Turing Based Service Level Agreement Assessment Model Over Cloud Deployments

Report submitted for the partial fulfillment of the requirements for the degree of Bachelor of Technology in
Information Technology

Submitted by

Koyena Choudhury – 11700214039

Nayanika Nandy – 11700214045

Srewasi Dutta – 11700215100

Under the Guidance of DR. INDRAJIT PAN

RCC Institute of Information Technology
Canal South Road, Beliaghata, Kolkata – 700 015
[Affiliated to West Bengal University of Technology]

Acknowledgement

We would like to express our sincere gratitude to DR. INDRAJEET PAN of the department of Information Technology, whose role as project guide was invaluable for the project. We are extremely thankful for the keen interest he / she took in advising us, for the books and reference materials provided for the moral support extended to us.

Last but not the least we convey our gratitude to all the teachers for providing us the technical skill that will always remain as our asset and to all non-teaching staff for the gracious hospitality they offered us.

Place: RCCIIT, Kolkata

Date:

……
Koyena Choudhury

……
Nayanika Nandy

……
Srewasi Dutta

Department of Information Technology
RCCIIT, Beliaghata,
Kolkata – 700 015,
West Bengal, India

Approval

This is to certify that the project report entitled "Turing Based Service Level Agreement Assessment Model Over Cloud Deployments" prepared under my supervision by KOYENA CHOWDHURY(11700214039), NAYANIKA NANDY(11700214045), SREWASI DUTTA(11700215100) be accepted in partial fulfillment for the degree of Bachelor of Technology in Information Technology.

It is to be understood that by this approval, the undersigned does not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn thereof, but approves the report only for the purpose for which it has been submitted.

…….. ……

Name & Designation of the HOD — DR. ABHIJIT DAS

Name & Designation of Internal Guide — DR. INDRAJIT PAN

INTRODUCTION

Cloud computing is emerging as an effortless computing tool for multiple needs. It is effortless because of its less financial need and simple configuration challenge.
Cloud service providers (CSP) offer cloud facilities in different modes. They are capable to scale up and scale down the offered quantum of services on the fly. All these service modalities are illustrated in Service Level Agreement (SLA).

Elasticity is one of the basic requirements of cloud services. It is indeed a challenging task to satisfy customers by providing their required service. Often the CSPs need to adapt with dynamic customer demand for cloud resources. This requires dynamic change in Quality of Service (QoS) parameters within cloud SLA. QoS parameters of a cloud service might involve service response time, tenure of service, backup mechanism, disaster management and recovery and many other aspects. Effectively all these are defined within an SLA and a SLA becomes very useful for a CSP to compete with others in terms of their service specifications and quality commitments. Thus a SLA should reflect present trend and demand of the market.

This paper presents a Turing model for verification and assessment of SLA under different cloud deployments. This model will help one customer to compare and assess his needs with the service attributes offered by a CSP and accordingly the customer will be able to make a decision about accepting or rejecting a CSP. In order to facilitate this service attribute validation, first a risk categorization of cloud services has been made to trace out parameters involved with service quality management. In the proposed model, these parameters are arranged in a sequence to perform validation check. A symbol table has been prepared to represent each state of validation. Quality quantification has been done to define an instruction table for setting up the rules for decision making process. Turing models provides fundamental mathematical automation in a decision making process. Turing model is not yet employed in cloud SLA models. Hence this was found to be an excellent prospect for modeling.

The information age has matured to the point where most citizens of developed nations have access to computing resources. Trust is strongly tied to Internet security. One study shows that in a survey of scholarly papers on security concerns for cloud computing, few papers actually concentrated on the subject of security itself. Our research shows that consumer trust in their cloud service providers (CSPs) is a significant issue and provides a proposed solution. We accomplish this by conducting a survey of Internet consumer opinions and analyzing the results to determine pathways to consumer trust. This will determine the extent of a problem with trust and what industry is currently doing about it.

Our research shows that consumer trust in their cloud service providers (CSPs) is a significant issue and provides a proposed solution. We accomplish this by conducting a survey of Internet consumer opinions and analyzing the results to determine pathways to consumer trust. This will determine the extent of a problem with trust and what industry is currently doing about it.

PROBLEM DEFINITION

Cloud services are gaining popularity with times. Service level agreement (SLA) serves a basic understanding between the clients and cloud service providers (CSP). Ensuring secured and adequate service is a basic need of the customers.

"Trust management is a top obstacle in cloud computing". Trust is strongly tied to Internet security.

A person or an industry having access over internet and adequate infrastructure for intranet can opt for various on-demand cloud services. Change management was a tough requirement in pre-cloud computing era. One had to think on different critical aspects before incorporating changes at infrastructure level or in application level . This challenge has softened with the advancement of cloud computing technology. All these service modalities are illustrated in Service Level Agreement (SLA).

In literature no such decision derivation tool is available for assessing services offered by cloud service providers. Turing models provides fundamental mathematical automation in a decision making process. Such models are easy to automate and will offer feasible roadmap to set up an application for such assessment. Turing model is not yet employed in cloud SLA models. Hence this was found to be an excellent prospect for modelling.

QoS parameters of a cloud service might involve service response time, tenure of service, backup mechanism, disaster management and recovery and many other aspects. This has imparted immense motivation to figure out a Turing based model on the basis of different quality parameters. The model will help a customer to assess different standards of offerings through a sequential validation towards deriving an automated decision. It has ensured confidentiality, integrity and availability.

There has been a lot of research on user's data security from technical aspects, however, there is not much work done to understand the psychology of consumer's trust in the new Internet marketplace. This module examines the issues surrounding the difficulty of the average Internet user to trust cloud service providers with the security of their data. By examining user sentiment we attempt to outline the scope of the problem and suggest how cloud service providers may overcome trust issues. We accomplished this by conducting a survey of Internet consumer opinions and analyzing the results to determine pathways to consumer trust. This will determine the extent of a problem with trust and what industry is currently doing about it.

LITERATURE SURVEY

Cloud computing enhances the ability to store data and various applications on remote servers, and accessing them via internet rather than saving it on personal computer and the word "cloud" is used because data and all the applications are stored on cloud based web servers and connected computers network owned by a third party and it can be accessed using a cloud computing software i.e;www.cloudcomputing.com web based server which helps to access all the files and applications required and its not only used to store data but it's also inexpensive, efficient and flexible comparable to high memory computers.

Clouds into four types**:**

(i) Public clouds, whose services can be hired by the general public,

(ii) Private clouds, which are deployed to be used by a single organization;

(iii) Hybrid clouds which is a combination of the public and private cloud models.

(iv) Virtual private clouds (VPC), which is an alternative solution to solve the limitations of public and private clouds.

Service Level Agreements (SLAs) are the formalization of the characteristics of a service. Several languages to specify SLAs and to automatize their evaluation and negotiation were proposed. An SLA is a contract negotiated and agreed upon between cloud users and cloud providers. It defines Quality of Services (QoS) that cloud providers promise to offer and a price that cloud users are willing to pay for received services.

An user was working on a computer and suddenly a mirror broke down into pieces in that particular place and the computer was no more but then also all the folders, music files, documents were present rather it was saved online in a specific location namely: cloud and when something is stored in cloud that means it is stored on internet servers which implies an extra hardware which is portable and data can be stored anywhere anytime if connected to the internet.

Fig 1: User accessing the cloud based applications

There are three services for cloud->IAAS,PAAS,SAAS..

In case of IAAS the infrastructure is only required and rent is paid on it only and rest platform can be installed or may be its already installed on it like windows or Linux and infrastructure means the hardware part it may be computer or network and software can be deployed if there is a group of IT people of some software developers are present.

In case of PAAS the platform is required to rent for and infrastructure is already there and software can be developed and in this case the companies like GOOGLE and so on has its own platform and infrastructure headache is not required and only programmers required.

In case of SAAS the software needs to be rented rest already present and here the leading company is sales force and it has thousands of software and play store and app store in android phone and i-phone apps are developed and here through app exchange we can download the software in cloud or our account in sales force and here only customization required on the basis of business requirement.

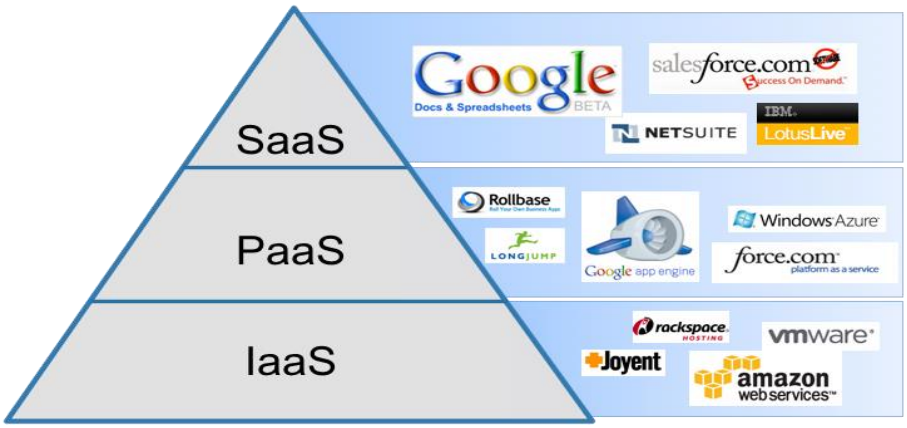


Fig 2: To show the leading companies with its services

Various types of aspects in SLA are present through cloud computing those are-
1) Volume of service.
2) Quality of service.
3) Peak and average loads of work.
4) Volume of demand at different types of day.
5) Penalty for the cloud provider in case the provider fails to meet these service requirements.
6) Variable Performance.
7) They over commit their computing resources and cut corners on infrastructure.
8) Specify memory allocation and leave CPU allocation unspecified, allowing total hardware memory to dictate the number of customers the hardware can support
9) Quote shared resource maximums instead of private allocations
10) Offer a range of performance for a particular instance, such as a range of GHz
11) Over allocate resources on a physical server, or thin provisioning.

Sukwong et al. have proposed a dynamic adjustment of resource allocation using control theory based approach for service differentiation that is "**Managing SLAs for highly consolidated cloud,"**. In **"A framework and ontology for dynamic web services selection,"** Internet Computing, and **"An overview of the galaxy management framework for scalable enterprise cluster computing,"** authors have emphasized on the issues like CPU cycles and single server processing for catering multiple customer requests for resource allocation or application provisioning. Appleby et al "Oceano-SLA based management of a computing utility," suggested an adjustment mechanism for CPU resources and its allocation to different virtual machine based on the load of customer at any point of time. A dynamic shift mechanism for resource allocation is the key proposal of this work. Granularity issues of whole virtual machines (VMs) and their server management are in the prime focus of SLARMS.

All these researches have proposed different mechanisms towards maintaining quality of services offered by cloud service providers. Mostly these researches have focused on load balancing in either –or another ways. However none of them unfolds the statement of quality to the clients and provides any opportunity of selection. This survey has imparted immense motivation to figure out a model on the basis of different quality parameters. The model will help a customer to assess different standards of offerings through a sequential validation towards deriving an automated decision.

The problem is user's trust in the services offered on Internet. If security is not handled properly, the entire area of cloud computing would fail since cloud computing mainly involves managing personal sensitive information in a public network. Data service providers of all types need innovative ways to be able to draw customers and learn from the data those customers use. Service providers must become the biggest proponents of data security and privacy to gain the trust and business of the masses. Trust is strongly tied to Internet security. Our proposed module shows that consumer trust in their cloud service providers (CSPs) is a significant issue and provides a proposed solution.

Our survey was designed to answer three underlying research questions. First, is there a consumer lack of trust with cloud service providers? Second, is there a way for cloud storage providers to earn consumer trust? Finally, will it be profitable for cloud service providers to work towards consumer trust? The questions have three areas of emphasis, demographics, opinions on security, and finally users' current online habits. They also vary in the data type collected. The survey is a mix of true/false, Likert scale, and opens ended questions. The section of open ended questions was given but the data from those questions is currently not processed.

We accomplish this by conducting a survey of Internet consumer opinions and analyzing the results to determine pathways to consumer trust. This will determine the extent of a problem with trust and what industry is currently doing about it.

SRS (SOFTWARE REQUIREMENT SPECIFICATION)

The SRS states the functions and capabilities that a software system needs to provide, as well as the constraints that it must respect. The SRS provides the basis for all subsequent project planning, design, coding, and testing.

There are many significant benefits to having a SRS document. For starters, the SRS improves communication between your team members by saving and displaying the product feature description in one central location that everybody can easily access. It also prevents confusion within your team by maintaining an up-to-date definition list of all the features included in the project. This way you ensure that everyone develops the same set of features, avoiding a situation in which there are several different versions of product documents out there. And because all that information is available in one document, the SRS makes it easy for new employees to quickly learn the details of the project.

Software Required: - JAVA

Interpreter application: - COMMAND PROMPT APPLICATION

Version: - jdk1.8.0_45

Path: - C:\Program Files\Java\jdk1.8.0_45\bin

Size:- 4.10 KB

PLANNING

This paper presents a Turing model for verification and assessment of SLA under different cloud deployments. This model will help one customer to compare and assess his needs with the service attributes offered by a CSP and accordingly the customer will be able to make a decision about accepting or rejecting a CSP.

In order to facilitate this service attribute validation, first a risk categorization of cloud services has been made to trace out parameters involved with service quality management. In the proposed model, these parameters are arranged in a sequence to perform validation check. A symbol table has been prepared to represent each state of validation. Quality quantification has been done to define an instruction table for setting up the rules for decision making process.

In this work some performance objectives of cloud service have been identified for evaluating service level agreement (SLA) of cloud service provider (CSP). A generic rule set is identified on those objectives to check the compliance of SLA. Proposed Turing model for SLA compliance checking is designed on those rule set and associated action classifier.

Risk factors involved in different cloud deployment models are varied on the basis of the nature and profiles of the services. Most of the auditing task in cloud deployment is specific to client types and their nature of attainments of services. Classification of associated risk factors can be categorized as:-confidentiality, integrity, availability.

This work proposes a Turing model where some key factors are tied in a sequence of test chain to perform checks for compliance of service level agreement (SLA) by cloud service providers (CSP). The parameters under consideration are:

(i) Credentials of service provider.
(ii) Quality of service including number of clients.
(iii) Sustainability of service.
(iv) Compliance of service standard.
(v) Disaster recovery and continuity of operation planning and testing.
(vi) Specification of exemption.
(vii) Declaration of penalty.

Now on the basis of above seven check points, a control flow for compliance check is defined in figure 1 and that acts as the basis for Turing model.
The check constraints defined in Fig. 1 are inter-dependent and the proposed rule set is designed on the basis of their inter-dependencies. However these seven parameters are classified in to three groups as shown in Table 1.

TABLE NO. 01:- CLASSIFICATION OF COMPLIANCE CHECK PARAMETERS

SLA Schema	Module Specification
Identity Assessment	Credential Check
	Service Quality Check
Reliability Assessment	Sustainability of Service
	Compliance of Standard
	Disaster Recovery
Corrective Assessment	Exemption Specification
	Declaration of Penalty

This section will illustrate different set of rules towards evaluation of service level agreement offered by a cloud service provider. According to the description of figure 1 and table 1, this rule set will be classified in to three major modules.
(i) **Identity assessment** to check the quality of service provided by the cloud service provider along with their credentials
(ii) **Reliability assessment** to verify obligation of the CSP for different standard norms, availability of alternative arrangements during failure and measures in adversary
(iii) **Corrective assessment** to ascertain the exemption rules and penal measures that can be initiated upon CSP in case of non-compliance

DESIGN

Fig: 03

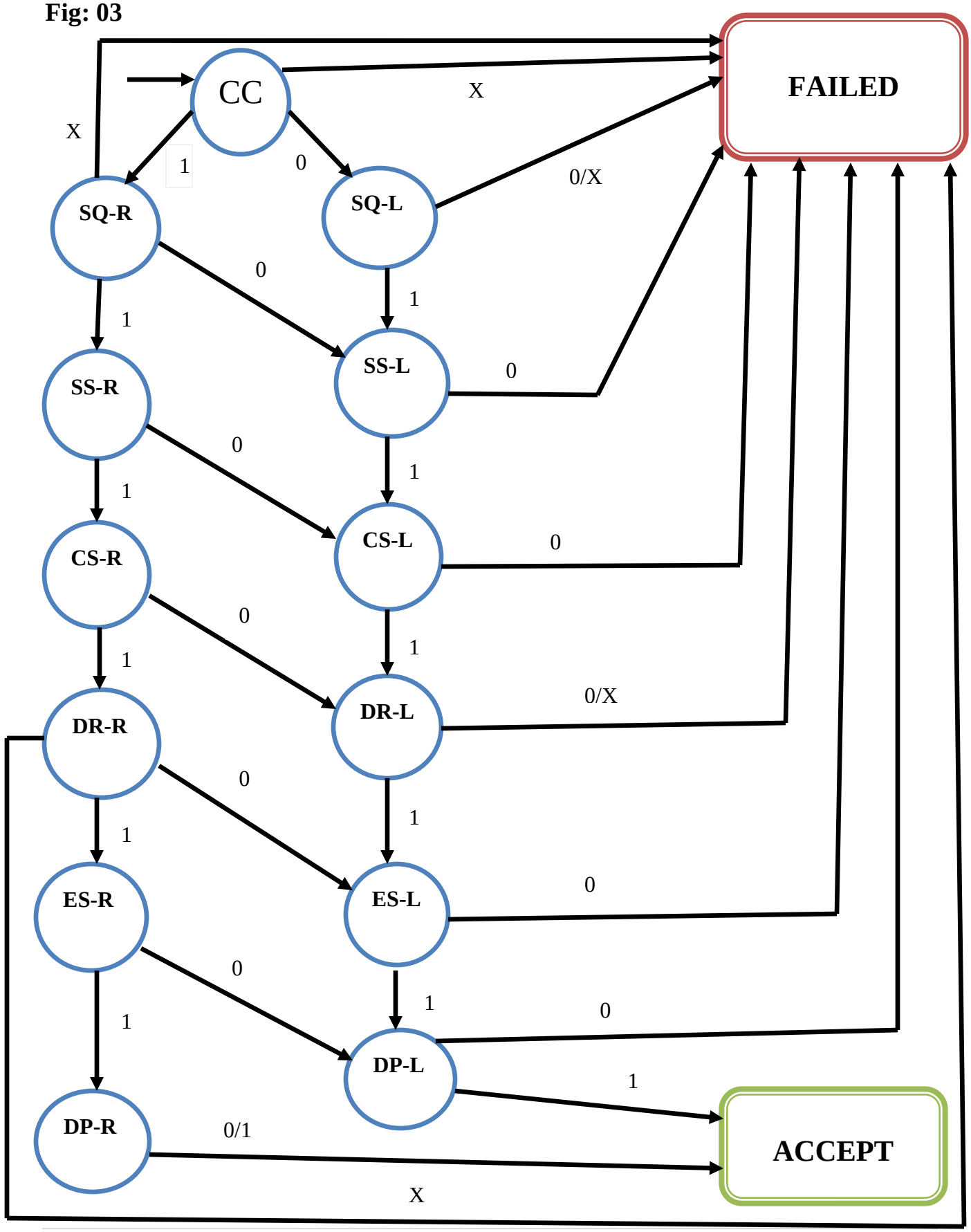


TABLE NO. 02:- INPUT DEFINITION FOR MODULE

MODULE NAME	STATE	SPECIFICATION	INPUT
Credential Check	**CC**	**Defined**	**1**
		Partially Defined	**0**
		Not Defined	**x**
Service Quality Check	**SQ**	**High**	**1**
		Medium	**0**
		Low	**x**
Sustainability Of Service	**SS**	**Available**	**1**
		Not available	**0**
Compliance Of Standard	**CS**	**Accreditation Available**	**1**
		Accreditation Not Available	**0**
Disaster Recovery	**DR**	**Strong**	**1**
		Medium	**0**
		Weak	**X**
Exemption Specification	**ES**	**Declared**	**1**
		Undeclared	**0**
Declaration Of Penalty	**DP**	**Available**	**1**
		Not Available	**0**

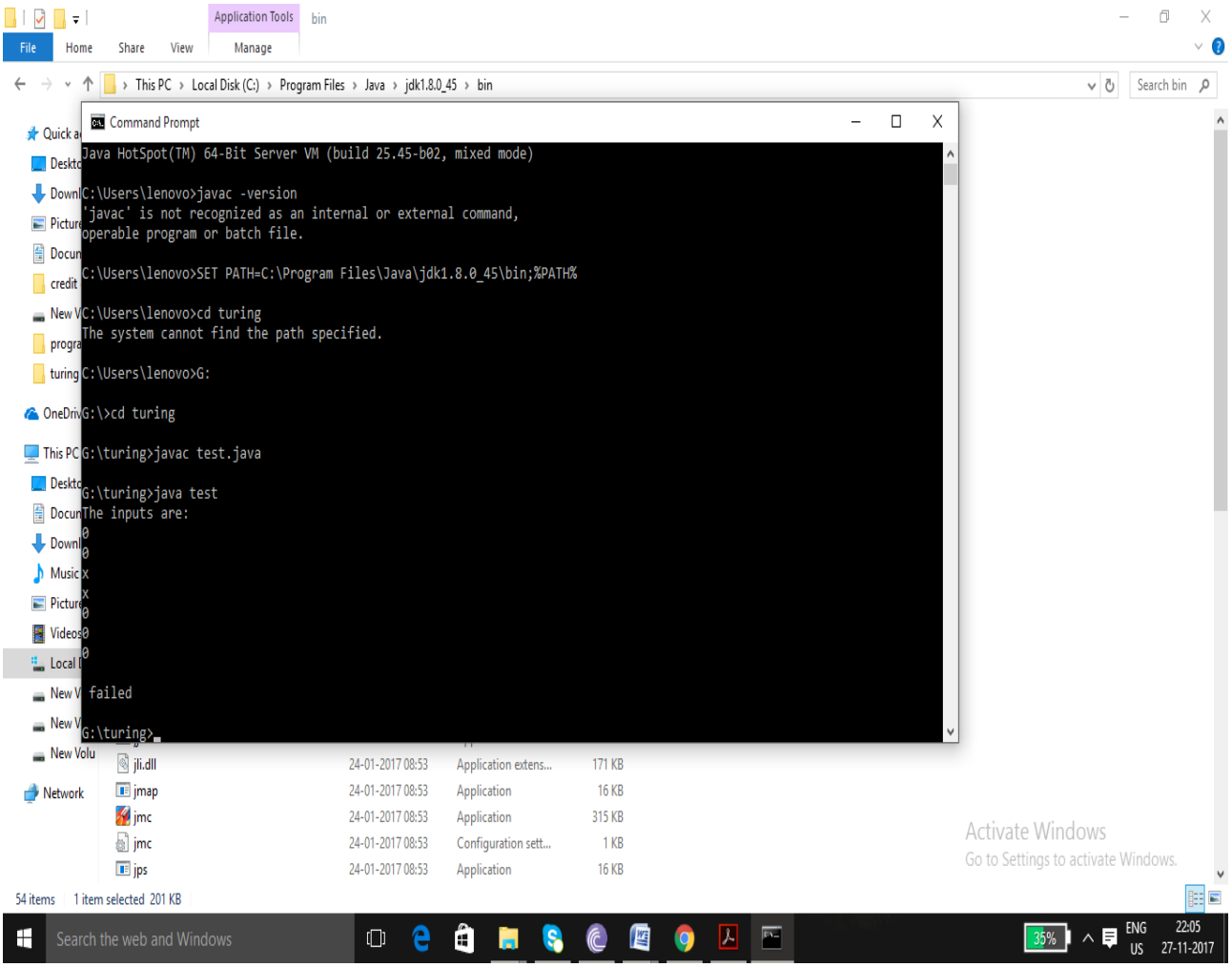
Table 2 represents different class of evaluation specifications under the modules described in table 1. These values are annotated with respective input symbols. In the input symbols, 1 represent good standard, 0 represent average or weak standard and X represent non-existence. Name of different states representing each module of table 1 are also given in table 2.

TABLE NO. 03:- RULES BASE AND INSTRUCTION TABLE

STATE	PRESENT STATE	INPUT	NEXT STATE	COMMENT
CC	START (CC)	1	SQ-RIGHT	
		0	SQ-LEFT	
		X	FAILED	FAILED
SQ	SQ-RIGHT	1	SS-RIGHT	
		0	SS-LEFT	
		X	FAILED	FAILED
	SQ-LEFT	1	SS-RIGHT	
		0	FAILED	FAILED
		X	FAILED	FAILED
SS	SS-RIGHT	1	CS-RIGHT	
		0	CS-LEFT	
	SS-LEFT	1	CS-LEFT	
		0	FAILED	FAILED
CS	CS-RIGHT	1	DR-RIGHT	
		0	DR-LEFT	
	CS-LEFT	1	DR-LEFT	
		0	FAILED	FAILED
DR	DR-RIGHT	1	ES-RIGHT	
		0	ES-LEFT	
		X	FAILED	FAILED
	DR-LEFT	1	ES-LEFT	
		0	FAILED	FAILED
		X	FAILED	FAILED
ES	ES-RIGHT	1	DP-RIGHT	
		0	DP-LEFT	
	ES-LEFT	1	DP-LEFT	
		0	FAILED	FAILED
DP	DP-RIGHT	1	FINAL	ACCEPT
		0	FINAL	ACCEPT
	DP-LEFT	1	FINAL	ACCEPT
		0	FAILED	FAILED

Table 3 represents rule base and instruction table on the basis of formal description given in table 1 and table 2. Overall transition of the Turing model will be governed by the instruction table depicted in table 3. In this table 3, F means failure in evaluation of SLA which will lead to decision of rejection. Success denotes approval. In this conceptualized rule base, any non-compliance of standards or non-availability will lead to outright rejection. Apart from this, if two consecutive performance criteria are measured to be poor/ unavailable/ undefined/ undeclared then that situation will also lead to termination. Otherwise the model will approve the proposed SLA compliance test. Figure 2 presents the Turing model diagram as per the discussion.

EXPERIMENTAL RESULTS



TRUST IN CLOUD COMPUTING

The information age has matured to the point where most citizens of developed nations have access to computing resources. To comfortably exist in a highly developed nation the average citizen is nearly required to have access to computing resources in order to have access to other basic services such as banking and bill paying. The efficiency that computing brings to business makes paying for basic utilities (water, electricity, gas, and telephony, and soon to be health care) on the Internet the norm. The Internet is often referred to now as the fifth utility. The problem is user's trust in the services offered on Internet. If security is not handled properly, the entire area of cloud computing would fail since cloud computing mainly involves managing personal sensitive information in a public network.

According to a 2010 survey conducted by the Fujitsu corporation, 88% of users, worldwide, are worried about who has access to their data and almost that much is worried about where their data is physically stored [1]. Data service providers of all types need innovative ways to be able to draw customers and learn from the data those customers use. Service providers must become the biggest proponents of data security and privacy to gain the trust and business of the masses. Trust is strongly tied to Internet security.

SURVEY TO MEASURE TRUST IN CLOUD COMPUTING

A. Survey Objectives

Our survey is designed to answer three underlying research questions. First, is there a consumer lack of trust with cloud service providers? Second, is there a way for cloud storage providers to earn consumer trust? Finally, will it be profitable for cloud service providers to work towards consumer trust? The questions have three areas of emphasis, demographics, opinions on security, and finally users' current online habits. They also vary in the data type collected. The survey is a mix of true/false, Linker scale, and opens ended questions. The section of open ended questions was given but the data from those questions is currently not processed. The questions were developed in consultation with subject matter experts and from observations gathered through literature review. We could not find another survey that discussed trust matters in cloud computing from a user's perspective.

B. Survey Methodology

The survey was distributed online through several different venues. There were 236 total respondents. The two primary distributions were Facebook and a list server for a group of United States Army Information Systems Managers. Facebook proved to be a powerful collection tool in that once respondents took the survey; many also shared it with their friends. This led to a more diverse population. The initial link was shared on two user's pages but quickly spread through resharing to many users that were completely unknown to the original posters. The US Army list server also produced good results. On the days that the request was posted, survey participation spiked. This was good for participation but due to the education level of the respondents on those days, it may have slightly skewed some of the results as will be seen. The respondents were given the definition of Personally Identifiable Information (PII) for purposes of the survey. PII, as used in US privacy law and information security.

ANALYSIS OF SURVEY RESULTS

Demographic questions:

The emphasis on the survey is intended to be about the nature of user opinions rather than comparing the opinions of differing demographics. In hindsight, more demographic information may have been helpful in answering the question in terms of finding certain ways for cloud service providers to earn the trust of consumers.

Internet use questions:

The following questions focused on opinions of the average consumer on the security of their data. The intent is to first try and figure out how respondents currently used the Internet in terms of PII security and then later ask what they expected in terms of security. These questions brought some surprising results in that it initially appears that respondents actually do put a lot of PII on the Internet already. In fact, we find that almost every conceivable form of PII is already placed on the Internet by respondents, just not all in the same place at the same time.

Security Habits:

Through the survey data, it is safe to say that education is important to trust. Respondents must understand what is in the terms and conditions of online transactions. It is also important that respondents understand where and how their data is stored. The more they know, the more they trust. For the cloud service provider it is, therefore, important to find out how much time people are willing to spend to learn more. This directly equates to respondent's willingness to try and trust a service provider. It can be interpreted from the results of the questions that the respondents clearly know there is a problem but they have not done much to correct it. They haven't read more about PII security and they see that it may be too complicated for them to solve. The good news is that they are willing to do something. They just need to be shown the way.

Opinion questions:

The technology savvy group may have had an effect on this answer. Technology workers understand that when data is given to them, it is their duty to protect it. Non-technology workers may not have this understanding. The question is an attempt to see if it would be profitable for cloud service providers to offer pay plans for increased protection. Based on the preliminary results it seems this would not be true. The problem is that the question may not have been clear or could be interpreted differently by different people. It may have been clearer if the question asked if respondents were willing to pay extra to keep their information secure. Throughout the survey it can be inferred that the respondents generally feel that it is the responsibility of the CSP to secure their data because they don't know where it is stored or how.

Fuzzy Implementation On Trust Evaluation

Fuzzy logic:

Fuzzy means uncertainty, not clear or distinct. A form of knowledge representation suitable for ideas that cannot be defined exactly, but which depends upon their contexts. It is also known a rule based system which is used to model human problem solving activities and a classical way to represent the human knowledge by IF-THEN rules. It is approximate rather than exact. Fuzzy logic derives from the fact that most modes of human reasoning are approximate in nature. Fuzzy inference methods are growing to be more strong and stretchy with approximate reasoning method of fuzzy logic. Also it provides a unique computational framework for inference in rule-based system.

Advantage Of using fuzzy logic includes:

- To understand physical system and control requirements.
- To develop a linear model of plant sensors and actuators
- To determine a simplified controller from control theory
- To develop an algorithm for the controller
- To simulate, debug and implement design.

In fuzzy logic two types of fuzzy inference method are **Mamdani** and **Sugeno** fuzzy inference methods.

In Mamdani Fuzzy models describes that Fuzzy system *components are* knowledged base, an inference system and the fuzzifier and defuzzifier interfaces. Fuzzifiers convert crisp numbers into fuzzy numbers, Defuzzifiers convert fuzzy numbers into crisp numbers.

Fuzzy controller includes:

Fuzzy knowledge base or rule base: A set of IF-THEN rules

Fuzzy inference: maps fuzzy sets onto other fuzzy sets using membership functions

Fuzzifying: Scales and maps input variables to fuzzy sets

Defuzzifying: mapping a set of fuzzy outputs onto a set of crisp output commands

Sugeno Fuzzy Model's objectives are Generation of fuzzy rules from a given input-output data set. Michio Sugeno suggested to use a single spike, a singleton, as the membership function of the rule consequent. A singleton, or more precisely a fuzzy singleton, is a fuzzy set with a membership function that is unity at a single particular point on the universe of discourse and zero everywhere

else. The main advantage is that they present a compact system equation which allows us to estimate the parameters and makes its design easier. It based on rules where antecedent is composed of linguistic variables and the resultant was represented by a function of input variables. This fuzzy rule based system separating the input space in several fuzzy subspaces and defining a linear input-output association in each one of these subspaces.

In this Turing model we use mamdani fuzzy inference method to analyze trust evaluation. Here seven different parameters are associated with service level agreement for compliance checking that acts as the basis of Turing model. These different parameters have different specification and different input values respectively. Considering those rule sets in fuzzy inference model for trust analysis is deployed. This fuzzy inference model implements trust analysis using rule base and instruction table for evaluation of trust model SLA by accepting or rejecting. As we use fuzzy rule base system for trust evaluation, so we consider mamdani fuzzy inference method.

Proposed Model

This paper proposes a fuzzy approach for Turing model where some key factors are considered in a sequence of test chain to ensure a trusted service from the part of service providers. We consider the key parameters such as credential check, service quality check, sustainability of service, compliance of standard, disaster recovery. Credentials of service provider to declare their activation date, service up-time. Quality of service including number of clients that can be served at a given time, response time for serving customer service request. Sustainability of service to ensure corrective measures in case of roll back of service provider. Compliance of service standard which involves self-compliance check and service auditing. Disaster recovery and continuity of operation planning and testing under adversary.

Here the basis of five key parameters, a control flow for compliance check is defined in figure and using fuzzy logic that acts as the basis for Turing model. The key parameters are inter-dependent and the proposed rule set is designed on the basis of their inter-dependencies. However these five parameters are classified into two groups one is identity assessment another is reliability assessment. Identity assessment is to check the quality of service provided by the cloud service provider along with their credentials and Reliability assessment to verify obligation of the CSP for different standard norms, availability of alternative arrangements during failure and measures in adversary.

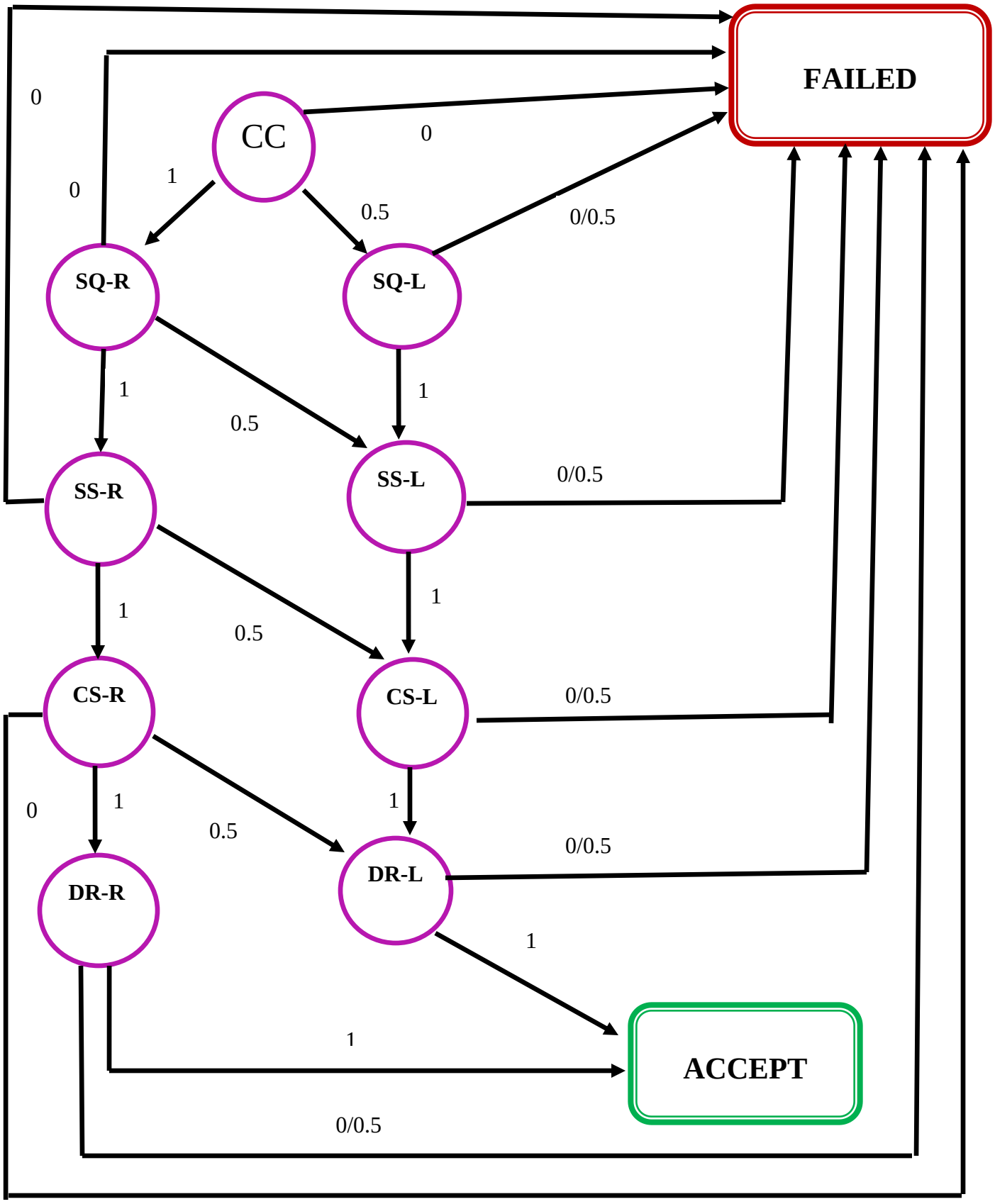
TABLE NO. 04:- INPUT DEFINITION FOR MODULE AFTER IMPLEMENTATION OF FUZZY LOGIC

MODULE NAME	STATE	SPECIFICATION	INPUT
Credential Check	**CC**	**Defined**	**1**
		Partially Defined	**0.5**
		Not Defined	**0**
Service Quality Check	**SQ**	**High**	**1**
		Medium	**0.5**
		Low	**0**
Sustainability Of Service	**SS**	**High**	**1**
		Medium	**0.5**
		Low	**0**
Compliance Of Standard	**CS**	**High**	**1**
		Medium	**0.5**
		Low	**0**
Disaster Recovery	**DR**	**Strong**	**1**
		Medium	**0.5**
		Weak	**0**

TABLE NO. 05:- RULES BASE AND INSTRUCTION TABLE AFTER IMPLEMENTATION OF FUZZY LOGIC

STATE	PRESENT STATE	INPUT	NEXT STATE	COMMENT
CC	START (CC)	1	SQ-RIGHT	
		0.5	SQ-LEFT	
		0	FAILED	FAILED
SQ	SQ-RIGHT	1	SS-RIGHT	
		0.5	SS-LEFT	
		0	FAILED	FAILED
	SQ-LEFT	1	SS-RIGHT	
		0.5	FAILED	FAILED
		0	FAILED	FAILED
SS	SS-RIGHT	1	CS-RIGHT	
		0.5	CS-LEFT	
		0	FAILED	FAILED
	SS-LEFT	1	CS-LEFT	
		0.5	FAILED	FAILED
		0	FAILED	FAILED
CS	CS-RIGHT	1	DR-RIGHT	
		0.5	DR-LEFT	
		0	FAILED	FAILED
	CS-LEFT	1	DR-LEFT	
		0.5	FAILED	FAILED
		0	FAILED	FAILED
DR	DR-RIGHT	1	FINAL	ACCEPT
		0.5	ES-LEFT	
		0	FAILED	FAILED
	DR-LEFT	1	FINAL	ACCEPT
		0.5	FAILED	FAILED
		0	FAILED	FAILED

Fig: 04: DFD of the design after Fuzzy Implementation



These values are annotated with respective input symbols. In the input symbols, 1 represents good standard, 0.5 represents average or weak standard and 0 represents`` non-existence. Name of different states representing each module and specification of each module defined by different input values.
Our Trust assessment model evaluates trust of cloud using fuzzy logic would comprise by the following step:

- Fuzzification of input compliance parameters for trust evaluation
- Determination of application rules and inference method
- Defuzzyfication of compliance parameters for trust evaluation
- Fuzzification of input compliance parameters for trust evaluation

Each compliance parameter is assigned with one of the linguistic variables namely Defined, Partially Defined, Not Defined, High, Medium, Low, Strong and Medium. Task of these variables to the compliance parameters vary significantly based on the other parameter input value. For example, if credential checking is defined and all other parameter value is high then the assessment model is accepted, but if the value of one parameter is low and the assessment model is rejected then it may affect the trust evaluation. So trust evaluation depends on the fuzzy Turing model. This will be discussed in the next section for better understanding of the model.

- Determination of application rules and inference method

Each parameter is assigned a crisp value, which helps us in inferring the compliance variable. In Table 3, each linguistic variable is used for compliance parameters.

TABLE NO. 06:- LINGUISTIC VARIABLES AND ASSIGNED VALUES

Linguistic Variables	Assigned value
High Medium	1 0.5
Low	0

Defuzzyfication of compliance parameters for trust evaluation

The value has obtained in the previous step must be converted to a crisp value. This process is known as defuzzification. According to the membership function of the output variable defuzzification is performed. The final value is obtained by dividing our crisp value as it gives the output value in the range 0-1. The fuzzy set of output variables are accepted and rejected .The list of following rules are formulated as:

- If credential checking is defined, service quality is high, sustainability of service is high, compliance of standard is high and disaster recovery is strong then assessment is accepted.
- If credential checking is partially defined, service quality is high, sustainability of service is high, compliance of standard is high and disaster recovery is strong then assessment is accepted.
- If credential checking is defined, service quality is medium, sustainability of service is high, compliance of service is high and disaster recovery is strong then assessment is accepted.
- If credential checking is defined, service quality is high, sustainability of service is medium, compliance of standard is high and disaster recovery is strong then assessment is accepted.
- If credential checking is defined, service quality is high, sustainability of service is high, compliance of service is medium and disaster recovery is strong then assessment is accepted.
- If credential checking is not defined, then assessment is rejected.
- If credential checking is partially defined and service quality is medium, then assessment is rejected.
- If credential checking is partially defined and service quality is low, then assessment is rejected.
- If credential checking is defined and service quality is low, then assessment is rejected.
- If credential checking is partially defined and service quality is high and sustainability of service is medium then assessment is rejected.
- If credential checking is partially defined and service quality is high and sustainability of service is low then assessment is rejected.
- If credential checking is defined and service quality is medium and sustainability of service is medium then assessment is rejected.

- If credential checking is defined and service quality is medium and sustainability of service is low then assessment is rejected.
- If credential checking is partially defined, service quality is high, sustainability of service is high and compliance of standard is medium then assessment is rejected.
- If credential checking is partially defined, service quality is high, sustainability of service is high and compliance of standard is low then assessment is rejected.
- If credential checking is defined, service quality is high, sustainability of service is medium and compliance of standard is medium then assessment is rejected.
- If credential checking is defined, service quality is high, sustainability of service is medium and compliance of standard is low then assessment is rejected.
- If credential checking is defined and service quality is high and sustainability of service is low then assessment is rejected.
- If credential checking is partially defined, service quality is high, sustainability of service is high, compliance of standard is high and disaster recovery is medium then assessment is rejected.
- If credential checking is partially defined, service quality is high, sustainability of service is high, compliance of standard is high and disaster recovery is weak then assessment is rejected.
- If credential checking is defined, service quality is high, sustainability of service is high, compliance of standard is medium and disaster recovery is medium then assessment is rejected.
- If credential checking is defined, service quality is high, sustainability of service is high, compliance of standard is medium and disaster recovery is weak then assessment is rejected.
- If credential checking is defined, service quality is high, sustainability of service is high and compliance of standard is low then assessment is rejected.
- If credential checking is defined, service quality is high, sustainability of service is high, compliance of standard is high and disaster recovery is medium then assessment is rejected.
- If credential checking is defined, service quality is high, sustainability of service is high, compliance of standard is high and disaster recovery is weak then assessment is rejected.

Fuzzy logic Implementation

Credential Check: Credential check has three input values namely defined, partially defined and not defined. In figure5 and figure6, the output of credential checking is obtained from the fuzzy model is accepted for all other compliance parameters input specification high in case of Cc input specification high and medium otherwise is rejected.

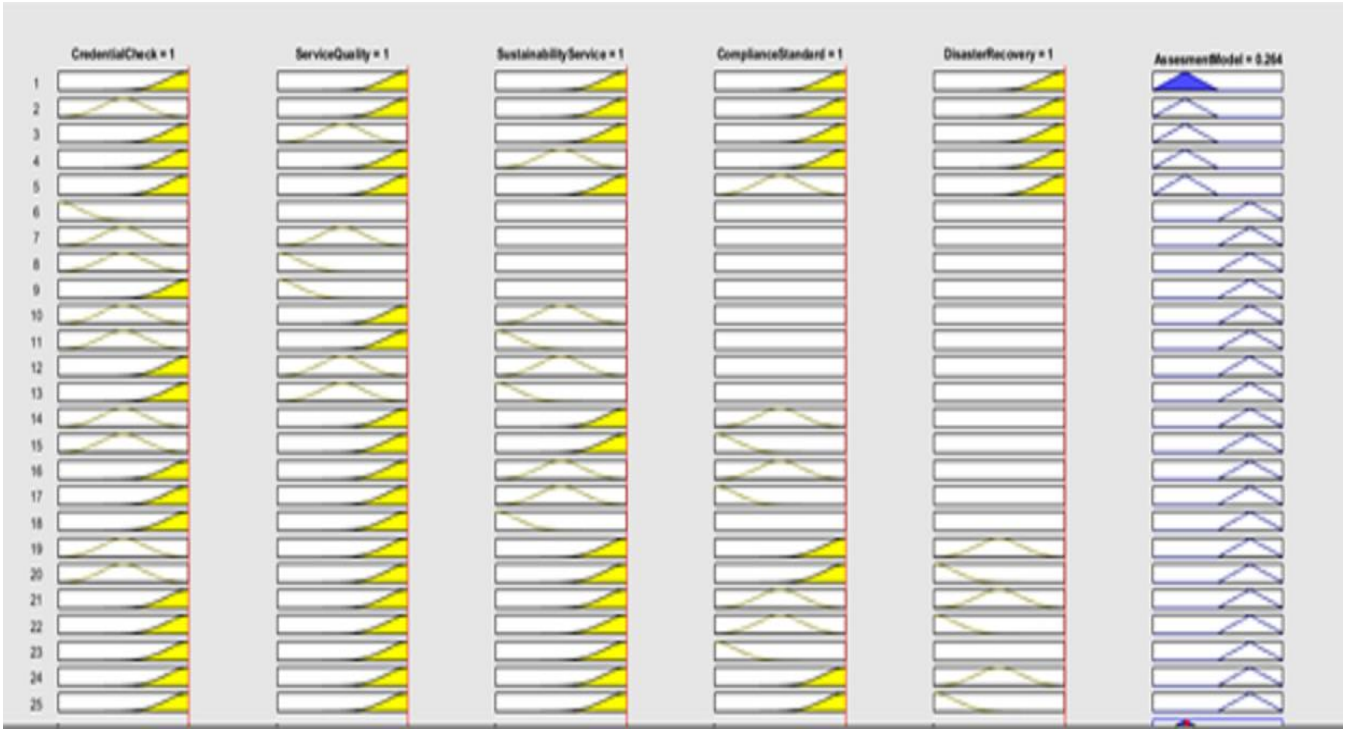


Fig: 05

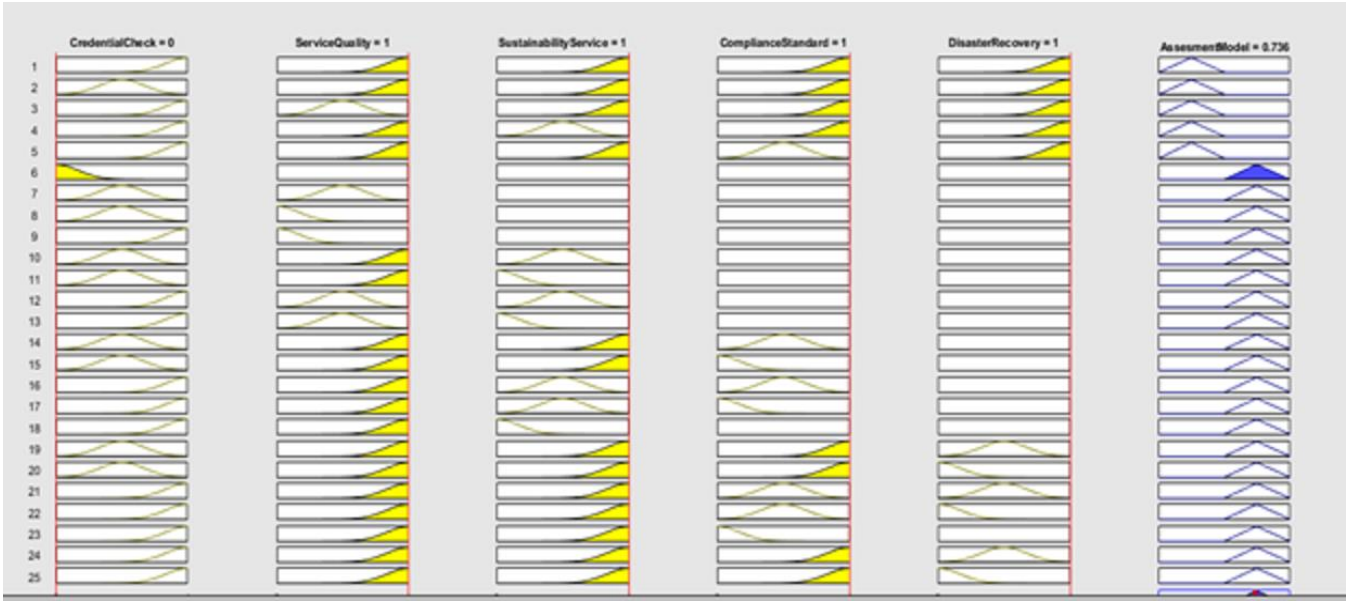


Fig: 06

Service Quality Check: This compliance parameter has three input value namely high, medium and low. In figure7 and figure8, for the parameter SQ-right if input specification high and medium if all other following parameter input specification is high then the assessment model is accepted otherwise rejected. Similarly In figure4 and figure5 for the parameter SQ-left if input specification high and the following parameter input specification is also high then the assessment model is accepted otherwise rejected.

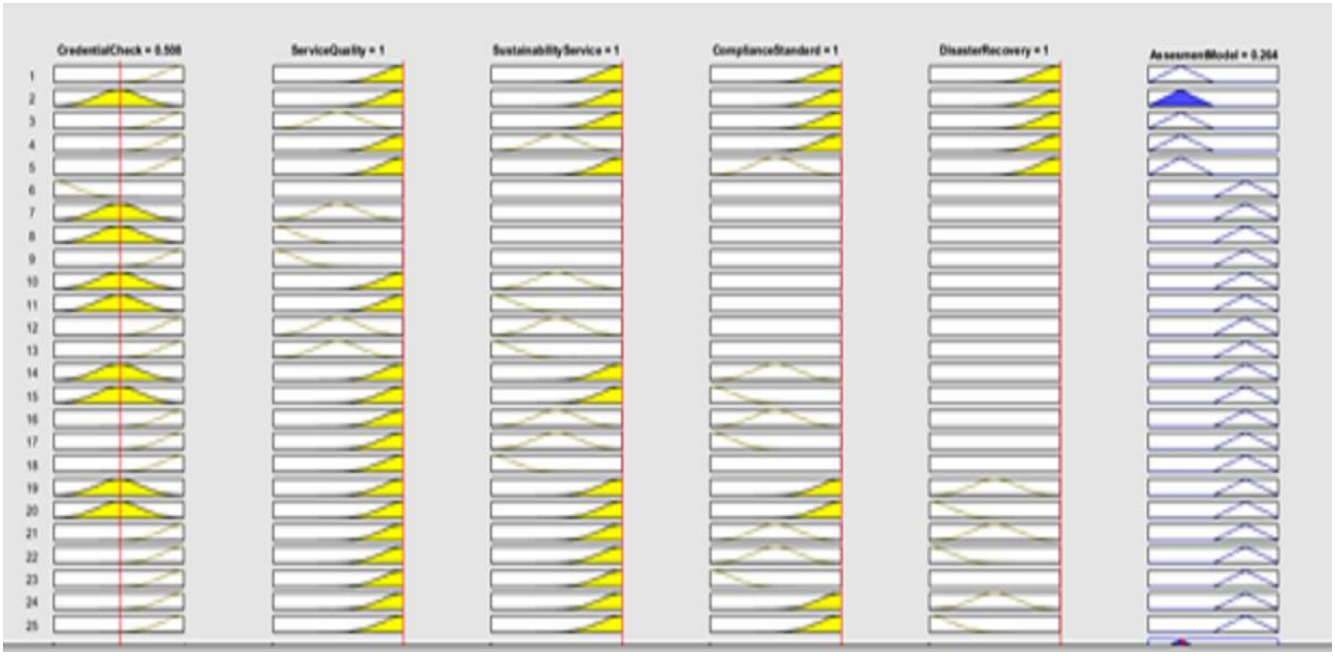


Fig: 07

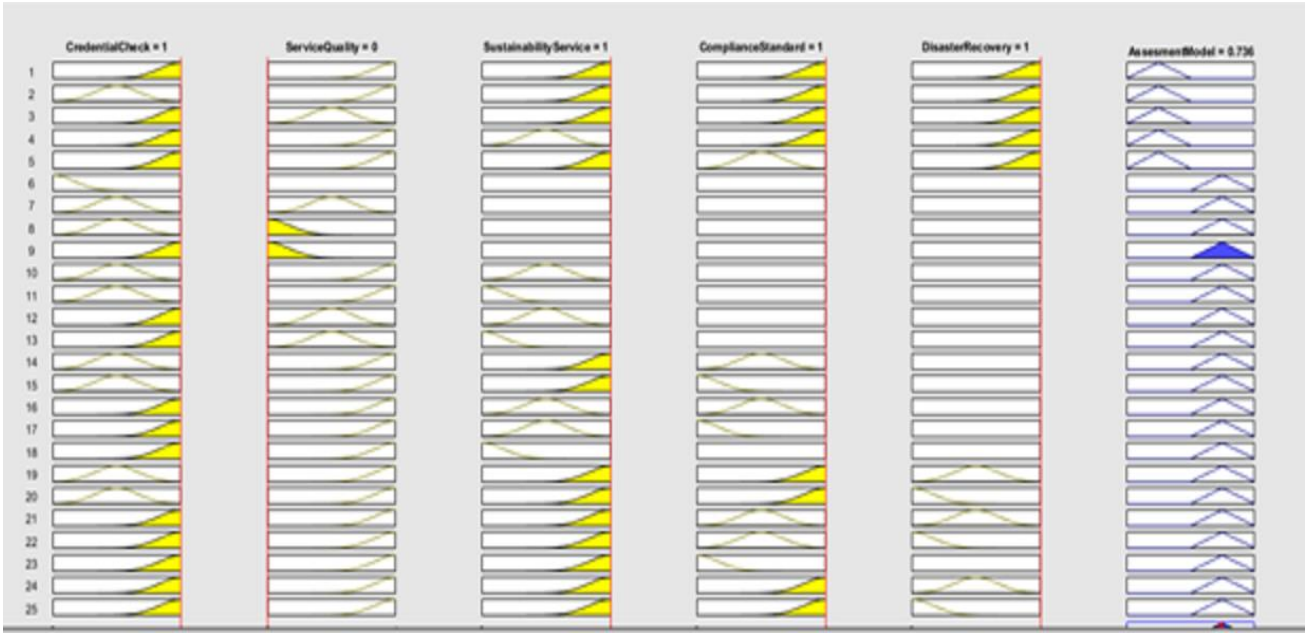


Fig: 08

Sustainability of Service: This service has three input value namely high, medium and low. In figure 9 and figure10, for the parameter SS-right if input specification high and medium if all other following parameter input specification is high then the assessment model is accepted otherwise rejected. Similarly in figure6 and figure7, for the parameter SS-left if input specification high and the following parameter input specification is also high then the assessment model is accepted otherwise rejected.

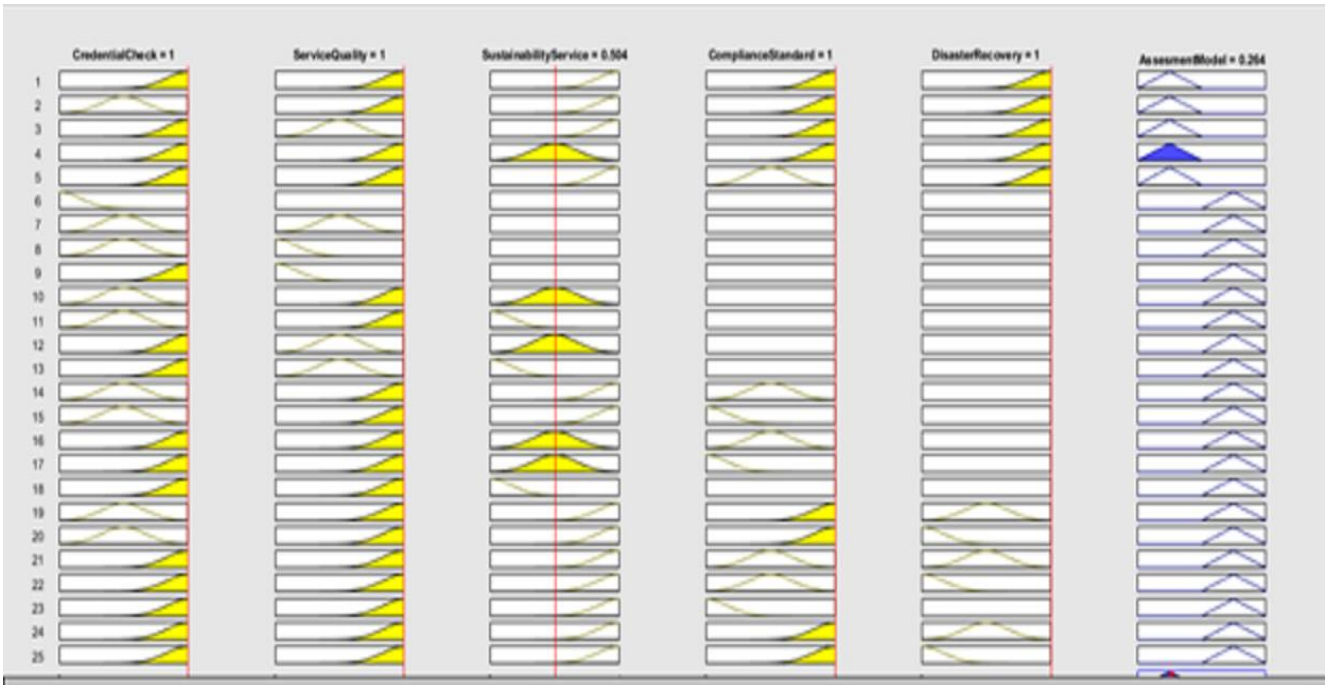


Fig: 09

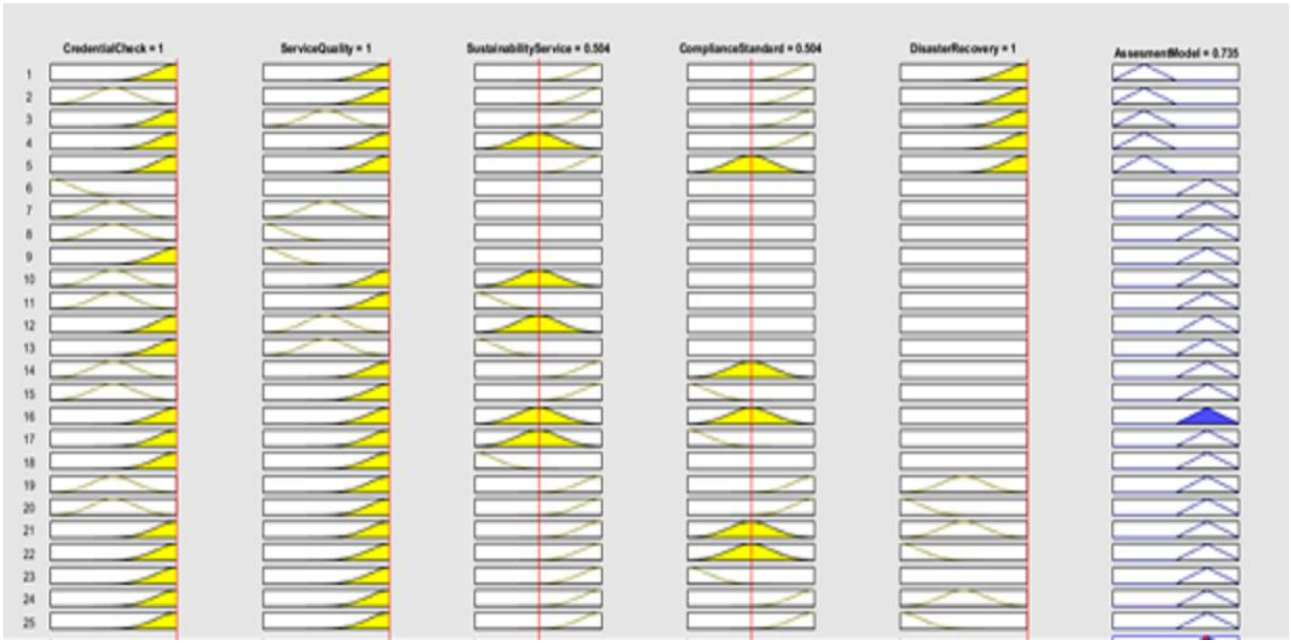


Fig: 10

Compliance of Standard: This standard has three input value namely high, medium and low. In figure8 and figure9, for the parameter CS-right if input specification high and medium if all other following parameter input specification is high then the assessment model is accepted otherwise rejected. Similarly In figure8 and figure9, for the parameter CS-left if input specification high and the following parameter input specification is also high then the assessment model is accepted otherwise rejected.

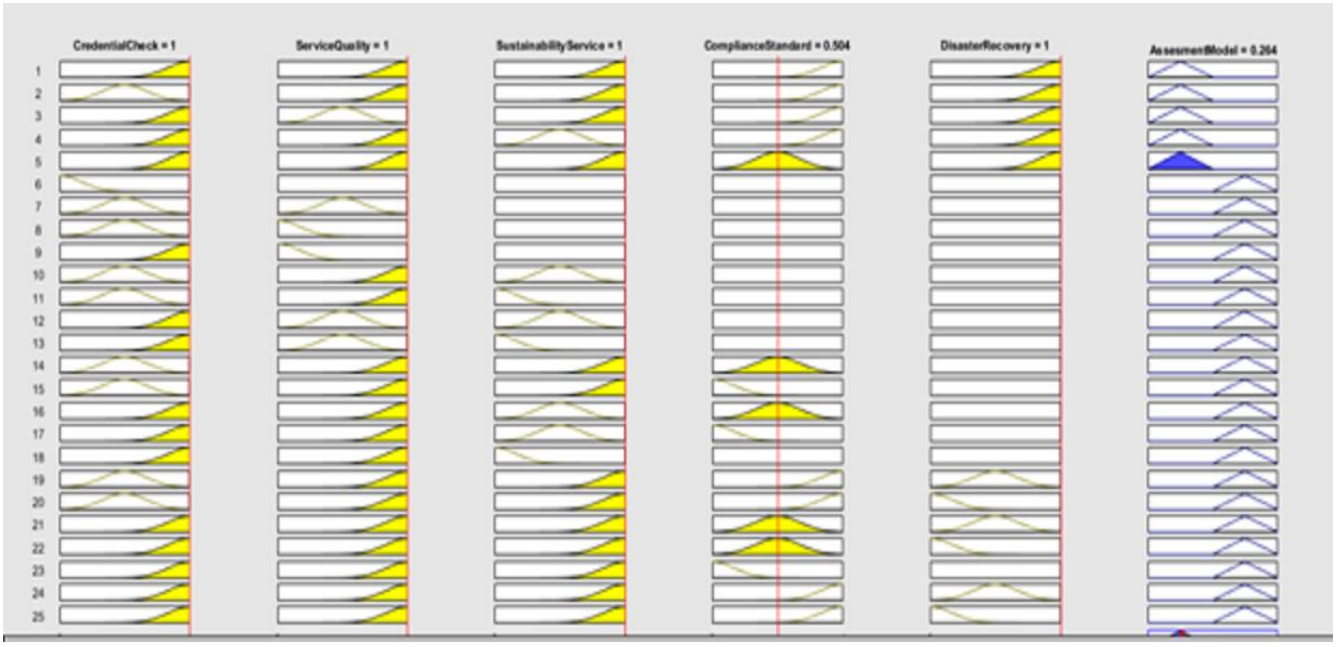


Fig: 11

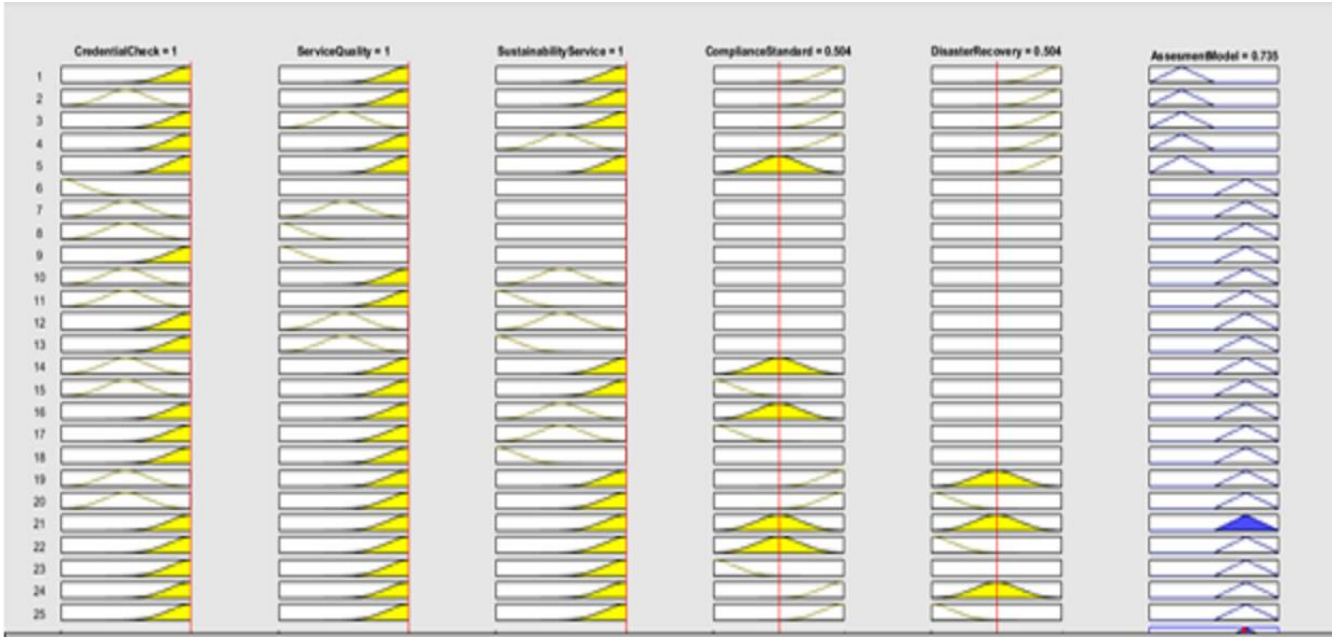


Fig: 12

Disaster Recovery: This service has three input value namely Strong, medium and weak. In figure13 and figure14, or the parameter DR-right if input specification strong then the assessment model is accepted otherwise rejected. Similarly in figure10 and figure11, for the parameter DR-left if input specification Strong then the assessment model is accepted otherwise rejected.

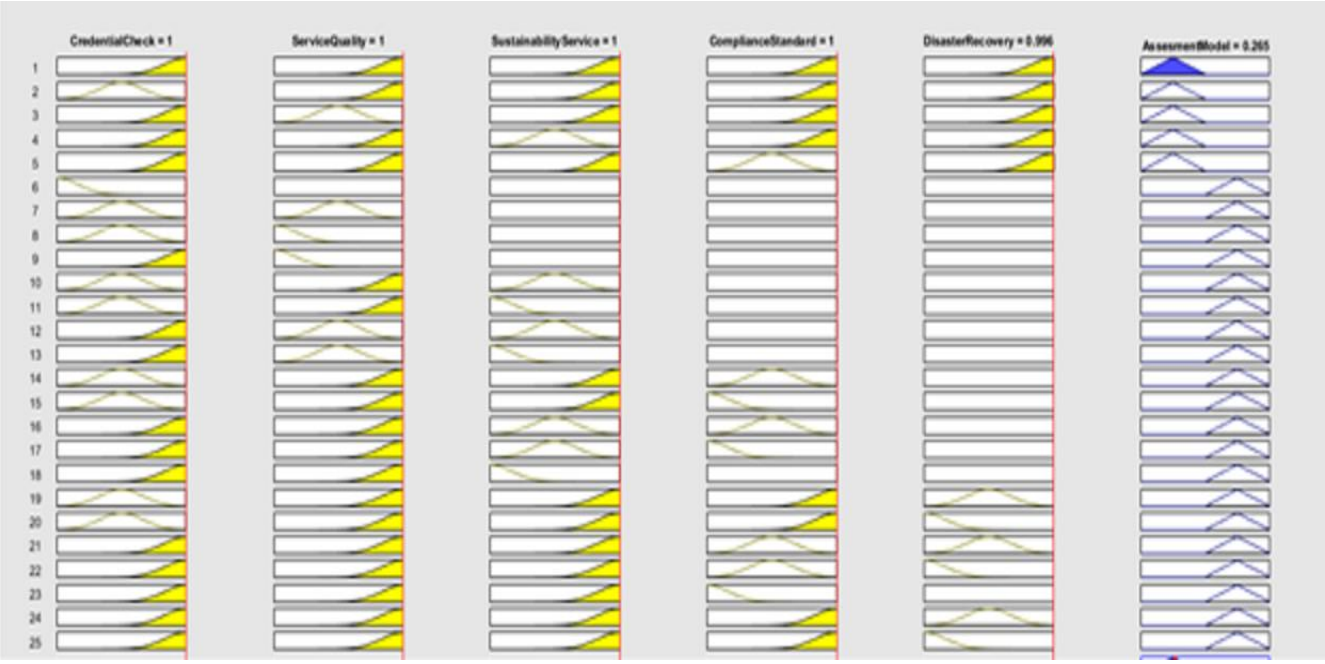


Fig: 13

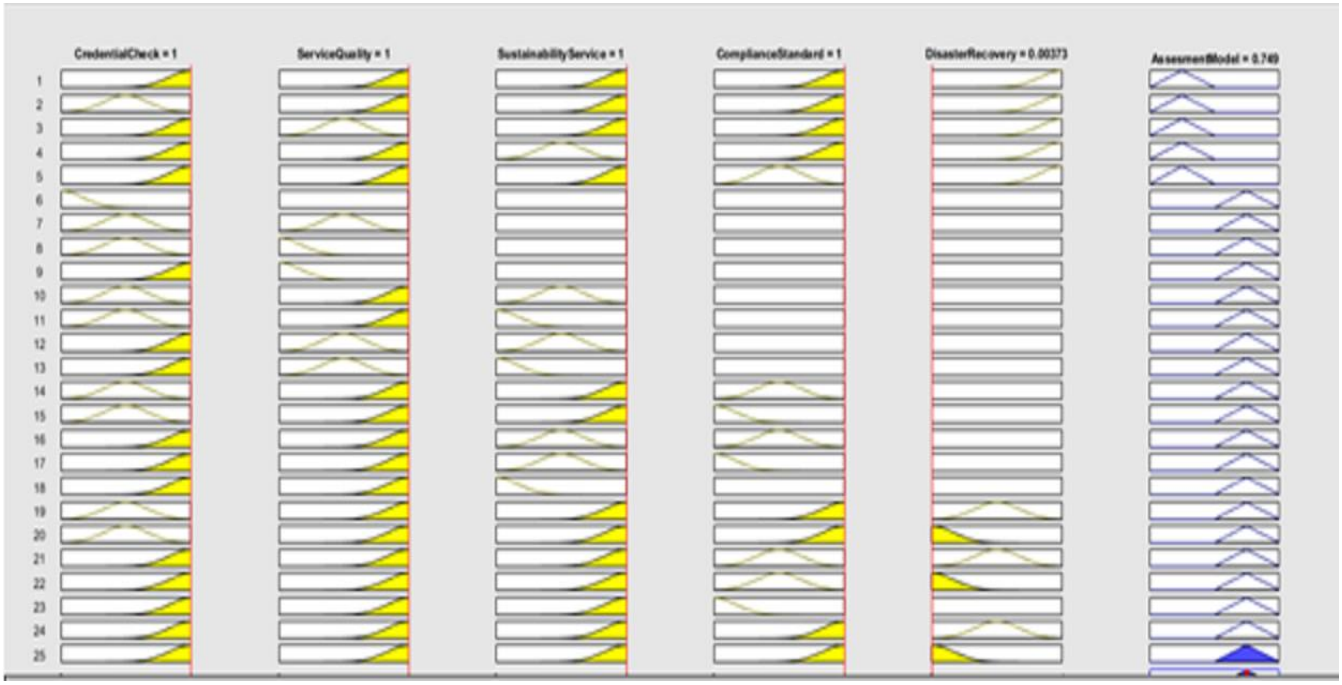


Fig: 14

BIBLIOGRAPHY

FOR TRUST

References

A. Cuomo, G. Di Modica, S. Distefano, A. Pulito, M. Rak, O. Tochio, S. Veque, and U. Villano, "An SLA-based broker for cloud infrastructures,"Journal of grid computing, vol. 11, no. 1, pp. 1–25, 2013.

B. [2] B. Calder, "Inside windows azure: the challenges and opportunities of a cloud operating system," in ACM SIGARCH Computer Architecture News, vol. 42, no. 1. ACM, 2014, pp. 1–2.

C. Sato, M. (2010). Personal data in the cloud: A global survey of consumer attitudes. Minato-ku, Tokyo 105-7123, JAPAN.

Websites

A. http://www.forbes.com/sites/niallmccarthy/2014/08/26/chart-thebiggest-Data-breaches-in-u-s-history/

B. http://www.nw3c.org/docs/research/criminal-use-of-socialmedia.Pdf?Sfvrsn=6

FOR TSLA

References:-

1. A. Cuomo, G. Di Modica, S. Distefano, A. Pulito, M. Rak, O. Tochio, S. Veque, and U. Villano, "An SLA-based broker for cloud infrastructures,"Journal of grid computing, vol. 11, no. 1, pp. 1–25, 2013.

2. B. Calder, "Inside windows azure: the challenges and opportunities of a cloud operating system," in ACM SIGARCH Computer Architecture News, vol. 42, no. 1. ACM, 2014, pp. 1–2.

3. E. M. Maximilien and M. P. Singh, "A framework and ontology for dynamic web services selection," Internet Computing, IEEE, vol. 8, no. 5, pp. 84–93, 2004.

FOR FUZZY IMPLEMENTATION

Reference:-

Fig: 11

[1] Alexander Stanik, Fridtjof Sander & Odej Kao(2014). "Autonomous Agreement-Mediation based on WS-Agreement for improving Cloud SLAs". 2014 IEEE 6th International Conference on Cloud Computing Technology and Science.

[2] Jingwei Huang and David M Nicol(2013). Trust mechanisms for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications* Advances, Systems and Applications2013.

[3] Albert S. Horvath III, Rajeev Agrawal (2015). "*Trust in Cloud Computing" A User's Perspective.* Proceedings of the IEEE SoutheastCon 2015.

Website

https://www.ibu.edu.ba/assets/userfiles/it/.../eee-Fuzzy-5.ppt *Fuzzy Inference Systems.*

CONCLUSION

We have studied SLA-based resource management in cloud computing where trustworthiness, percentile response time, and availability are considered as our QoS metrics. We have first proposed an approach for SLA-based resource management and provided an illustrative example to demonstrate how the proposed approach is used for solving the SLA-based resource management problem in high performance cloud auditing. We have solved the SLA-based resource management problem using an efficient numerical procedure. Our numerical validations have showed that our proposed algorithm has reached a good accuracy. Customers need to trust on cloud dependability. Making relevant information available to them may help aggregating value to cloud solutions, promoting guidance for SLAs' negotiation, and contributing to consolidate cloud services into critical information-dependent economic sectors.

Evaluation of different service parameters and assessment of their compliance is an important task in cloud computing scenario. Presently no such effective and generic model is available in the literature which can work across different cloud deployment model. Most of the available models are even service centric. Design of a generic automated evaluation and assessment of cloud SLA was the objective of this present work. Accordingly a Turing based service level agreement assessment model for all types of cloud deployment is proposed through this work. Various aspects of service level agreement assessment are short-listed and defined in this work to develop the set of rules for compliance checking. These rule set are augmented with a couple of definitive classifier. Finally the rule set was used to develop a Turing model for SLA evaluation. These Turing transitions are finite and unambiguous.

We did a survey to measure consumer trust in cloud computing. What we found is that consumers trust cloud computing more than they admit to even themselves. They trust only to the extent that the risk is perceived to be low and the convenience payoff for them is big. There still is a problem with consumer trust and it is beneficial for consumers and industry to come to an agreement where the Internet becomes more useful to the consumer and the consumer becomes more profitable for industry. Ultimately, the information gathered would produce a model or best practices for Internet businesses to use for improving sales. This model would ideally also improve security for consumers.

LIST OF TABLES

There are 6 tables in our project report.

Numbers of tables with Specification are given below:

LIST OF FIGURES

In our project report we gave 14 figures. These are as follow: