-max structure. The parameters of each category rules are combined with min structure and the categories rules are connected by Max structure. These simple min-max structures of mamdani are easily incorporated into this trust evaluation model to combine the two levels of structure (Parameters and Categories). We classified the health care service providers trust evaluation model

THE IIOAB JOURNAL ISSN: 0976-3104

into two levels, three categories of HSP and each category is further classified into set of parameters. Hence the Mamdani inference system with min-max structure is well suited for Fuzzy based trust evaluation model. The user expectation model has three or four input parameters in each category mapped to one output. The input and parameter has three member functions: low, medium, high and output parameter has four membership functions: very low, low, medium and high. [20] claimed that "Fuzzy logic is a logic of approximate reasoning whose distinguishing features are (i) fuzzy truth-values expressed by linguistic terms, (ii) imprecise truth-tables..." Didier Dubois, Toulouse (France) and with Stefan Lehmke, Dortmund stated as

Fuzzy logic = many value logic+ partial belief.

I.e. extend the weighted formula in possibilitic logic and many valued logic conjointly [paper] into a genuine fuzzy logic. This paper uses the weighted parameters as multi value logic with rules of possibilitic logic made the final model as fuzzy based trust evaluation model.

Trust Expectations of Users

Trust based Health Care system is developed using Mamdani-Type Fuzzy Inference Systems model. CSP trust value has three categories: Security, Behaviour and Capability. The Category 1 consists of four attributes as inputs from user feedback on the subject of authentication, authorization, data security level and data recovery level. The system has one output for the category 1 that decides Trust value for the CSP on the subject of Security. The same is repeated for Capability and Behaviors as shown in **Table- 1**. We have collected user feedback from Health centre to fix the weightage of Categories and we have given options to users to choose parameters under categories as given in section 1.3.2. The collected feedback has been given as data to train the system. The authentication, authorization, data security and data recovery are taken to be in range of low, medium, high based on SLAs issued by CSPs and feedback from users. The fuzzification (fuzzifier) process converts crisp inputs to non-crisp (fuzzy) outputs. The Trust value range for Authentication is fixed based on user requirement as shown in **Table- 2**. For example, if user requirement for authentication is Login & Password based, then trust value range is low, medium for One Time Password (OTP) and high for biometric authentication. The Attributes of three categories and its Scenario and Range are stated in **Table- 2**.

Table: 1. Parameter's Weightage and Attributes

Parameters & Weightage	Attributes
Security - 50%	Authentication
	Authorization
	Data Security Level
	Data Recovery Level
Capability - 20 %	Server Capacity
	Storage Capacity
	RAM Capacity
Behaviors - 30 %	User Feedback
	SLA accomplishment
	Availability

THE IIOAB JOURNAL
ISSN: 0976-3104

Table: 2. Range of Attributes

Attributes	Range	Scenario	Attributes	Range	Scenario
Authentication	Low (1)	Password based	Storage Capacity	Low (1)	Limited with <= 1 GB
	Medium (2)	OTP based		Medium (2)	Limited up to 1 TB
	High (3)	Biometric based		High (3)	Unlimited
Authorization	Low (1)	Role based	RAM Capacity	Low (1)	<=2GB
	Medium (2)	Attribute based		Medium (2)	2 GB to 8 GB
	High (3)	Semantic based		High (3)	More than 8 GB
Data Security Level	Low (1)	http	User Feed back	Low (1)	Less aggregate Feedback value
	Medium (2)	https		Medium (2)	Avg. aggregate feedback
	High (3)	https with high key value		High (3)	Good aggregate Feedback
Data Recovery Level	Low (1)	No recovery	SLA Accomplishment	Low (1)	Not at all Accomplished
	Medium (2)	Partial recovery		Medium (2)	Partially Accomplished
	High (3)	Complete recovery		High (3)	Completely Accomplished
Server Capacity	Low (1)	Non-replicated	Availability	Low (1)	50% to 69%
	Medium (2)	Replicated-min		Medium (2)	70 % to 89%
	High (3)	Replicated-max		High (3)	90% and above

The following is a simple calculation which takes input as attributes of security as mentioned in **Table- 2**, and the rule is framed to find the output for Security. The output ranges are very low, low, medium and high. The sample rules for the security are described in **Table- 3**.

Rule to calculate output of Security

We have collected expert's feedback from cloud users, software industry and Health care professionals for setting the rules to calculate the output for Security, Capability and Behaviors. For example security can be fixed as high only if total is higher than 9, i.e. if one parameter may be low but other parameters should be high to pass security category as output the result – high. The same rules we fixed for behavior and capability.

Total =Authentication + Authorization + Data Security + Data Recovery

if total>=4 and total <=5

security = very low

else if (total >= 6 and total<=7)

security = low

else if(total>=8 and total <=9)

security = medium

else

security = high

THE IIOAB JOURNAL
ISSN: 0976-3104

Table: 3. Sample Rule Base of Mamdani FIS for the Parameter - Security

Authentication	Authorization	Data Security	Data Recovery	Security
Low(1)	Low(1)	Low(1)	Low(1)	Very Low
Low(1)	Low(1)	Low(1)	Medium(2)	Very Low
Low(1)	Low(1)	Low(1)	High(3)	Low
Low(1)	Medium(2)	High(3)	High(3)	Medium
Low(1)	High(3)	High(3)	Low(1)	Medium
Low(1)	High(3)	High(3)	Medium(2)	Medium
Low(1)	High(3)	High(3)	High(3)	High
Medium(2)	Low(1)	Low(1)	Low(1)	Very Low
Medium(2)	Low(1)	Low(1)	Medium(2)	Low
Medium(2)	High(3)	Medium(2)	High(3)	High
Medium(2)	High(3)	High(3)	Low(1)	Medium
Medium(2)	High(3)	High(3)	Medium(2)	High
Medium(2)	High(3)	High(3)	High(3)	High
High(3)	Low(1)	Low(1)	Low(1)	Low
High(3)	Low(1)	Low(1)	Medium(2)	Low
High(3)	Low(1)	Low(1)	High(3)	Medium
High(3)	High(3)	Medium(2)	Low(1)	Medium
High(3)	High(3)	High(3)	Medium(2)	High
High(3)	High(3)	High(3)	High(3)	High

The following is a simple calculation which takes input as attributes of Behavior and Capability and the rule is framed to find the output for Behavior and Capability.

Rules to calculate output of Behavior

total = user feedback +SLA accomplishment + availability

if total<=4

behavior = very low

else if (total == 5)

behavior = low

else if(total>=6 and total <=7)

behavior = medium

else

behavior = high

Rules to calculate output of capability

total =server capacity + storage capacity + RAM capacity

if total<=4

capability = very low

else if (total == 5)

capability = low

else if(total>=6 and total <=7)

capability = medium

else

capability = high

Triangular Membership Functions

The rules included for the Trust based Health Care system for Category Security are described in **Table- 3** and other rules are not explicitly mentioned in the paper. For the calculation of Trust value of CSP using Mamdani model, the inputs are taken from security as shown in **Figure- 4**, Capability as shown in **Figure- 5** and Behavior as shown in **Figure- 6** and produces output as shown in **Figure- 7** that decides the trust value of each CSP. The output membership functions are very low, low, medium and high.

THE IIOAB JOURNAL
ISSN: 0976-3104

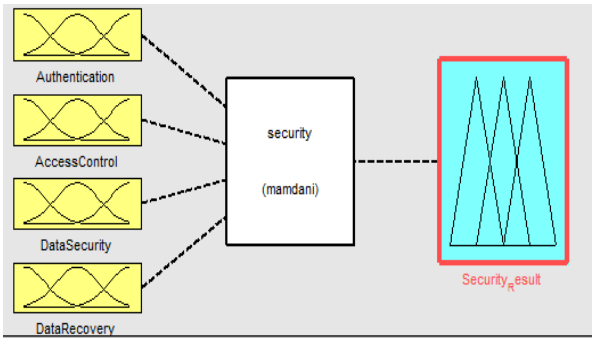

Fig: 4. Security Membership Function

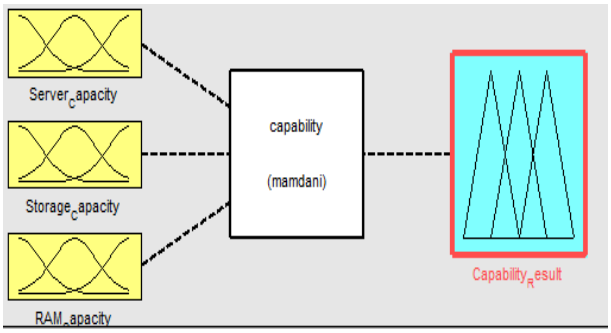

Fig: 5. Capability Membership Function

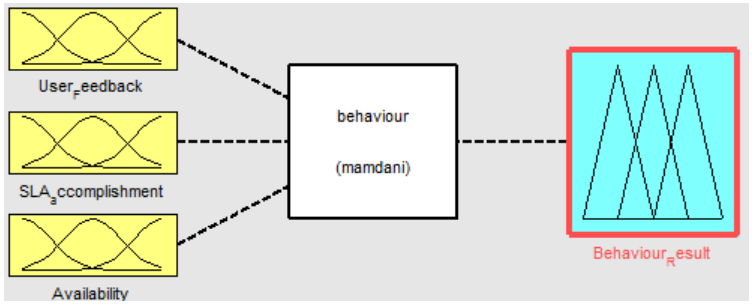

Fig: 6. Behavior Membership Function

The outputs of Security, Behavior and Capability membership functions are given as input to the Membership ship for trust expectation of users. The crisp value for output of parameters is assigned as shown in **Table- 4**.

Table: 4. Membership Function of Parameters - Security, Behavior and Capability

Parameter Output	Constant Value
Very low	0.25
Low	0.50
Medium	0.75
High	1.00

The inputs for the calculation of resultant membership function as constant value x weightage/100. For example, if the output of security parameter is high, 1 x 50/100 = 0.5 is given as crisp input for the resultant membership function. The sample outputs of Triangular membership function for Trust value of CSP are as shown in **Table- 5**. The crisp value generated from F-TEM is given as Trust value of CSP in percentage to the CSUs. The CSUs can choose their service provider according to their expectations.

Table: 5. Sample Trust Values of CSP

Security	Behavior	Capability	F-TEM Output	Constant Value in %
Very low	Very low	Very low	Very low	25
High	Medium	Medium	Medium	75

THE IIOAB JOURNAL
ISSN: 0976-3104

Medium	low	low	low	50
Very low	Very low	low	Very low	25

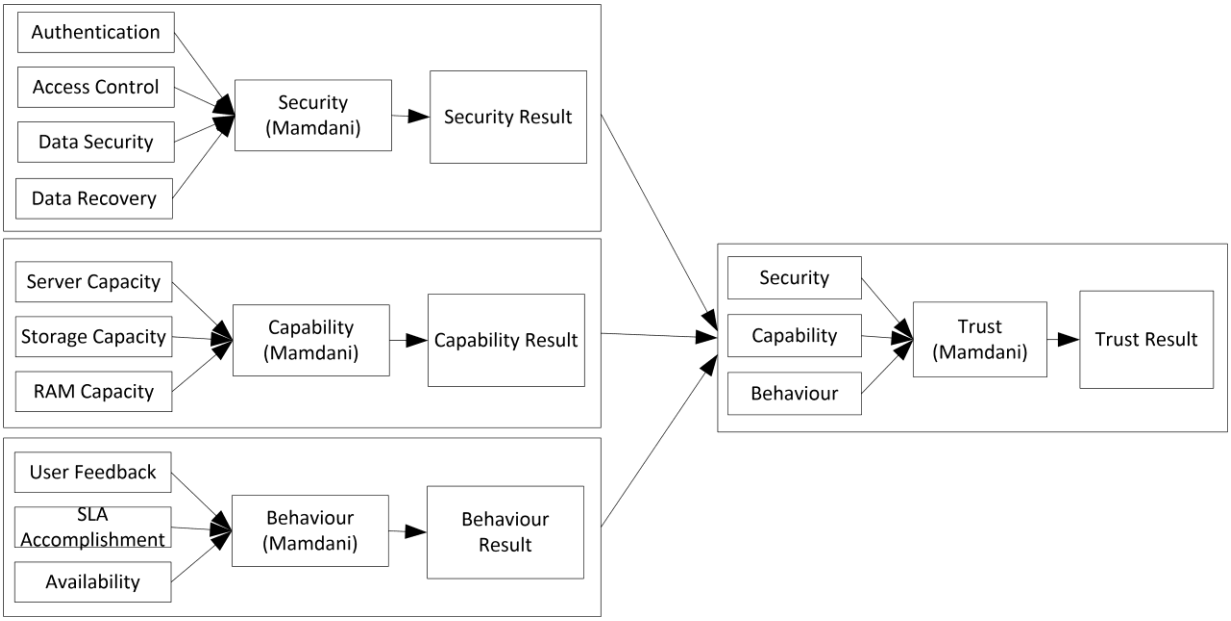

Fig: 7. Membership Function for Trust value of CSP

RESULTS AND DISCUSSION

This section shows our proposed method results to verify the cloud based trust calculation. The proposed model is provided with the results of the experiment using Matlab. The Matlab toolbox for fuzzy logic is used to implement our methodology. This toolbox has ready functions and calculation for fuzzy inference systems Mamdani and Sugeno fuzzy inference system. We have used Mamdani model inference system for calculating Trust value for parameters Security, Behaviors and Capability and final Trust value of CSP. We have collected real time datasets from maximum of 100 different users from Health Centers and trained the system. The service catalogue details from 10 to 20 CSPs and the feedback from users on the subject of CSPs are fixed randomly. The output of membership function is calculated as shown in **Figure- 7.** Number of CSUs and CSPs in total varies from 13 to 110 and time taken by the F-TEM is calculated. The following results show that time taken by the F-TEM to calculate trust value will not be much varied by number of CSUs and CSPs. Hence it is proved that F-TEM is not creating any time complexity overhead in choosing the right CSP by using fuzzy logic inference system.

Table :6 .Time Taken by the F-TEM

Sl.No	No. of CSU and CSP	Time in ms
1	13	5.0
2	23	5.2
3	36	6.3
4	46	6.6
5	58	7.1
6	68	7.2
7	110	8.0

THE IIOAB JOURNAL
ISSN: 0976-3104

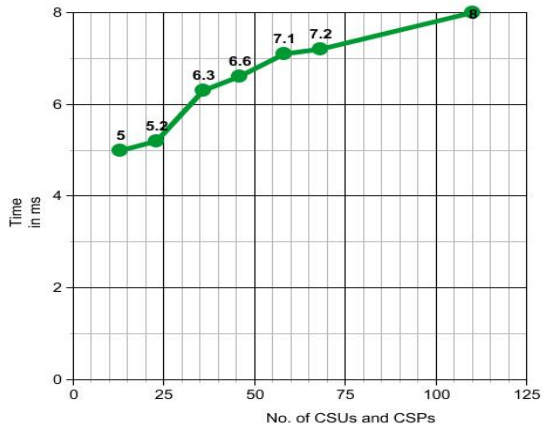

Fig: 8. Time Taken by the F-TEM

We have implemented the proposed method on fuzzy logic in three methods: user feedback based (without Fuzzy), Fuzzy logic, Fuzzy with dynamic feedback and the results are compared with traditional method in **Figure- 9.** In traditional method (feedback), we have taken average of the values of parameters. The second results are feedback with Fuzzy logic and third results are one the subject of fuzzy logic with dynamic feedbacks from CSUs who uses CSPs. The dynamic feedback on the subject of CSPs added greater strength to choose right CSP. The category Behavior is fixed based on user's feedback on SLA accomplishments, feedback percentage and availability during access. The trust value results are taken from F-TEM with and without dynamic user feedback. The results shows that the fuzzy logic and fuzzy logic with user's feedback creates greater impact than traditional method.

Table: 7. Comparison of F-TEM with Traditional Model

Techniques	CSU and CSP - % of match
Feedback based	50%
Fuzzy logic Methods(without dynamic Feedback)	80%
F-TEM model with dynamic user feedback	87.5%

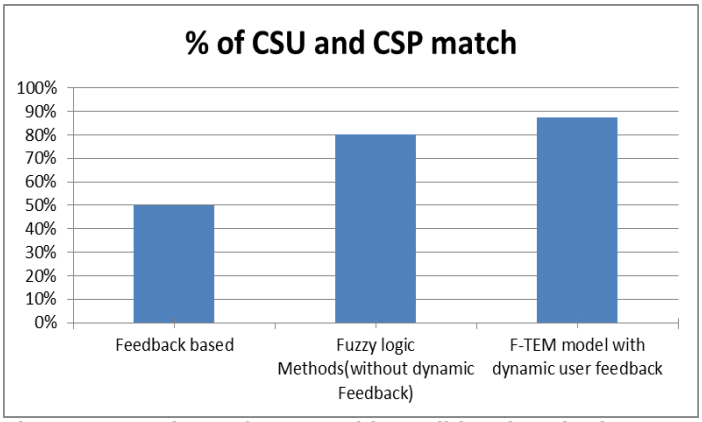

Fig: 9. Comparison of F-TEM with Traditional Method

THE IIOAB JOURNAL
ISSN: 0976-3104

CONCLUSION

In this paper, a trust evaluation scheme based on fuzzy logic inference system for Health care service is described. The proposed system evaluates the trustworthiness of cloud service providers. We have collected user feedback from Health centre to fix weightage of Categories and we have given options to users to choose parameters under categories. The collected feedback has been given as data to train the system. The results show that time complexity is not the major concern when we calculate trust value with F-TEM. Hence it is proved that F-TEM is not creating any time complexity overhead in choosing the right CSP by using fuzzy logic inference system. This F-TEM method experiments on Matlab show that the dynamic feedback from the users, assigning proper weightage(Security 50%, Behavior 30% and Capability 20%) and Fuzzy logic inference system assist cloud service users to choose right CSPs. The work can be extended as F-TEM product or web service, which is used to choose any service providers such as Internet service providers, cloud service providers based on dynamic user's feedback.

FINANCIAL DISCLOSURE

No financial support was received to carry out this project.

ACKNOWLEDGEMENT

None

CONFLICT OF INTERESTS

Authors declare no conflict of interest.

REFERENCES

[1] Bamiah MA, Brohi SN, Chuprat S, Manan JA,[2014] TRUSTED CLOUD COMPUTING. *J Comput Sci*,10(2):240–250.

[2] Buyya R, Yeo CS, Venugopal S.,[2008] Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. 2008 10th IEEE IntConf High Perform ComputCommun .*IEEE*,5–13.

[3] Wul R, Ahnl G.[2012] Secure Sharing of Electronic Health Records in Clouds. 8th International Conference on Collaborative Computing: Networking, Applications and Worksharing, Collaboratecom 2012 Pittsburgh, PA, United States, 711–718.

[4] Buyya R, Ranjan R, Calheiros RN. [2009]. Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities. *Proceedings of the 7th High Performance Computing and Simulation Conference*, Germany. Leipzig, Germany,1-11

[5] Yan C, Qi L, Ni J.[2014] Building Feedback Rating-based Reputation System for Trusted Delivery of Cloud Services. Proc 2014 IntConf Mechatronics, Electron Ind Control Eng. Paris, France: *Atlantis Press*;(Meic):684–687.

[6] Noor TH, Sheng QZ.,[2011] Credibility-Based Trust Management for Services in Cloud Environments. ICSOC 2011, LNCS 7084, *Springer-Verlag Berlin Heidelb*,328–343.

[7] Alhamad M, Dillon T, Chang E.,[2010] SLA-Based Trust Model for Cloud Computing. 2010 13th IntConf Network-Based InfSyst .*Ieee*, 321–324.

[8] Tian L, Lin C, Ni Y, [2010] Evaluation of user behaviour trust in cloud computing. *ComputApplSyst*. 2010;(Iccasm 2010):567–572.

[9] Kim M, Park SO.[2013] Trust management on user behavioral patterns for a mobile cloud computing. *Cluster Comput*, 16(4):725–731.

[10] Gokulnath K, Uthariaraj R.,[2015] Game Theory Based Trust Model for Cloud Environment. *Sci World J*.2015(2015):1–10.

[11] Zhu C, Member S, Nicanfar H, Leung VCM, Yang LT.[2015] An Authenticated Trust and Reputation Calculation and Management System for Cloud and. *IEEE Trans Inf FORENSICS Secur*. 2015,10(1):118–131.

[12] Xu Wu., [2012] A Fuzzy Reputation-based Trust Management Scheme for Cloud Computing. *Int J Digit Content Technol its Appl* .2012 Sep 30, 6(17):437–445.

[13] Alhamad M, Dillon T, Chang E. [2011] A Trust-Evaluation Metric for Cloud applications. *Int J Mach Learn Comput* .2011; 1(4):416–421.

[14] Iltaf N, Ghafoor a.,[2013] A fuzzy based credibility evaluation of recommended trust in pervasive computing environment. 2013 *IEEE 10th ConsumCommunNetwConf.Ieee*, 617–620.

[15] Javanmardi S. FR trust, [2014] a fuzzy reputation–based model for trust management in semantic P2P grids. *J Grid*,6(1):57-66

[16] Lin G, Lin C, Chou C, Lee Y. [2014] Fuzzy Modeling for Information Security Management Issues in Cloud Computing. *Int J Fuzzy* 16(4):529–540.

[17] Qu C, Buyya R.,[2014] A Cloud Trust Evaluation System Using Hierarchical Fuzzy Inference System for Service Selection. 2014 IEEE 28th IntConfAdvInfNetwAppl.,850–7.

[18] Zhou Z, Luo Y, Guo L, Sun L.[2013] Assessment of P2P Trust Model Based on Fuzzy Comprehensive Evaluation. *J Softw* 2013 Nov,8(11):2711–2714.

[19] Arshdeep Kaur, Amrit Kaur,[2012] Comparison Of Mamdani-type And Sugeno-type Fuzzy Inference Systems For Air Conditioning System. *International Journal Of Soft Computing And Engineering.*, 2(2):323-325.

[20] LA Zadeh,[1975] Fuzzy logic and approximate reasoning. *J Synthese* 3(30):407–428.

THE IIOAB JOURNAL
ISSN: 0976-3104

ABOUT AUTHORS

Mr. K. Mohan *is a research scholar in computer science and engineering department at Sathyabama University. He is also working as an Assistant Professor in School of Computer Science and Engineering at VIT University. His research interest includes cloud security, healthcare system, Internet of Things. He can be reached at meetmohan.k@gmail.com*

Dr. M. Aramudhan *is an Associate Professor in IT department of PKIET, karaikal. His research interest includes cloud security, semantic web, Internet of Things, web mining. He can be reached at aranagai@yahoo.co.in*

Dr. Sasikala Ramasamy *is an Associate Professor in School of Computer Science and Engineering, VIT University. Her research interest includes cloud security, semantic web, Internet of Things, Big data Analytics and social networking. She can be reached at sasikala.ra@vit.ac.in*

Dr. Swarnalatha P *is an Associate Professor in School of Computer Science and Engineering, VIT University. Her research interest includes Image Processing, Artificial Intelligence, Remote Sensing, Software Engineering BigData and Internet of Thing. She can be reached at pswarnalatha@vit.ac.in*