A Trust Model in cloud computing based on Fuzzy Logic

Reflective Diary and other Document submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Information Security

Submitted by

Ritu

(801433023)

Under the Supervision of

Dr. Sushma Jain

Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

June 2016

Certificate

I hereby certify that the work which is being presented in the thesis entitled, "*A Trust Model in Cloud Computing based on Fuzzy Logic* ", in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Information Security* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Sushma Jain* refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Ritu
(Ritu)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Sushma Jain)
Assistant Professor,
CSED

Countersigned by

Deepak Garg 13/5/16

(Dr. Deepak Garg)
Head
Computer Science and Engineering Department
Thapar University
Patiala

(Dr. S. S. Bhatia)
Dean (Academic Affairs)
Thapar University
Patiala

Acknowledgement

During the course of this thesis I have been lucky to be blessed by a lot of kind people. Let me take a moment to thank each one of them.

To begin with, I am thankful to God for his blessings and for consistently showing me the right direction.

I wish to express my sincerest gratitude towards the guidance and help that I have received from my supervisor Dr. Sushma Jain. I shall ever remain indebted for her consistent support and encouragement. She provided me help whenever needed, and also arranged for me the resources required to complete this thesis report on time.

I am also thankful to Dr. Deepak Garg, Head, Computer Science and Engineering Department, Thapar University for his help and cooperation. Along with that I express my gratitude to all the staff and faculty members of Computer Science and Engineering Department, Thapar University for providing me with the facilities required for this thesis.

I would like to thank all my friends especially Anita for their support. Also I want to express my appreciation to every person who contributed with either inspirational or actual work to this thesis.

Last but not the least I am very grateful to all my family members for their inspiration and moral support which kept me motivated to pursue my studies.

Ritu

Ritu

Abstract

It is common to hear organizations-big or small are moving to cloud computing for its scalability and cost savings. But, how do you decide which cloud provider to trust? Trust is a vital factor, especially for service oriented systems in the area of Information Technology and Security. Several issues have been raised by enterprises and individuals concerning the reliability of the cloud resources. In cloud computing, trust helps the consumer to choose the service of a cloud provider for storing and processing their sensitive information. In this thesis, a trust model is proposed which uses Quality of Service parameters (QoS) to evaluate trust. The fuzzy nature of trust has encouraged us to use fuzzy logic to calculate trust value of a provider in a cloud environment, thus increasing the effectiveness of the system. QoS parameters such as turnaround time, availability and reliability are taken for trust evaluation.

The proposed model has been simulated using CloudSim and NetBeans IDE. Experimental analysis of the proposed approach has proved the better efficiency of the system. A comparison of the proposed model and weighted model is also presented.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

The developments of storage and processing technologies have made the computing resources cheaper and easily available. In past few years, the technology has made the lives of people very easy by making the services accessible anytime and anywhere. So many profitable and educational institutions have made large systems from commodity computers, storage disks, and networks to make the hardware easy to manage and use.

1.1 Cloud Computing

Cloud Computing [1] connects huge number of systems in a network: private or public. It gives us highly scalable framework for storing data and applications. After arrival of this kind of computing, the price of computing power, web hosting, data and delivery reduced remarkably. Cloud computing provides direct price profits and it has the ability to convert a data center from an investment-intensive setting to a variable priced setting.

The notion of cloud computing is dependent on a very elementary principal of "reusability of IT resources". The difference that cloud computing has brought in comparison to conventional notions of grid, distributed and utility computing is to widen horizons across organizational limitations. Cloud computing divides the role of cloud service providers in two categories: the providers that organize the platforms and rent their resources such as memory, Vm, bandwidth etc. according to pay-per-use model of pricing, and the service providers that lease their cloud resource from various cloud providers to end users. Computing has been transformed into commodities which are delivered alike to services such as water supply, house electricity, gas, and telecommunication. In this kind of model [2], customers or cloud users access cloud service applications based on their need without considering the location and method of delivery of these services. A number of computing standard have assured to bring this Utility Computing idea and these include Grid computing, and now-a-days Cloud computing.

Cloud computing helps businesses and users to use cloud applications from anyplace on demand. So the computing world is swiftly changing towards emerging software

applications for millions to use as an application service, rather than running on their personal computers. These days it is usual to access data across the Internet autonomously without reference to the basic hosting infrastructure. This infrastructure consists of monitored and maintained data centers given by data providers. It is an extension of this idea in which the abilities of applications involved in business are computing services that are accessed over a network.

Though, since cloud applications may be important to the core business operations of the clients, it is necessary that the customers have guarantees of service delivery by providers. SLAs provide this guarantee between the service providers and customers. Some service Providers such as Amazon, Dimension data, Google, Salesforce, IBM, iWeb, Microsoft, and Sun Microsystems have started to launch new data centers for hosting applications of cloud computing in different locations around the world to offer redundancy and guarantee reliability in case of site failures.

As the requirements of cloud services are variable in nature, service provider's needs to guarantee that they are flexible in delivery of resource services while protecting the users from the underlying infrastructure. Latest advancements in microprocessor technology and application software have led to the increasing capability of service hardware to execute applications within Virtual Machines in efficient way.

VMs permit both the isolation of cloud applications from device hardware and other VMs. Providers depict applications running within virtual machines, or give access to VMs themselves as a cloud service and allowing clients to install their personal applications. The use of VMs increases additional encounters such as the intelligent resource allocation of physical cloud resources for managing demands for competing resource of the users.

Regardless of the quick development of Infrastructure-as-a-Service (IaaS,) techniques such as Amazon EC2 1 service, Microsoft Azure 2 service, and services offered by RackSpace 3 and other services, IaaS services continue to be beset by vulnerabilities at many levels of software stack, also to leakage of information, to collocated malware infected VM instances. The need for protected cloud storage has been recalled on many occasions.

For example, in [3] the author has cited industry decision takers to highlight the fact that security concern is one of the major factors that prevent business entities from deploying their organization's data and computations. General reasons are deficiency of knowledge of the status of the data and computing algorithms and procedures as

soon as it is in the cloud setup, as well as concerns about cloud provider liquidation and successive unclearness and recognized procedures of data safety and retrieval.

The reasons for this include both practical, e.g. distress of data leakage, data infringement and data modification as well as organizational, such as destroying reputation. In this condition, a danger is there that the economic profit obtained through the fast pace adoption of cloud service technologies will in some cases be rewarded or even over compensated by data losses resulting from unpredicted lack of accessibility as well as theft and destruction of data.

1.1.1 Cloud computing Evolution

The concept of Cloud Computing was introduced in 1950 along with application of mainframe computers, available via static cloud clients.

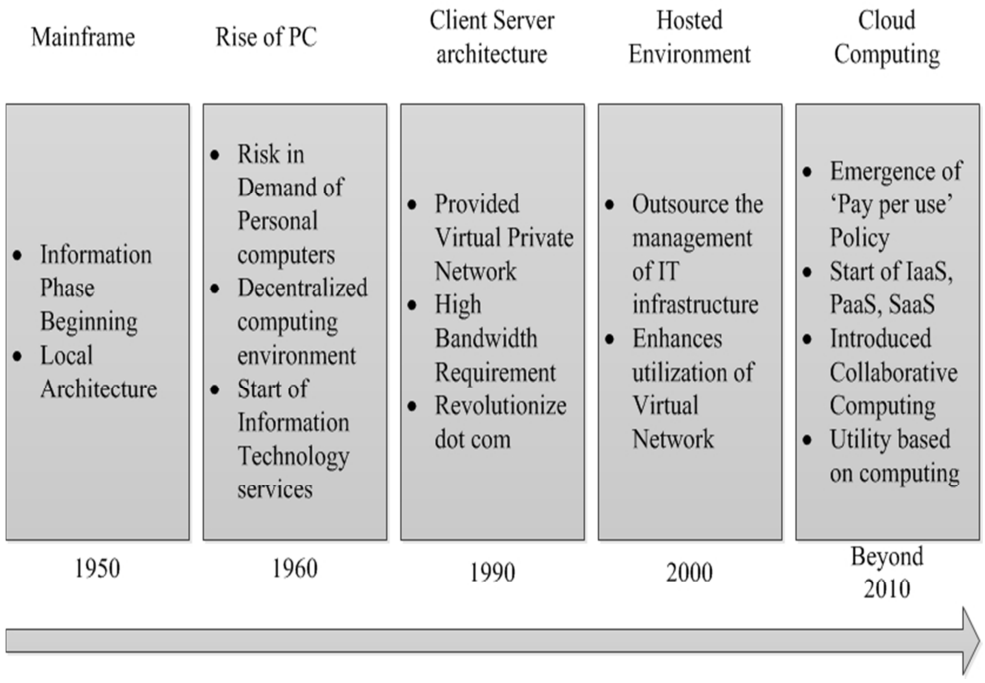

Figure 1.1 Evolution of Cloud Computing

Since then, this type of computing has been progressed from fixed clients to dynamic clients and from computing software to computing services. The figure 1.1 has explained the progress of cloud computing till now.

1.2 Architecture of Cloud Computing

This segment defines various models of cloud computing related architecture, business and operational [4].

1.2.1 Layers of cloud computing

The structural design of cloud computing is described in 4 layers: the hardware layer, the infrastructure layer, platform layer, and the application layer, as shown in Fig.1.2. The description of each of them is as follows:

- ***The Hardware Layer*:** The main responsibility of this layer is to manage the physical assets of cloud which includes physical data and application data servers, network routers, connecting devices, power source and cooling systems. Practically, the hardware layer works on datacenters. A datacenter typically comprises of thousands of cloud servers structured in shelves and connected with each other through network switches, network routers or other connecting material. Come time consuming and complex issues in this layer are the configuration of hardware, fault tolerance, data traffic control, power utilization and managing cooling source.
- ***The Platform Layer*:** It is the third layer from bottom; the platform layer consists of application frameworks and operating system files. The task of this layer is to reduce the trouble of application deployment in VM containers presented in the cloud. For example, Google App Engine (GAE) runs on this layer to provide support for APIs for implementing storing, storage and business logic of distinctive web applications.
- ***The Application Layer*:** This layer resides on top of the architecture. This layer contains actual applications of cloud. Different from conventional applications, the applications resides on cloud controls the automatic-scaling aspect to achieve increasing performance, accessibility and lower usage cost for resources provided. The design of cloud computing is more flexible than the traditional cloud hosting settings such as dedicated data and application server farms.

  Every layer is loosely united with the layers exist above and below it, and by doing so it allows every cloud layer to progress distinctly. This is similar to the model of the OSI network protocol model. The architectural flexibility allows cloud computing to support a broad range of application requirements while minimizing management and maintenance overhead of the system.
- ***Infrastructure layer*:** It is also called virtualization layer; the cloud infrastructure layer makes large storage space and cloud resources by separating the physical

cloud resources by using virtualization techniques such as VMware, Zen and many others.

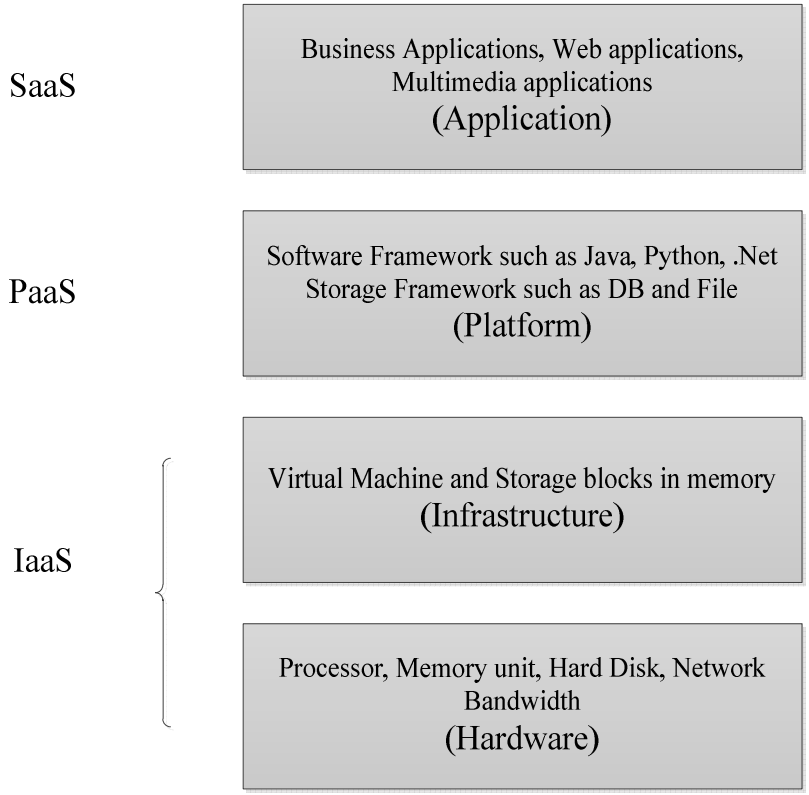

Figure 1.2 A layered modeling architecture of cloud computing

The infrastructure layer provides many important aspects, such as dynamic resource allocation which are only made accessible using virtualization technologies.

1.3 Characteristics of Cloud Computing

Various outstanding aspects that are different from conventional computing technologies are summarized below:

- ***Multi-Tenancy*:** The cloud services provided by different cloud providers are located on one datacenter server. The service and infrastructure provider shares performance, efficiency and management issues of these services. The layered structure of cloud offers a regular partition of service responsibilities: the owner of every layer only needs to concentrate on the specific objectives related with this layer. On the other hand, multiple tenancies also face problems in understanding and handling the communications between different investors.

- ***Resource Pooling Facility*:** The cloud providers allocate the resources which can be employed to different cloud users in dynamic way. This facility lets the provider to give extra flexibility. It facilitates the provider to manage to create resource utilization and cost of operation. For illustration, an IaaS provider can influence VM relocation technology to accomplish better server consolidation, thereby maximizing utilization of resource while decreasing cost such as cooling and power utilization.
- ***Universal Access*:** Such computing provides universal access on the internet and us the features of internet to deliver the services to different users. Many devices connect with the cloud system such as mobile phones, tablets, and laptops to access its services. To get better network efficiency and performance, data centers are located on network on different geographical locations. Cloud providers enhance service utilization using this facility.
- ***Service Oriented*:** Being a service-driven network model, Cloud computing focuses more on management of services provided in cloud. Every layer of lcoud computing provides its services in accordance with the SLA generated between two parties. This is a reason of cloud provider giving more important to SLA document.
- ***Dynamic Resource Provisioning*:** An important property of cloud computing is that cloud resources are accessed and freed on the fly. In comparison to the conventional model that supplies computing resources according to high demands of users; this mechanism allows service providers to gain on-demand, which significantly lowers the cost of operation.
- ***Self-Organizing*:** As resources are allocated according to user's demand, service providers can manage the consumption of resources with respect to their own requirements. Additionally, the automatic resource management aspect of cloud computing gives high quickness that facilitates cloud service providers to respond rapidly to frequent changes in cloud service demand i.e. the effect of flash crowd.
- ***Pricing based on Utility*:** The cloud computing uses pay-per-use model for pricing resources. The precise pricing scheme varies from service to service for different cloud providers. For instance, the service provider can charge for any resource it provides to any cloud user on per hour basis. This feature of cloud

computing offers better service operating rate. It also imposes complexities to control the cost of operating a service.

1.4 Cloud Computing Models

Cloud Computing follows a service based business model which means that the hardware and platform level cloud resources are provided by the cloud provider as services. Conceptually, each layer of this architecture is employed as a service of cloud to the layer above it. Conversely, each layer is perceived as a user of the layer below.

1.4.1 Service Models

Though, in practice, cloud offers three categories of services which are explained below:

a) Infrastructure as a Service (IaaS)

This model facilitates the costumer with the ability to provision processing, storage space, networks, and other elementary computing resources, and allows the end user to set up and run random software, which comprises of operating systems and applications.

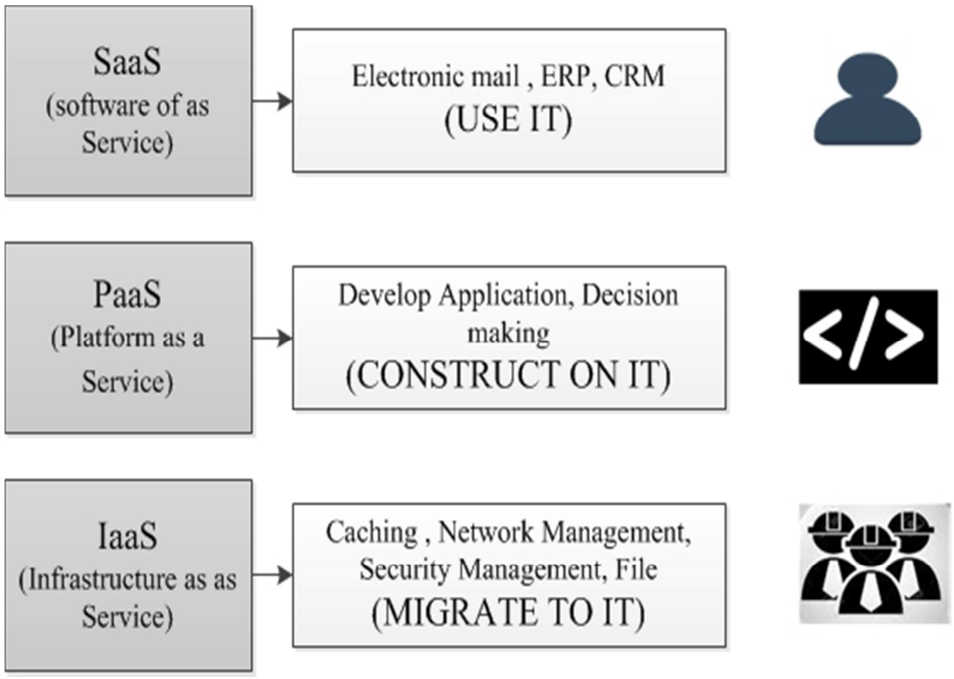

Figure 1.3 Service Models of Cloud

The end user has regulation over computer operating systems, storage, mounted applications, and limited control of particular components of networking.

Examples of cloud infrastructure providers are Amazon EC2, Dimension Data, GoGrid and Flexiscale.

b) Platform as a Service (PaaS)

It facilitates the customer to set up onto the infrastructure of cloud, the applications developed or acquired by user, produced with programming languages and application building tools supported by the cloud provider. The end user does not control or handle the core cloud infrastructure including network, data servers, operating systems, and storage space, but has regulation over the deployed cloud applications and possibly application that hosts. Google App Engine (GAE), Microsoft Windows Azure (MWA) and Force.com are few examples of PaaS providers.

c) Software as a Service (SaaS)

This type of service model provides on-demand applications anywhere on Internet. Salesforce.com, Rackspace3 and SAP Business by Design are a few examples of SaaS providers. The cloud business model is depicted by Figure 1.3. According to the cloud design, it is absolutely possible in cloud that a PaaS service provider executes its cloud above IaaS. This is reason that the PaaS and IaaS providers are repeatedly called the Platform Providers and infrastructure providers.

1.4.2 Deployment Models

Different cloud models are explained below:

***a) Public Clouds*:** In this kind of deployment model, the resources provided by the service providers are in the form of services. Public clouds provide many important benefits to the providers which include no starting cost on service infrastructure and passing of threats to infrastructure cloud providers. Nevertheless, public clouds don't provide complete control over information, protection and privacy settings that restrict their efficiency in various business scenarios.

***b) Private Clouds*:** Private clouds are internal clouds; these are designed exclusively for single organization. This type of cloud can be constructed and coped by the provider party. A private cloud control performance, reliability and security.

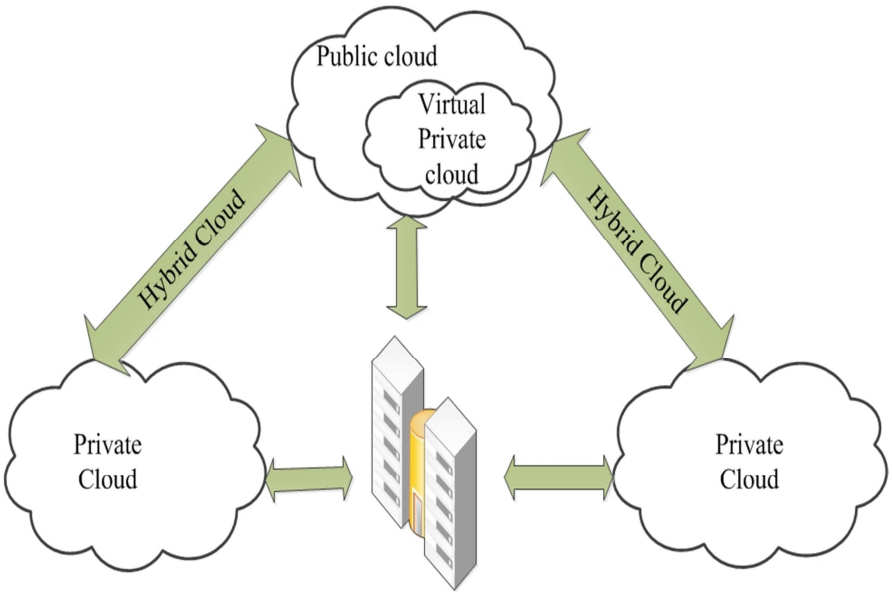

Figure 1.4 Deployment Models in Cloud

c) ***Hybrid Clouds*****:** A hybrid cloud combines public and private types and tries to express limitations of both. In a hybrid cloud, private clouds runs service infrastructure while the other parts run by public clouds. This cloud is more flexible than the private and public cloud.

d) ***Virtual Private Cloud*****:** It is an alternate solution to deal with the shortcomings of both public and private clouds. It is implemented on the top level. Such model is effective in architectural model because it can virtualize the application servers.

VPC is principally a extra effective in design because it virtualizes servers and applications. This model has the feature to unbroken transition in cloud network which gives better performance. It lets the providers to delop their personalized topology and network settings related to security. It can also customize firewall settings.

1.5 Cloud Computing Risks

Although Cloud Computing is the fastest growing technology in computing world, there also exists some disadvantage or cons of cloud computing [1]. Some of them are explained below:

- **Security and Privacy**

  The biggest problem in cloud computing is the security of data stored on cloud. The reason is that the data control and infrastructure is provided by the third party. The involvement of third entity creates the risk of data theft and security loopholes. While the provider of cloud resources assured extra security and

authentication methods, any indication of violation to security would lead to decreased number of cloud clients.

- **Lock-In**

  The switching between one cloud providers to the other is not an easy task.

  It is not easy for the clients to switch from one CSP to the other. It makes the clients dependent upon a specific CSP for a service.

- **Failure of isolation**

  This risk consists of the breakdown of isolation mechanism which separates storage space, memory, routing technique between different occupiers.

- **Management Interface**

  Public cloud providers provides interface which is accessible through internet.

- **Unsafe Deletion of Data**

  It is likely that the data which the user has demanded for removal may not get removed. It happens because of two reasons; extra copies of cloud data are stored but not existing and second that the storage disk destroyed also stores user's data from other consumers.

1.6 Trust in Cloud

Trust comprises of three factors; Expectancy, belief and willingness to take risks. Trust in cloud computing is a measure of reputation of the specific cloud provider which has some set of resources for users. Trust in cloud plays a vital role to make the cloud business grow and the provider can get more profit. To make the provider trustable, some criteria is needed to help the user in selecting a provider.

1.6.1 Trust Semantics

Trust is frequently utilized in the writings on Trust in cloud, often as a common term for "privacy" and "security" [5]. What is the meaning of the term "trust"? It is a multifaceted social phenomenon. Based on social science trust, we have used the following definition:

It is a state of mind comprising:

(1) Expectancy - It is the expectation of one party from another participating party (such as providing legal content or efficiently performing cooperative procedures);

(2) Belief - the trustor considers that the behavior he has expected would occur, dependent on the information evidence of capability of the trustee, reliability, and helpfulness;

(3) Willingness of Risk taking - for that belief the trustor is prepared to take risk.

It is essential to note that the trustor cannot control the expected behavior of trustee; the trustor's faith in those predictable actions of trustee is dependent on the ability of trustee, capability, and integrity. The truthfulness of the trustee provides the trustor assurance with reference to the expectedness of the trustee's behavior. In cloud computing two kinds of trust have been identified, based on the expectancy of trustor: the *trust in performance* tells about performance of the trustee, but, the *trust in belief* is trust comprised of trustee's belief. The performance of trustee could be what the trustee claim or the successfulness trustee's actions. Trust in performance and trust in belief are related to each other.

Trust in belief is transitive in nature; *trust in performance* is not; though, *trust in performance* is broadcasted through *trust in belief* [6, 7]. From the above definition, the trustor's belief depends upon the evidence related to the trustee's capability, truthfulness, and concern. This leads to rational structures of interpretation from belief in proof to faith in expectancy. This is the basic idea behind trust in cloud computing. Now, we will discuss about different categories of trust in Cloud computing.

1.6.1 Types of Trust

I) Basic Categories of Trust

a) Direct Trust

Direct trust comes into picture when an entity estimate for another based on previous experiences.

b) Indirect Trust

Indirect trust is the trust in which one entity trust another entity based on the recommendation of any third entity.

II) Classifications of Trust

The trust in cloud computing is divided into two categories explained below:

a) Reputation Based Trust in Cloud

Reputation and trust are related to each other, but also different. Fundamentally, trust is between two parties; but the status of an entity is the collected estimation

of public towards that entity. Generally, many individuals in that community trust an entity that has high reputation; an entity, which is required to build trust decision on a trustee, uses the reputation to compute or approximate the trust level of the trustee. These systems are commonly applied and utilized in electronic commerce and Peer-to-Peer networks. The reputation of cloud affects the selection process of services on cloud; therefore, cloud service providers try to construct and preserve higher reputation. Logically, reputation-based trust move into the idea of making trust decision in cloud computing system.

Reputation is classically characterized by a broad mark reflecting the complete outlook, or a lesser quantity of marks on various foremost aspects of performance. It is not a good solution to enquire a large group of users to give rating to a cloud service in opposition to a huge set of fine-grained criteria. Repute is useful when initially choosing a cloud service, but is not completely enough subsequently. Specifically, when the user uses the service of a cloud provider then it gains some experience and trust on that provider.

b) SLA Verification based Trust

To deal with relationships between user and cloud providers, there must be trust and verification between both the parties. After launching the preliminary trust technique and accessing a cloud facility, the cloud user is required to validate and re-examine the trust value. An SLA is a lawful agreement between the two communicating parties, the user and the provider. Therefore, monitoring the Quality of service (QoS) and verification of SLA document are essential source of trust management in cloud computing scenario.

Some prototypes that obtain trust from SLA document verification have been suggested. A most important matter is that SLA gives importance to “visible” cloud components of cloud computing service performance, and does not concentrate on “invisible” ones such as privacy and security. Another problem is that several cloud users lack the potential to do excellently grained QoS monitoring process and SLA verification; a third cloud provider party is required to provide these types of services.

A cloud broker is there, which is trustworthy in the confidence area of the private cloud; therefore, the cloud user gets such a facility. A cloud user inside a private cloud might still depend upon the trust authority of private cloud to accomplish Quality of Service observing process and SLA confirmation;

conversely, cloud users and some low sized organizations without technical competence may use a commercial certified cloud entity as their trust broker, in a public cloud.

c) Policy-based Trust

In cloud computing, it is required to construct a "formal". In a related area, PKI (Public Key Infrastructure) is an extensively used established technoique that utilizes "formal" trust methodologies to support key certification, digital signature, and validation. It also supports data attribute certification and validation.

As PKI is currently used in practice, in this the trust in a CA (certification authority) is dependent on the CA's confirmation with definite certificate policies. It is taken w.r.t to delivering and retaining public key certificates which are validated. License guidelines are main role in PKI trust. Such trust mechanism is called as *policy-based trust*. Some policy must be imposed on the participants.

d) Evidence-based Trust

A belief of trustor in the predictable behavior of trustee entity is based on the proof about attributes of adeptness, helpfulness, and honesty, w.r.t that expectation evidence-based trust is expressed as follows:

*believe(c, attrb*1*(sb,* a*v*1*))*∧... ∧ *believe(c, attrbn(sb,* a*vn)) → trust_ * (c, sb, x, ct)*

which states that if a cloud user *c* considers a subject *sb* has attribute *attrb*1 with value a*v*1, ..., attribute *attrbn* with value a*vn*, then *u* trusts (it is either *trust in belief* or *other one*) b*s* w.r.t *x*, the performance of *sb* or information believed by *sb*, in a particular context *ct*.

e) Societal Trust

Societal trust consists of any individual and a company. Just as in society, each individual has to maintain trust in some important parts of the social entities; In cloud also each entity must be trusted. In Information security service sector, trust plays a vital role between the supplier and the client to help the business grow.

1.7 Fuzzy Logic

Fuzzy logic was introduced by researcher Zadeh in 1965 [8]. Since then; it has been used in various classification fields and control applications. Fuzzy set consists of following components and procedures:-

- **Crisp set**

  In a crisp fuzzy set, any data element either exists in the set or not. It is a real value or variable. For example, a jelly bean belongs to food class which is known as candy. But, mashed potatoes do not belong. It is taken as an input variable for fuzzification process.

- **Fuzzy sets**

  Fuzzy sets permit elements to be *partially* in a set of elements. Every element is specified as an extent of fuzzy membership in a set. This value of fuzzy membership ranges from "zero (0)" (non-member of the fuzzy set) to "one (1)" (member of the fuzzy set). It is visible that if extreme membership value of 0 and 1 then that would be called as crisp set.

- **Membership Function in Fuzzy**

  A Fuzzy membership function is the association between the values of an existing element in the set and its membership degree in a set. The sets are large, medium, small, and near zero in nature. The value, μ, represents the amount of fuzzy membership in the set. Membership function lies in the range 0 and 1.

$$\mu_A(x) \in [0, 1]$$

  For crisp sets,

$$\mu_A(x) = \begin{cases} 0, & if \quad x \in X \\ 1, & otherwise \end{cases}$$

- **Fuzzification**

  It is the method of altering a real value into a fuzzy set value. This is done with the help of different types of fuzzifiers (also called membership functions).

- **Defuzzification**

  It is the reverse process of fuzzification. It generates crisp values form fuzzy sets. This process is used to find crisp value in fuzzy logic.

- **Rule Based System in Fuzzy**

  A fuzzy rule based system is defined a collection of proportions which contains linguistic variables and the rules are represented in the form of: If X_1 is A_1, X_2 is A_2 ……, and X_m A_2 then Y is B.

1.8 Structure of Thesis

The structure of the thesis is planned as follows:

Chapter 2: This chapter includes the literature survey which involves evolution of Trust models in different computing techniques. It has also contained the work of many researchers in the area of cloud computing and fuzzy logic.

Chapter 3: Thesis background, problem statement**,** and objectives of proposed work are explained here.

Chapter 4: It consists of the proposed work which involves the fuzzy based trust model using Quality of Service parameters.

Chapter 5: This chapter consists of the evaluation parameters and the results obtained via simulation and its comparison with other works.

Chapter 6: It includes the conclusion, summary and future scope of the work proposed in this thesis.

Chapter 2

State of Art

In this chapter trust management and its technologies are discussed. Trust models in grid, cloud and ad-hoc networks are discussed. Fuzzy logic and models based on fuzzy are also discussed.

2.1 Trust and Trust Management

Firdous *et al.* [9] and Han *et al.* [10] have studied that the status and trust have originated from society which studies the pattern of human behavior. Zaobin *et al.* [11] have explained the relationship among various entities of social network in trust management system. Trust is analyzed by examiners in various fields such as human psychology, sociology and business economics. McKnight and Chervany [12] have elaborated that trust is a mental outlook which focuses on the effects of trusting and not trusting someone. Trust is a social relationship between people in the society. Paoli *et al.* [13] and Akhoondi *et al.* [14] have explained that the social outline of trust is commonly used in multi user systems and social networking. Economic experts recognize trust with regard to usefulness. Huang *et al.* [15] and Mui [16] have explained that the scientists in information technology have utilized the advantages of all these research as they offer critical vision of human mind. The computing technology researchers have studied trust in various fields such as distributed systems (public e-commerce), open, peer to peer networking , cloud computing , semantic web technology, cloud computing, web services, and mobile networks. Though there has been various studies done on trust; it has also increased the complexity of trust in several areas of computing. The thought behind this is that there is no common description of trust in cloud computing such as beliefs, outlook, possibilities, expected behavior, honest quotient and so on.

Some common descriptions of trust are:

- Trust comes into picture indecisive and risky environment.
- Trust is based on past decision made during different situations.
- Trust can be developed on the basis of previous experience and prior-facts.
- Trust is a subjective which is opinion dependent.

- Trust varies according to time and new entries of facts while practice will have overruling control over the old knowledge.
- Trust is dependent on context w.r.t system.
- Trust is multi-talented.

McKnight and Chervany [12] have recognized 16 aspects of trust which are classified as follows

- proficiency; capable, skilled, dynamic
- expectedness; predictable
- generosity; first-class (or moral), caring, responsive
- reliability; truthful, plausible, consistent, loyal
- Other; direct, cautious, common understanding, personally smart .

De Oliveira and Maziero have categorized relationships of trust into social networks, hierarchical trust, and social groups. Zhang *et al.* [17], have divided trust into following categories.

- Rank-based vs. Threshold-based
- Complete information vs. Local information
- Transaction-based vs. Opinion-based
- Subjective trust vs. Objective trust

2.1.1 Trust Management Requirement

In this section, prerequisite of an efficient trust management system are given.

a) Accuracy of Information

Chong *et al.* [18] have explained that precision of facts and information is known as accuracy of trust which means that the computation of trust is accurate at estimation time. There is no power on correctness of the value of trust provided by the trust management system. So much of information was needed to evaluate the value of trust in a network system. This set of information could be misleading or false in nature to make us trust the service provider. Correct calculation of trust was important because it has enhanced the relationship between service provider and its consumers. It has also helped to improve the business of e-commerce websites in which trust is the crucial factor. Also, the incorrect information has led to false business conclusions which results in low quality verdict and outcomes. Trust has been improvised by sharing the experience of users about the quality of service

offered by different providers. This was why the user needed the guarantee of the information validness to trust that particular provider. The issue in providing accurate trust to users was that the data of trust was excessively common. It did not indicate the required trust information by the user but it gave a single value as a trust value. Transactions have taken as applicable when computing trust value related to a new transaction. For instance, a service provider may be excellent in one service but not so good in other service. Hence the earlier transaction was taken as one of the parameter in evaluating trust. Trust computation needs much information such as trust value of different services provider by different service providers. E-commerce also has faced the problem of consistency of trust evaluation system. False and biased ratings may affect trust evaluation. The purpose of false rating is to increase or decrease a supplier's reputation. False feedbacks may affect the reliability of the trust system and level of trust of service provider. Most vulnerable system to false ratings is e-commerce where anybody can temper with ratings.

For instance, the cause of bad quality of trust level could even be a small amount of false information. Hence the overall reputation of the provider will get affected and trust system becomes unreliable. As it is impracticable to anticipate all ranking providers to supply genuine assessments in an open atmosphere such as e-Commerce, it is essential to have an approach that is proficient to identify false ratings to defend the truthfulness of the trust system. Hence a process is needed which can identify and check the false ratings to build an efficient trust evaluation technique. As the worth of such trust evaluation system is relied on the accuracy of ratings gathered as input, thus efficient security against inequitable ratings is fundamental requirement of trust computation system.

b) Information Security

Security is shield of data in online transactions and is considered as a basic factor in e-commerce as it led to some new security threats. The acceptance of security systems is required for trust management. When security loophole occurs then the trust management system must act in quick manner to lessen the level of threat, operational effects and the day to day business. The method must be competent enough to support mixture of response ratings from large number of users. To provision high service availability, the cloud trust management service, all previously recorded data managed become available for evaluations of trust. It also

bears the utilization of diverse trust evaluation functions by distinct clients over similar rating taken from an entirely distributed ecommerce users.

Additionally as the communication about diverse services raises, the request for trust information may increase and boost its complication of the system to acquire data. The trust maintenance system must have the ability to vary dynamically in several distinct ways which could have an effect on the value of trust of multiple users with no communication details. The websites which involves online transaction also relies on trust models that support integrity, availability, reliability and secrecy of the data and information.

The user cannot do a transaction of some product without revealing their personal details, address to ship the product, bill details, or priority of the item. The service users might be not interested in providing these details if they have trust issues with the provider. Online shopping websites are required to make sure that their trust system is safe and reliable to users and it can work well in dealing with sensitive information also. Efficient prevention procedures should be considered and flawlessly incorporated with the plan of trust administration systems. For example, using control to supervise traffic and sustain network connection during an interruption and restricting the outcome and level of a risk or attack.

2.2 Trust Management Framework

Framework of trust management system should be able to facilitate the cloud providers to allow the users to calculate and decide values related to potential transactions. The techniques which can provide accurate value for trustworthiness is needed for trust administration system. It combines the fundamental safety procedures and trust assessment components that can filter ratings.

2.3 Trust Model

2.3.1 Trust Model Definition

Foster *et al.* [19] have explained that the trust model is defined as the scale of trust among two parties on each other. The idea of trust was taken from the relationship between customer and cloud provider. Such relation has some scope defined which is security threats. When the service provider monitors the actions of cloud system, the user or the clients generate ratings.

There are two outlooks to define a trust model in computing world:
Customer's outlook - what security does the service provider have?
Provider's outlook – what type of customer does it have?

The clients must be informed about the security faults and vulnerabilities that exists in the system or that have the possibilities. Trust model is nothing but some set of protocols which are to be followed by the service provider and their users or customers. Users also have the facility to provide some rules to overpower the activities on cloud according to their choices. The syntax of the protocol must be in understandable and standard form. It must be able to interpret into instructions every time the user made a request. The continuous mentoring of the activities happening in the cloud helps the users or clients and provider to have the information about the threats breaching the security of the cloud network. The rating provided by the clients does not add much to the trust management system. It is better to make list of expectations from the cloud user's activities so that the provider will know about his expectations form the user. Also it tells about how the provider can manage the cloud instances. If there is an increase in the count of cloud instances within same time phase every year then the provider will allocate the resources automatically thereby increasing satisfaction.

2.3.2 Types of Trust Models

Trust models are classified as follows:

- Centralized trust management - After one transaction completion the client report rating to the trusted party
- Decentralized trust management - A peer to peer system
- Distributed trust management - Data is shred among different brokers

Another category is based on flow of a transaction:

- Static trust management - Rules are defined by trust administration system
- Dynamic trust management - Profiles are as a trust model engine that defines

Static trust model have a predefined design and flow of the process of transaction. The model worked according to the design defined at the starting. A dynamic model works with future activities and unidentified process flow. The static model works according to system manner but dynamic model adjust with different parameters and progress based on the previous cached data stored in a data store.

2.4 Various Trust Models in Network

- **Various Models in Network**

Liu *et al.* [20] have elaborated a ubiquitous model to reduce some limitations and introduced a trust model which worked on distributed environment. This model has prevented the system from various attacks.

Spitz and T¨uchelmann [21] have reported a new model which manage the momentarily idle members and evaluate the computation of trust which is context dependent as well as status dependent. It results in truth telling property of the provider. This model has worked for both central and distributed network environment.

Wu *et al.* [22] have suggested a model which calculates trust based on reputation. Trust was computed based on seven parameters and also calculated on the basis of direct communication as well as peer's decisions.

Chhabra *et al.* [23] has introduced a model called supP2Prep. In this model with some changes were required. Problem of polling only in regard of trust has encouraged the author to add the perspective of distrust for the first time. This model has offered an efficient approach to avoid various security intrusion attacks. It also has resolved the issue occurs when a new peer enters the system.

Hu *et al.* [24] have proposed a trust model for p2p environment which works on feedback credibility and improve the terrace-based method of storage. It has given the mathematical study and execution strategy. The simulation and experimental has showed that this model worked better than global trust models. This model has prevented the network system from various malicious activities from peers and resulted enhancement in message operating cost.

Li *et al.* [25] have suggested a method comprised of two initial trust development models for network data system which were analyzed and compared at logical as well as practical level. The first one was introduced by McKnight, Choudhury and Kacmar in 2002 in electronic commerce environment. And the second was developed to calculate individual trust in NID. It has worked on theory of organized behavior and theory of reasoned activities. This model has worked more efficiently in evaluating a client's trust in information system. The authors also have done the analysis study to compare the above specified models in the perspective of user's trust computation. It has explained proper understanding of trust in IS.

Wen *et al.* [26] have concluded several trust models by studying them and introduced a new model which contains direct as well as indirect trust factors. In this model the direct trust has more weighting value than the indirect one. In that way the indirect computation has less value. The author has followed the phenomenon of slow rise and quick declination for trust. Additionally, the integrity of other experienced user opinions also taken into consideration to evaluate indirect trust. It has led to the objective nature of indirect trust. The procedure of transfer of reliability has also taken for estimation of indirect trust. Integrity assessment is the base of removing lesser credibility and enhancing trust estimation.

Yang *et al.* [27] have elaborated a trust model rely on algebra aiming to solve basic trust circulation and implication of trust in graphs. The authors have also reported a trust implication method and trust assessment algorithm using algebra. As the nature of trust is uncertain, the author gave informative details to measure the quantity of trust. The authors have proved the betterment of this trust model in comparison to other trust models and it's a common for distinct computing atmospheres or platforms reason being the abstraction of algebra.

Dorri *et al.* [28] have reported a trust model in which the quantification of vagueness is done based on confidence time intervals in certainty trust models and simulating environment find their parameters. The simulation results have shown the qualities and improbability of HMM (Hidden Markov Model) trust model. Additionally, an uncertain approach is introduced that decreases the danger implicated in trust model with respect to ambiguity.

Manuel [29] has elaborated the preparation of Service Level Agreement (SLA) by incorporating QoS requirements of cloud user and proficiencies of cloud providers. These requirements are turnaround Time, Cost, Security Level, and Computing Power, Networking speed. It has explained the calculation of trust value based on these requirements.

Guo *et al.* [30] have proposed a model name ETEC, which consist of a broad estimation method which is time-varient to express direct trust method and a space-variant estimation method for computing recommendation trust. This model effectively and reasonably calculated trust value using an algorithm.

Li and Du [31] have presented a better trust model in cloud for evaluating the quality of cloud service. In this model two varieties of adaptive modeling tools were combined and productively employed to trust system data mining and knowledge discovery.

Guizani *et al.* [32] have proposed a trust model named Efficient Distributed Trust Model EDTM. Direct trust, recommendation trust and indirect trust were discussed in this paper.

- **Trust Models in Grid computing**

Manuel *et al.* [33] have introduced a trust model which computes the resources of grid and cloud by cloud broker. In heterogeneous atmosphere the cloud broker selects the suitable resources on the basis of individual users. This model was executed with Kerberos authentication and PERMIS authorization to improve the broker's belief. This trust model has estimated the value of trust based on identity based trust and behavioral trust. The introduced method took parameters for both grid and cloud entities.

Varalakshmil *et al.* [34] have reported a trust model which is based on a reputation of a cloud provider. This model has used intermediate entities and brokers. This design depends on several brokers in every sphere. The entities are linked with various brokers. The entities are shared among different brokers, with each entities linked with two or more brokers. This increases the problem of redundant data managed at broker. This has also enhanced the network passage at broker's site and side by side

handles client's requests. The issues related with the maintenance of brokers were resolved using this model.

- **Trust Model in Mobile ad-Hoc**

Theodorakopoulos and Baras [35] have introduced a trust model to compute the trust proofs in ad-hoc networks. The evidences of trust were unsure and partial. The process was considered as path problem existing in directed graphs where points are entities and connection links are relations. The architectural issues and other important requirements are discussed. The author has showed the indirect relation of trust with no direct interaction. This semi-ring standard has worked efficiently to convey trust model. This model better has worked against malicious attacks implicated by the attackers.

Luo *et al.* [36] have described a trust model, RFSTrust, for mobile ad-hoc networks based on fuzzy. It has shown that RFSTrust has an entity identification and inhibition ability in synergies cheating and promotes data packet forwarding between nodes.

- **Trust Model in Cloud**

Abawajy [37] has presented a distributed standard that has enabled client and provider communication via trust based model. This method has efficiently controlled false ratings. It has diluted the effects of wrong ratings consequences and giving accurate and quality assessment of cloud services.

Zhang *et al.* [38] have proposed a model which works on neutral factors of trusted environment. This model is consistent and trustworthy as it has used the TCCP model which has moved from third party trust to trusted platform of IaaS.

Hwang *et al.* [39] have proposed an approach to integrate virtual clusters, cloud data centers, and trusted data accessibility according to reputed systems. A peer to peer cloud system was introduced for security of clouds and data storage area at scope of system. It has protected an entity objects at document accessibility level. Some computing technology organization such as Amazon, Google, and IBM employ protective solutions to give safety to service models in cloud i.e. IaaS, PaaS, and SaaS.

Zhang [40] have suggested that trusted computing motivates clients to use sharable resources and application services provided by the provider. Trust is the main factor in choosing a cloud service provider from the list to use the services. When the customer wants a service, he first checks if the provider meets all the requirements. Then he checks two things. First, the present capabilities of the provider and second is the past credentials of the provider. Past credentials define the former reputation of provider and records of services provided by the provider. It consists of different factors i.e. reliability, availability, and turnaround time and data integrity. Present capabilities illustrate about the services provided at present. It comprises of factors like speed of processor, average throughput, hard disk capacity, RAM size, network bandwidth, latency of the given resource

Pearson [41] has elaborated the theoretical background and provided a basic view of how cloud computing not only impacted information technology (IT) budgeting but also affected conventional mechanisms. In this chapter, the author has explained different issues related to security, trust and privacy in a cloud.

Zissis and Lekkas [42] have proposed the solutions based upon cryptography, specifically Public Key Infrastructure operating in coordination with LDAP and SSO, to make sure that the system authentication, integrity and data confidentiality of storage and communications. The generic design ethics of a cloud environment were identified in this paper which originated from the necessity to control important vulnerabilities and threats.

Firdous *et al.* [43] have elaborated a complete survey on the topic of the trust management systems which is implemented on distributed computing systems with a special focus cloud computing.

Huang and Nicol [44] has suggested that trust in cloud computing relies on the reputation of the provider and self-estimation of their services. Trust is comprised of expectation, belief, willingness to take risk. Trust is reputation based which is an aggregate opinion of a community, SLA verification based trust which focuses on visible elements, Trust as a Service, which includes Cloud Trust Authority (CTA) to give a single point for organizing security of cloud services from different cloud providers, Policy based, Evidence-based trust.

- **Fuzzy Logic based Trust Model in Cloud**

Chang et *al.* [45] have elaborated a subjective trust management architecture based on fuzzy set theory in cloud computing which was based on in-depth research on forgoing studies.

Gu *et al.* [46] have introduced virtual machines based trust model for cloud computing considering two aspects. The timeliness strategy was used to ensure the response time and idle time of servers was minimized. The trust values for each cloud provider are calculated using fuzzy theory to get successful response.

Xia *et al.* [47] have introduced a trust evaluation model with multiple trust decision parameters which are based on fuzzy set theory. The fuzzy AHP theory was used which is based on entropy weight mechanism.

Wagng *et al.* [48] have suggested that the current strategies which were based on probability and fuzzy set theory didn't give sufficient importance to ambiguity. To eliminate this problem, the authors have proposed a quantifiable subjective trust evaluation approach. This approach has used projected value and hyper-entropy of the particular cloud to compute the reputation of trust objects.

2.5 Fuzzy Logic Review

Burhan Tiirkgen [49] has introduced an organized structure of fuzzy logic. The organized structure was accomplished by extrication of the membership function assignment with the fuzzy sets and the truth with propositions. There are several classes of classical as well as fuzzy logic theory.

Ramot *et al.* [50] have explained that the originality of complexity in fuzzy logic is that the sets in the process of reasoning are complex fuzzy sets, which are done by membership function includes complex set values. The range in classical fuzzy set is from 0 to 1 but in this complex fuzzy set the range is in unit circle. It has provided a procedure to explain membership sets in complex form of sets. Some theoretic functions available in this paper are complex union of fuzzy sets, relation between complex fuzzy sets, composition, intersection, and aggregation of vectors.

John Yen [51] has elaborated that initially fuzzy logic was used in artificial intelligence to manage vagueness. But nowadays fuzzy logic is utilized for mapping standard.

Lee and Hong [52] have introduced a method to automatically derive fuzzy membership functions. A fuzzy if-then rules is derived from training examples to construct a prototype fuzzy based expert system. The author has applied fuzzy inference procedure based on the expert system.

Pedrycz [53] has shown a study of triangular membership function and concluded that under some assumptions these fuzzy sets comply with codebook and gives satisfaction of no-error criteria

Wang [54] has elaborated that the centroid defuzzification is a general method used to rank fuzzy numbers and require membership function. The author has derived two formulas assuming that the membership function is approximated with the help of piecewise linear functions. this function is based on alpha level sets.

Chapter 3

Problem Statement

3.1 Barriers in Previous Work

Trust is an essential in case of decentralized data sites and the cloud resources are shared among a large number of hosts, which is specifically a fact in a cloud computing environment. The main issue with cloud computing nowadays is the security requirement. The biggest and necessary concern of cloud users is that " if the data they have shared is also being shared with someone else on the same resource?" Controlling and possession is also a difficult issue. The clients don't use a system when he has no power over the properties provided by them. For instance, when people withdraw some cash from ATM machine, they trust that the accurate amount of cash will be given to them because the device is under their control. But this is not the case when we deposit money via ATM because they have no control on the cash they deposited. In the same way, the cloud providers must provide control over the data to clients. The two leveled variable trust relation is formed between the provider and the client when the enterprise stores or deliver their data to the resources provider. The enterprise trust on the provider and the user's of that enterprise also trust the cloud provider. The services which are based on clouds are so common nowadays. Threats on security and privacy of user's data are quite a big distress.

Some problems may occur, such as legal issues, standard SLA's because the cloud provider is a self-regulating firm. Security became the main concern for protecting the cloud services from service failures and refining trust in cloud. The cloud provider has to deliver differentiated services to distinct consumers, which lead to safety issues in a virtual cloud atmosphere. In a virtual environment, some of the privacy issues are identification management, data loss due to sharing of resources, usage control, virtualization hardware safety, user's content protection, and malware attacks. The cloud user's mindset is that a cloud is not much safe than local system. If good level of transparency is provided by the cloud resource provider then it would result in secure cloud system. The data located on cloud is not actually presented at single location but located across all over the virtual layer of cloud network.

The problems related to transparency are physical locality of the data and protection profiles of the data processing sites. Set up assurance between the provider and the consumer entity is very important. The reputation of cloud provider is becoming the obstacle for the user to employ cloud services. Cloud providers face some difficulty in making their own reputation because the SaaS (software as a service) mechanism is new to everyone. When there is less clarity for user about why their private information is being asked for, or who is going to process their data? , this lack of command and lack of observance of the cloud supplier will result in doubt or distrust.

There exist a security concern about the data is protected or not. Consequently the cloud users may hesitate from utilizing the services available by cloud providers. They worry about their sensitive information being shared all over the network without their consent. Some fake provider's uses customer's data and make profit out of it without getting noticed by the users. A lot of risk is involved in sharing the data on different cloud storage locations, especially your private content or confidential information. But the problem is the lack of standards provided by trust models available in cloud infrastructure.

3.2 Problem Statement

There are several cloud trust models introduced by various researchers and organizations with their best parameters and efficiency. Security becomes most important criteria for the clients to choose one of the available cloud resources. When the user wants to choose a specific service, then he will need some ranking application to evaluate the quality of cloud service. A standard which assesses the reliability of cloud resources is the requirement of cloud clients to choose a service. This thesis focuses on making such a framework for cloud environment.

The main focus of this thesis is constructing such a framework. This kind of framework must be able to discover the mechanism for providing safety in a cloud atmosphere to be evaluated and ranked. So a tool which helps us to rely on the services of a cloud is the essential demand of the cloud computing network. Here a model to compute the trust value for different cloud resources is proposed. It calculates the strength of the services provided by the cloud. The Model must contain factors to wrap all the security features.

An evaluation approach is constructed to calculate trust value. Identification of parameters and estimation of formulae is done to calculate the trust for a particular cloud service provider. The result of this research is the trust model for cloud resources. The values given by the trust model are static in nature. Trust rate is affected, on the basis of user feedback and transfer of data during a span of time. Simulation and experimental results of these trust values will be also required. The model is verified and its accuracy is validated with regards to cloud services. The trust value computed by the model provides the trust for services considering various levels of security measures. The services and resources can be estimated for trust values. The trust model rank the services provided by the cloud provider and so that the user can select the provider who satisfies the demand of user and whose trust value is better. It can be utilized as a standard to implement the cloud service security. Following are few research questions which need to be addressed in order to implement a robust trust model in cloud computing:

1. How accurately can a trust model compute the information gathered from multiple heterogeneous information sources?
2. How to bring consensus by modeling multiple attributes of cloud computing?
3. How to use accurately, the trust values in a given context which has been computed in a different context?
4. How trust model improves the cloud resource utilization?

The complexity of cloud computing makes us consider both the physical security parameters and architectural configurations. The subjective characteristic of trust is appropriate for acquiring the complexity of cloud. Some of the trust models are presented in the state of art in this thesis.

3.3 Objectives of Proposed Work

The objectives of the research are:

- To study existing trust model and what are the different trust evaluation parameters.
- To model a less complex and reliable trust model for cloud computing environment.
- To estimate the performance of the proposed trust model.

Chapter 4

Proposed Solution

The problem statement and objective of the proposed work is defined in previous chapter describing the way to lead the work. This chapter includes the solution of problem statement defined in previous chapter and the architecture of the proposed work. Also the used algorithm and technique is also elaborated.

4.1 Proposed Model

The proposed work is combining the QoS based trust model with fuzzy logic mappings to construct a novel trust based model which provides strong policy to select required cloud resources from a pool of resources available on the cloud.

4.1.1 Architecture Proposed Model

The architecture of the proposed model is shown in figure 4.1. This model consists of three main modules and other general modules. Important modules are System Manager, SLA Manager Module, and Trust Management Module.

Other components are Authorization & Authentication, User Interface, Cloud Directory, and Scheduler. User Interface is used by the cloud user to interact with the cloud provider.

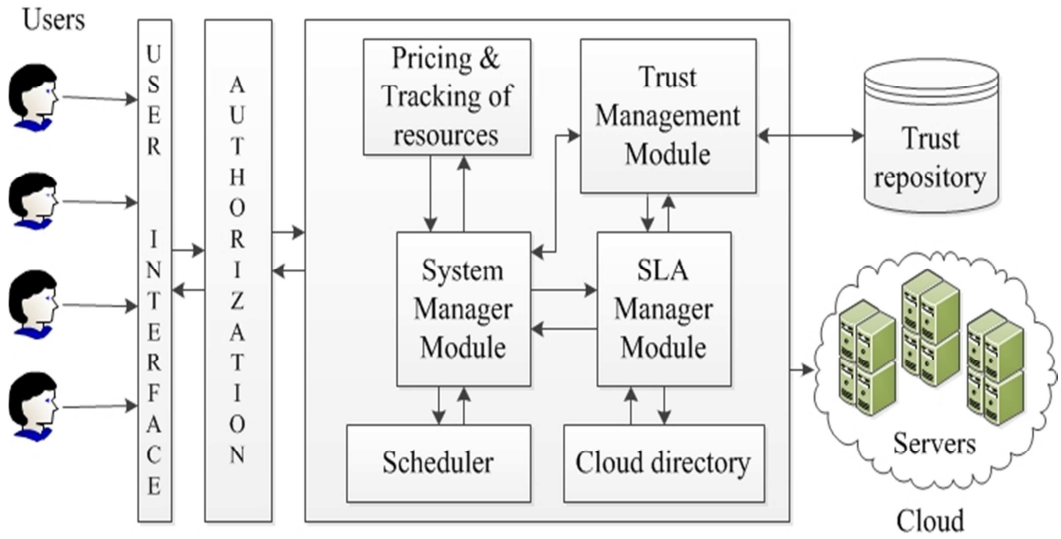

Figure 4.1 Architecture of a Trust Model

The brief description of all the components of the proposed model is given below:

- **Cloud user:** The cloud users are the users which have their registered account with the available cloud service providers. The customer or the end user request for a resource available on the cloud service provider, then the authentication of this user is checked by the cloud provider. If the CSP verifies that the user is a valid user then the access is given to him else access denied.
- **Cloud resources:** The resources available on the cloud can be any hardware or the software which is accessed and used by the customers. The resources which are available on cloud must be of good quality and satisfies the eligibility requirements of Quality of service (QoS) parameters. The QoS parameters are specified in the service level agreement described by the provider for negotiating.
- **Pricing & Tracking Module:** While communicating to the cloud provider, the user checks for illegal actions or malicious behavior. This module tracks and observes all the processes implemented by the process.
- **SLA monitoring module:** Service level agreement Module prepares an agreement between the user and the provider which is used to assure the quality of service of the resources. This module checks whether the efficiency of the resources are in accordance with SLA document. This agreement collects the information when processes interact with user and service providers.
- **Authorization Process:** Authorization is the process in which the cloud user and providers are authenticated and their identity is verified. The trust values for user are also calculated using trust parameters. To verify the authenticity of user Authorization module checks the details of a user, verifies them on the basis of some checks and let them choose a provider among a list of cloud service providers available in the database.
- **Trust Management Module (TMM):** This module evaluates the value of direct trust by taking values from different parameters of cloud computing. Parameters used are turnaround time, data integrity, availability. This module applies all the fuzzy logic evaluation technique on these parameters and estimates the final trust value.
- **Trust repository:** Trust repository contains trust values of resources available on different cloud providers. It updates the value time by time based on the user

behavior and cloud provider quality. If the quality gets lower then the value will be updated in this repository because it contains performance based trust values.

- **Scheduler:** This module schedule the resources selected by the user according to some scheduling policy.
- **Cloud directory:** It contains all the information about the existing providers and users registered on the cloud network.

4.2 Fuzzy based Trust Management Module

Trust management module is the main component of the architecture.

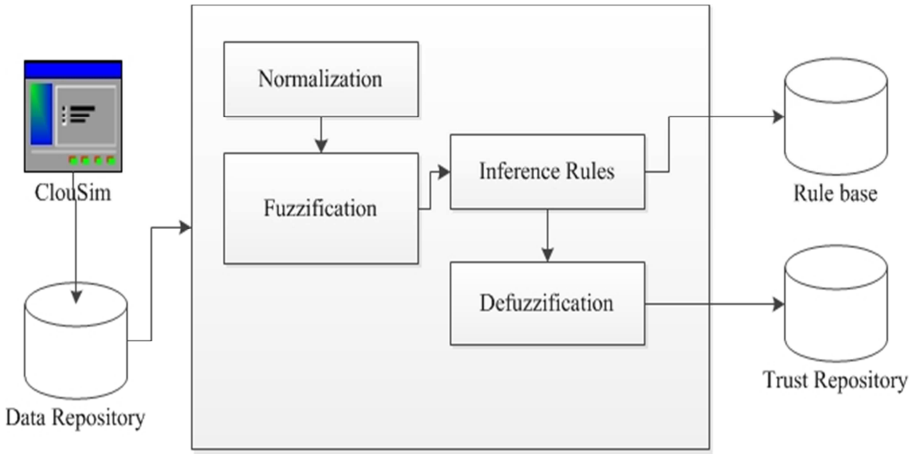

Figure 4.2 Architecture of trust Management Module

Figure 4.2 shows the trust management module comprises of many small-small modules. These small modules process the parameters to evaluate the trust value of a particular resource of cloud providers. TMM works with cloud service providers to observe the behavior of the cloud user and quality of the services availed by the cloud provider. This module processes the data received from the cloud clients, broker and the service provider. This process includes various calculations and phases for computation of trust.

Components of TMM are elaborated below:

- **Normalization Module**

  This module scales the values generated by the CloudSim Simulation environment. If the range of values is high then we have to normalize the values in a scale of 1-10 or 1-100 so that the fuzzy sets can be generated. The fuzzy sets are generated with the help of fuzzy membership function.

- **Fuzzification Module**

  This module converts the value of different parameters into fuzzy sets using fuzzy membership functions and then the value is mapped to Low, Avg or High fuzzy set. The input to this module is the crisp value and output will be the fuzzy set value. The Triangular membership function is used to convert the crisp value of parameters into fuzzy linguistic variables.

- **Defuzzification Module**

  This module converts the fuzzy sets into crisp values using fuzzy logic formula for defuzzification. The defuzzification is done using the Centroid method defuzzification. Input to this module is the fuzzy set value (low, avg, or high). The outputs of the module is the crisp value of trust for a particular resource availed by the cloud provider.

- **Inference Engine Module**

  This module maps the fuzzy set values to crisp values using some set or protocols or rules which are also known as inference rules. Inference rules are defined using different cases (low, avg or high) of all the factors which can occur during usage of the model. Based on these cases the implications are defined which represents the output of trust value.

- **Update Module**

  This module updates the value of trust for various resources of cloud time by time based on their performance. The quality of services is checked regularly and user feedback value is also taken as a parameter to update this value.

- **Data Repository**

  This repository contains the raw value of different parameters calculated using CloudSim and the fuzzy range of all of them. The providers of different cloud resources store the QoS parameter values of their resources in this database. The fuzzification process takes value from this repository. Fuzzy range will help in estimating the fuzzy set of different parameters.

- **CloudSim**

  It is a simulation and analysis tool for cloud computing, which gives an interface to create a cloud network and analyze different algorithm on the resources of cloud. It lets us create hosts, virtual machines, cloudlets, and datacenters on

cloud. It is a Graphical User Interface (GUI) which is easy to use and learn the functionalities of cloud and network.

4.3 Execution Flow of the a Trust Model

Following are the steps used by the proposed model:

Step 1 - The cloud users register themselves on different cloud providers and their credentials are stored in a database.

Step 2 - The cloud user specifies the name of the resource, Quality of Service requirements and a list of available cloud providers of that specific resource to this model.

Step 3 - These lists are given to the System Manager.

Step 4 - System Manager checks from the data repository if these resources are available or not.

Step 5 - System Manager forwards this list of user requirements and cloud providers to SLA Manager.

Step 6 - SLA manager checks the trust values for these providers from Trust repository provided by Trust Management Module (TMM).

Step 7 - After that, Service Level Agreement (SLA) is prepared by the model, between the user and the cloud provider.

Step 8 - SLA Manager forwards this SLA document to System Manager.

Step 9 - Simultaneously resource allocation and billing is done.

Step 10 - Also the trust repository gets updated after use of resources.

4.4 Resource Selection

A cloud resource is chosen based on the following criteria:

1) *Turnaround Time* – Time interval between the job submission and delivery of a task.
2) *Cost* – subscription fee for a resource
3) *Network Bandwidth* – The rate at which data transform

4) *Latency* - The delay in time between the reason and consequence of any type of physical variation in the computer or network system.

Let us assume that the cloud system has *K* cloud resource or service providers P_1, P_2, P_3 ……P_k who meets the above requirements. The cloud user first surrenders the cloud provider's list along with the QoS essential criteria to the system manager. Then the system manager passes on this list to the SLA manager. Afterwards the list is sorted by SLA manager on the basis of trust values of different resources received from Trust Management Module. Let us take a scenario of a user and two cloud providers. The user specifies the required QoS parameter values in table 4.1. Two cloud providers C_x and C_y also has given their QoS values of their resources which is shown in table 4.2.

Table 4.1 Requirements of User A

QoS parameters	**QoS requirement by user A**
Processor Speed	2GHz Clock Speed, 8 MB Cache, 1024 MHz Bus Speed
Turnaround Time	150 min
Cost	2300 $
Security	LDAP
Networking Speed	Bandwidth – 9 Gbit/s, 4 ms (mili sec.)

Table 4.2 Availability by Provider C_x & C_y

QoS parameters	**QoS requirement by user A**	**Availability on C_x** **TRUST VALUE – 0.42**	**Availability on C_y** **TRUST VALUE – 0.95**
Processor Speed	Clock Speed -2GHz Bus Speed - 850 MHz Cache - 9 MB	Clock Speed - 3GHz Cache - 9MB Bus Speed - 1000 MHz	Clock speed - 2GHz Cache - 6MB Bus Speed - 880 MHz
Turnaround Time	150 min	160 min	170 min
Cost	2300 $	2300 $	2500 $
Security	LDAP	LDAP	LDAP
Networking Speed	Bandwidth – 9 Gbit/s Latency - 4 ms	Bandwidth- 11 Gbit/s Latency – 3.5 ms	Bandwidth - 12 Gbit/s Latency – 4.7 ms

C_x is more capable than C_y but the trust value of C_x is less than C_y. Let us assume that C_y is selected by the user A. Then the SLA manager prepares an agreement between user A and the provider through system manager after some negotiation and compromises. After that the provider executes the job given by user according to the SLA. Following is the SLA parameter value agreed between the user and the provider:

Table 4.3 SLA between User and Cloud Provider

QoS Factors	QoS agreed by both the parties
Turnaround Time (min)	130 min
Cost (in dollars)	2500 $
Security Level	LDAP authentication
Computing Power	2GHz Clock Speed, 8MB Cache 800MHz Bus Speed
Network Speed	N/W Bandwidth – 9 Gbit/s, Latency – 4ms

4.5 Trust Evaluation

The evaluation of trust is done using quality of service parameters which are the measure of performance and efficiency of the system. Fuzzy logic is applied on these parameters.

4.5.1 Trust Evaluation Parameters

Trust values are calculated from attributes of resource provider, such as resource reliability, service and resource availability, and turnaround time and data integrity.

Availability- divide the total number of jobs accepted by the number of jobs submitted to compute availability of a resource [33].

$$Availability = \frac{total\_number\_of\_jobs\_accepted}{total\_jobs\_submitted} \quad (1)$$

Reliability is measured by the number of successfully completed jobs given by the cloud provider resource [33].

$$Reliability = \frac{number\_of\_jobs\_completed}{number\_of\_jobs\_accepted} \quad (2)$$

Turnaround Time (TE): Turnaround time is the time duration from when the job is submitted to when it is delivered to the user [33].

$$Turnaround\ time = Delivery\ time - Job\ submission\ time \quad (3)$$

4.5.2 Fuzzification

A fuzzy logic is described as the method of mapping a data to a scalar data as output. This system consists of fuzzification, inference rules, decision component, and defuzzification. Figure 4.3 shows the components of fuzzy systems. The Crisp values are provided as input to this fuzzification system and these values are transformed to a fuzzy logic set using linguistic set variables, terms and fuzzy membership functions. This process is termed as *fuzzification*. After fuzzification, Fuzzy inference rules are used to get the fuzzy outcome value. *Defuzzification* is done by mapping the fuzzy outcome to the crisp value.

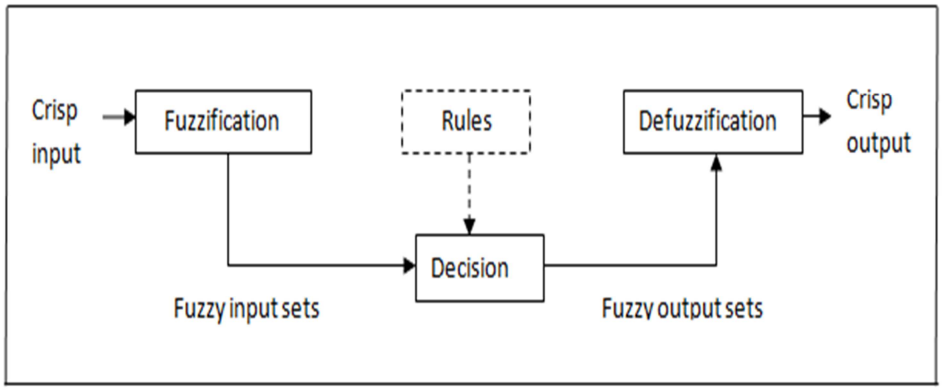

Figure 4.3 Fuzzification Process

4.5.3 Trust Evaluation Strategy

In this thesis, trust is evaluated using Fuzzy Logic theory. First the fuzzification is done on the crisp values of data and then Inference rules are applied to get the category of trust values. Defuzzification is applied to get the Crisp trust value for the cloud provider.

Trust can to some extent belong to a fuzzy set and set membership function is used to represent it. Let $S = \{s_0, s_1, s_2 \ldots\ldots, s_n\}$ is the domain set where s is the elements of the set and $i = 1,2,3 \ldots\ldots,n.\ \forall s \in S$ and S can be represented by

$$S \rightarrow [0, 1],\ \mu_A(s) \in [0, 1]$$

In cloud computing, the trust can be described as the degree or level of membership of fuzzy sets in S which represents different levels of trust. Three fuzzy logic sets are used to express trust which is as follows:

T1 = “Low trust”

T2= “Average trust”

T3= “high trust”

The values of these parameters are calculated using CloudSim Tool by creating virtual machines and cloudlets. After taking these values, *fuzzy logic* is applied on it. After analyzing the value of T, anyone can easily interpret the reputation and quality of resources of a particular cloud provider. These factors help both the provider and cloud user.

4.5.4 Fuzzy Membership Function

The proposed model is using a triangular membership function [53] shown in equation (4) to map crisp values to fuzzy sets. This function consists of a vector d, and is dependent upon three arguments l, m, and n which are scalar in nature. Now, Values for turnaround time are calculated using CloudSim and Netbeans IDE and used in plotting the membership function graph.

$$triangle(d; l, m, n) = \begin{cases} 0, & d \leq l \\ \dfrac{d - l}{m - l}, & l \leq d \leq m \\ \dfrac{n - d}{n - m}, & m \leq d \leq n \\ 0, & n \leq d \end{cases} \quad (4)$$

Define the range for all the three levels (Low, Avg, and High). For example, for turnaround time, the values for l, m and n are:

For Low, l=1, m=17.5, n=35.

For Average, l=30, m=47.5, n=65.

For High, l=60, m=80, n=100.

4.5.5 Trust Range of parameters

Range of trust parameters (Turnaround time, Availability, and reliability) are shown in tables 4.4, 4.5 and 4.6.

Table 4.4 Range of Turnaround Time

Class Name	Turnaround Time	Symbol
Low	0-35	L
Avg	30-65	Avg
High	60-100	H

Table 4.5 Range of Availability

Class Name	Availability	Symbol
Low	0-4	L
Avg	3.5-7	Avg
High	6.5-10	H

Table 4.6 Range of Reliability

Class Name	Availability	Symbol
Low	0-4	L
Avg	3.5-7	Avg
High	6.5-10	H

4.5.6 Trust Range

The values for the Trust is calculated by passing the fuzzy sets described above through fuzzy inference rules. By drawing the trust values using the *Triangular membership function*, a graph can be generated for Trust T as shown in figure 4.4. It is also classified into three categories. Here X-axis denotes the trust values.

Table 4.7 Range of Trust

Class Name	Trust Range Value	Symbols
Low	0-3.5	LT
Avg	3-6.5	AvgT
High	6-10	HT

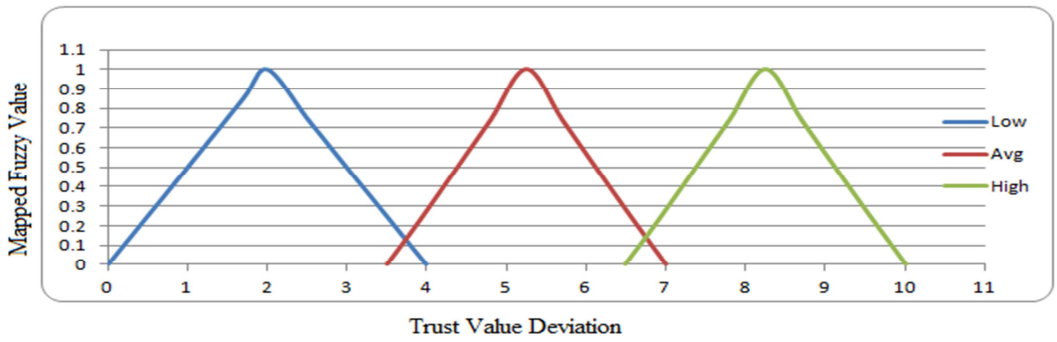

Figure 4.4 Membership function of Trust Value

4.5.7 Fuzzy Inference Rules

Inference rules are the steps used to map a given input value to an output fuzzified value. Such mapping strategy is used to make decisions, or fuzzy patterns. There are two concepts: - Linguistic Fuzzy rules and if-then-else rule. In linguistic approach, the values comprises of English words and some sentences. And in If-Then-Else rules have two parts; the antecedents and consequent which consists of linguistic variables propositions.

$$R_{(q)}: \; IF\ x \in P_1\ and \ldots\ldots and\ x_n \in P_n \text{ THEN } y \in q_j.$$

Where, $q = 1, 2, \ldots w$. W is the number of rules. P and T are the fuzzy value for parameters and Trust respectively. According to the rules discussed above, the proposed model is preceded. There are 3x3x3=27 fuzzy rules in our extension model. For example, one of the inference rule is-"*If Availability is low, Turnaround Time is low, and Reliability is low then the final Trust outcome is low*". According to these rules the fuzzy value for Trust can be generated.

4.5.8 Defuzzification

After Fuzzification, the next task is to do defuzzification to get crisp values using any mathematical method. Centroid method of defuzzification [54] in the equation (5) is used in the proposed model, which is also very popular and used mostly. The equation used:-

$$z^* = \frac{\int \mu_B(z)\, z\, dz}{\int \mu_B(z)\, dz} \tag{5}$$

where $\mu_B(z)$ is the fuzzy membership function.

4.6 Flow Diagrams

Flow Chart of Trust Model is shown below:

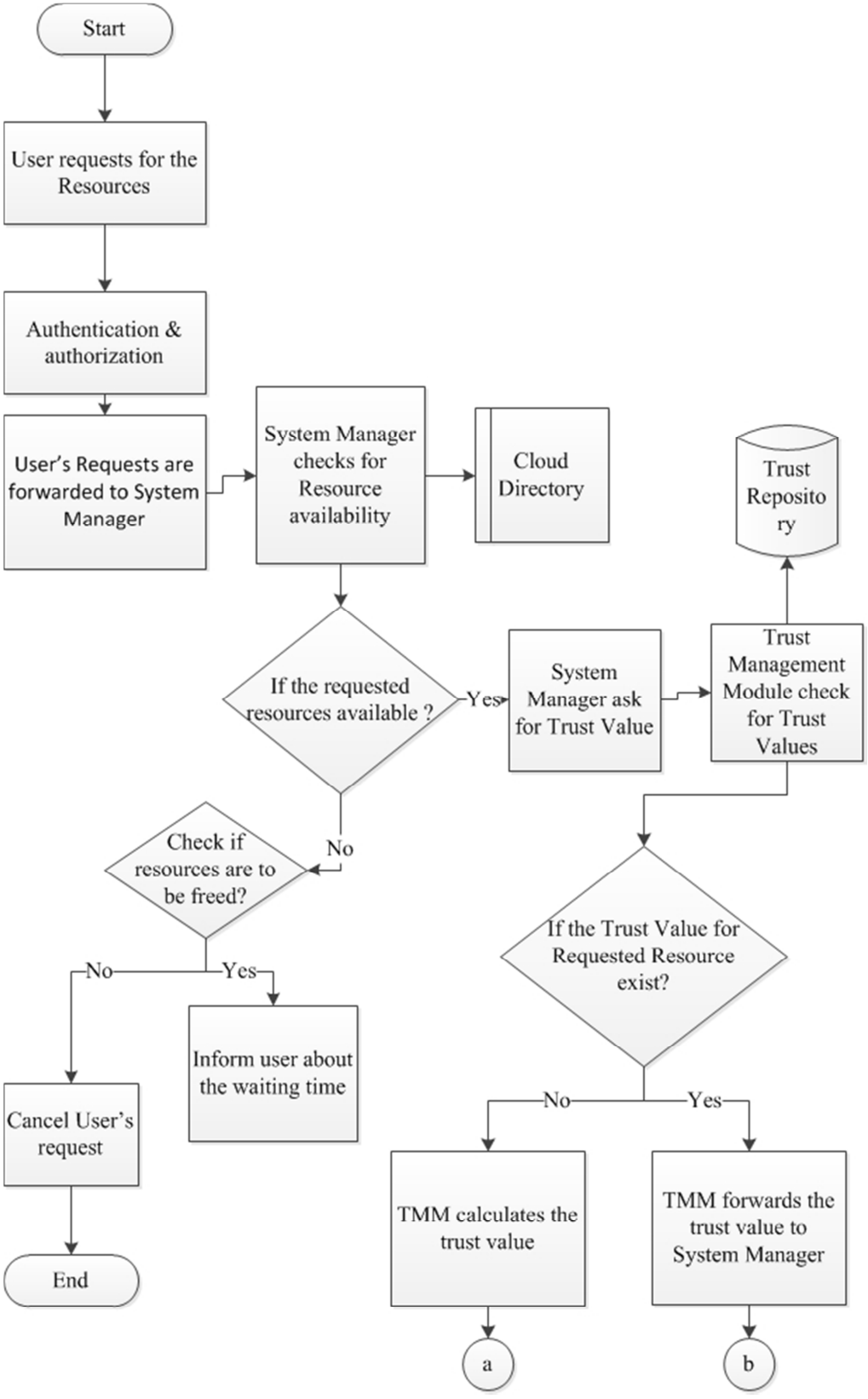

Figure 4.5 Flow diagram of Trust Model (part a)

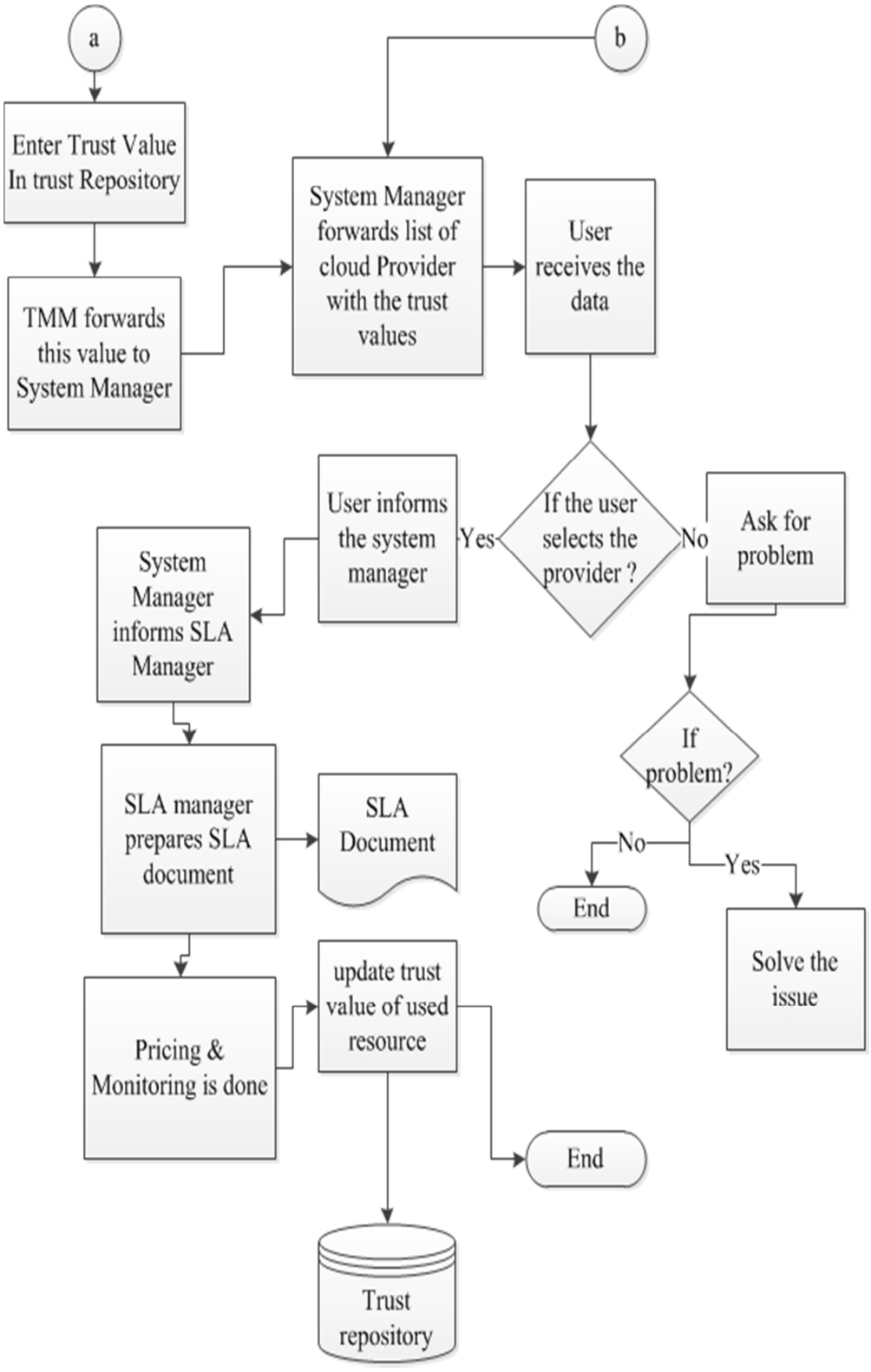

Figure 4.6 Flow diagram of Trust Model (Part b)

Flow diagram of Fuzzy based Trust Management Module:

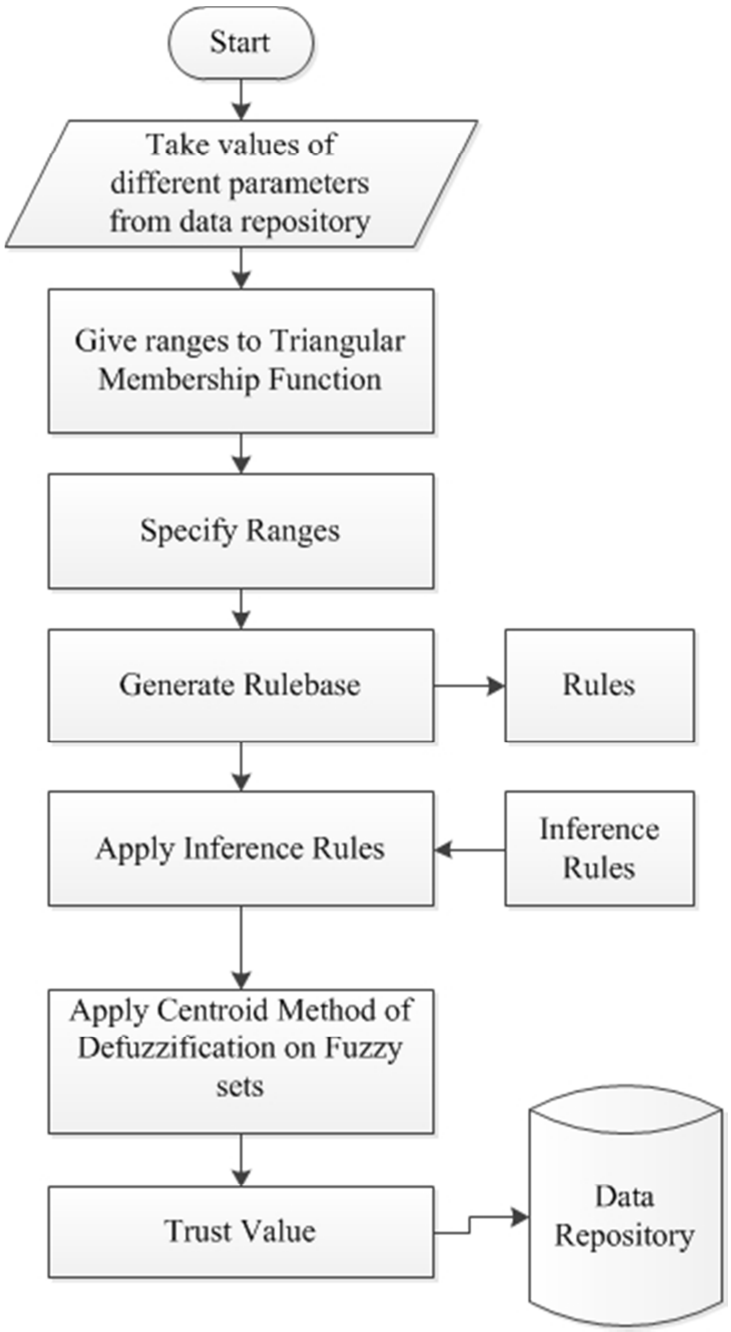

Figure 4.7 Flow Diagram of Trust Management Module

Chapter 5

Simulation & Results

In this chapter, the simulation and result analysis are discussed using Graphical User Interfaces and result Graphs.

5.1 Experimental Setup

A virtual cloud setup is created in CloudSim to define computing resources. A virtual cloud environment is created in which the resources of different capabilities are defined. First the user submits their quality of service requirements such as security, computing power, and networking speed to the cloud provider. We implement our proposed model using the following platform:

- CloudSim
- NetBeans IDE

5.1.1 CloudSim

CloudSim is a widely used software framework for demonstrating and simulation of Cloud Computing environments. CloudSim is a platform to create simulation environment using virtual machines, cloudlets, datacenters, hosts, etc. It is a java based entity which makes it highly scalable. Scheduling policies, network topologies, VM migration, power management and much more, are the features of CloudSim.

5.1.2 NetBeans IDE

Netbeans is a sophisticated tool which is used to build any kind of application for official as well as personal purpose. It provides Graphical User Interface (GUI) and runs on different Linux, Mac, OS, Unix, Windows xp/vista/7/8/10, and Solaris. It supports multiple languages such as Java, C , C++ , html and CSS. It has following features:

- Swing GUI builder – build GUI using swing components
- Profiler - monitor speed and memory usage.
- Platform - NetBeans platform facilitates user to develop application easily using APIs.

5.2 Model Simulation & Results

5.2.1 Simulation Parameters

Simulation is done using CloudSim and NetBeans IDE. Trust value is evaluated using QoS parameters such as Turnaround Time, availability, and Reliability. The values of all these parameters are calculated using the netbeans IDE with CloudSim toolkit. Following are the Trust Evaluation parameters:

- Availability
- Reliability
- Turnaround Time

5.2.2 GUI and Results Obtained

Figure 5.1 and 5.2 shows the interface of the tool to calculate trust values for different cloud providers.

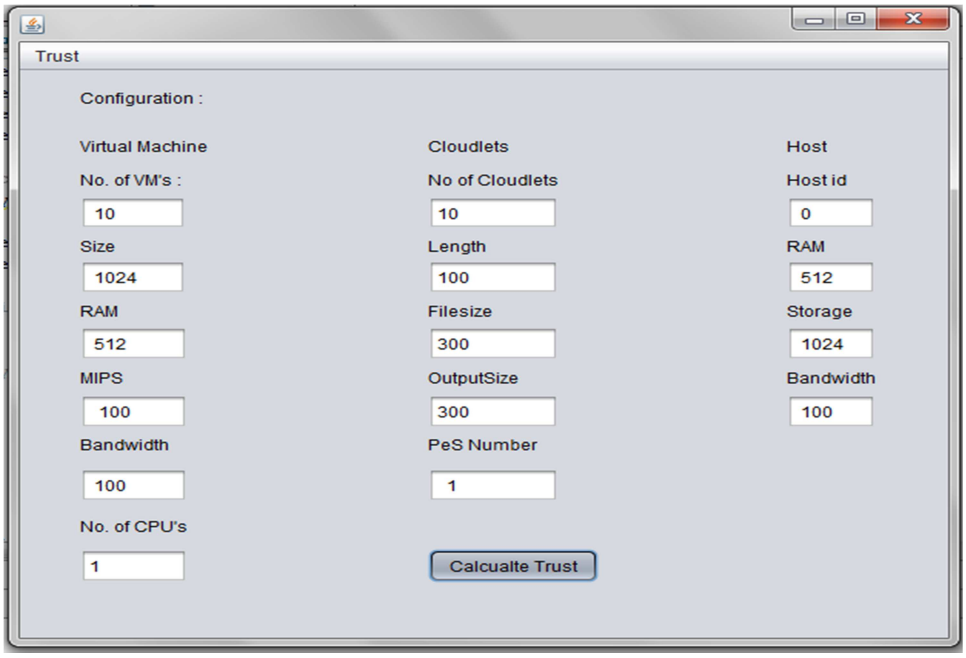

Figure 5.1 Trust Evaluation Interface

This interface is generated using NetBeans JFrame component. Figure 5.1 shows the interface to enter system configuration, number of cloudlets, and number of VM and its configurations. The figure 5.2 shows the result table showing the different values of QoS parameters and the calculated value of trust.

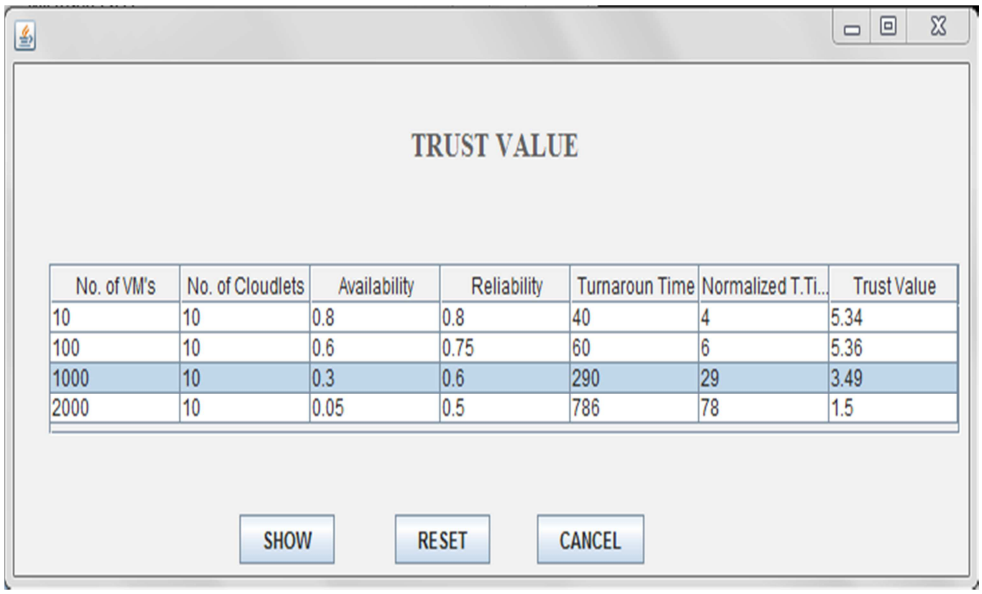

Figure 5.2 Calculated Trust Values

The value of the above said parameters is calculated and stored in a table 5.1, 5.2 and 5.3 using this model. Table 5.1 shows the calculated and normalized value for turnaround time. The range of turnaround time was very high, so we have normalized those values to a range of [1-100].

Table 5.1 Calculated Turnaround Time Values

Low	**Mapped Value (Low)**	**Avg**	**Mapped Value(Avg)**	**High**	**Mapped Value(High)**
0	0	30	0	60	0
2.5	0.09	31.2	0.068	63.5	0.175
6	0.3	35.5	0.314	66.9	0.345
8	0.48	39	0.514	70.1	0.5
15.5	0.87	42.6	0.72	73.4	0.67
17.5	1	47.5	1	80	1
20	0.85	51.7	0.75	80.5	0.97
25	0.57	57.4	0.43	83.9	0.8
26.7	0.47	59.2	0.33	89.4	0.52
30.4	0.26	63.9	0.06	95.6	0.22
35	0	65	0	100	0

Turnaround time is divided into three categories Low (0-35), Average (30-65), and High (60-100).

Table 5.2 Calculated Availability Values

Low	Mapped Value	Avg	Mapped Value	High	Mapped Value
0	0	3.5	0	6.5	0
0.5	0.25	3.7	0.11	6.8	0.17
1	0.5	4.3	0.45	7.4	0.51
1.7	0.85	4.9	0.8	8.1	0.91
2	1	5.25	1	8.25	1
2.5	0.75	5.7	0.74	8.7	0.74
2.8	0.6	6.1	0.51	9.1	0.51
3.7	0.149	6.8	0.11	9.7	0.17
4	0	7	0	10	0

The calculated value is taken on the x-axis and fuzzy membership value is evaluated and written in the column y-axis. The fuzzy set values are calculated using triangular membership function that maps the float values of the parameters to a fuzzy set value which lies between 0 and 1.

X-axis takes the value of parameter turnaround time in nano-seconds and y-axis value is calculated using the triangular membership function given in equation (4). For example, when turnaround time value is 15.5 ns (Low range), then the fuzzy value calculated using equation (4) is 0.87. Some of the generated values are shown in table 5.1 (Range 1-100).

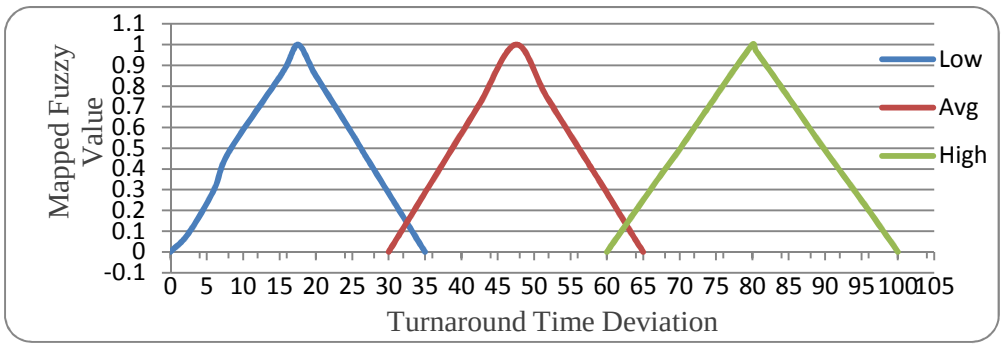

Figure 5.3 Membership Function for Turnaround Time

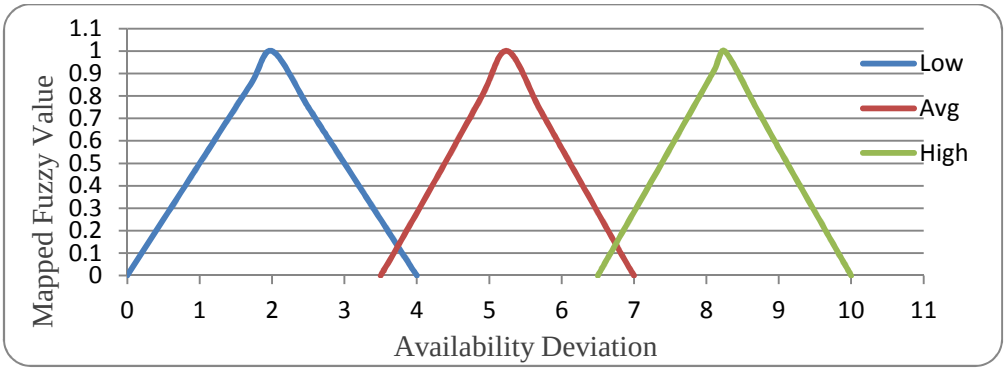

Figure 5.4 Membership Function for Availability

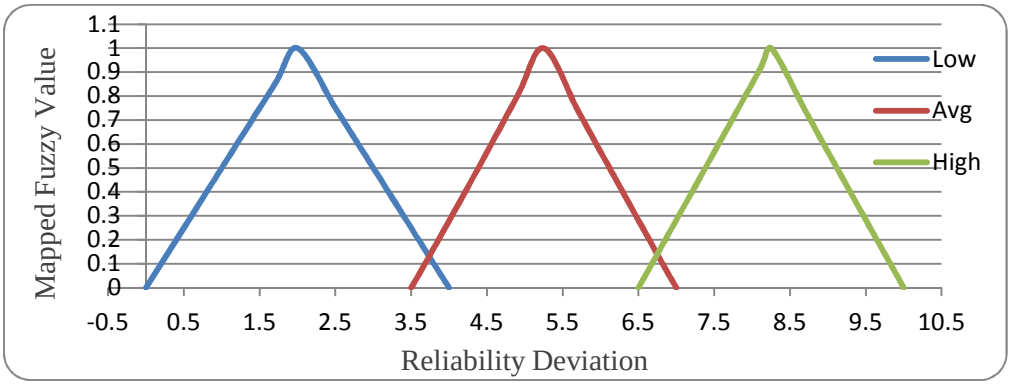

Figure 5.5 Membership Function for Reliability

Then the membership function graph is plotted as shown in Figure 5.3 using the values of table 5.1. Similarly the graph for Availability and Reliability is plotted using calculated values as shown in Figure 5.4 and Figure 5.5.

5.2.3 Implication Process

The first task before the implication is to find the fuzzy set's value for each parameter and plot them on a graph as shown in figure 5.9. The input value to this process is a numeric value and output is a fuzzy set value. Then Crisp value is calculated for trust using equation (5). Map that value according to table 4.8.

For example, if the turnaround time is low (0.4), Reliability is average (0.6) and Availability (0.4) value is high then value of trust is average (4.94). From figure 5.9, It can be seen that Turnaround time is low (0-3), Reliability is average (3-6) and Availability is high (7-10). Then the graph of all three parameters is integrated into one. Then the value of trust is calculated for 1st case of table 5.1 in the following ways:

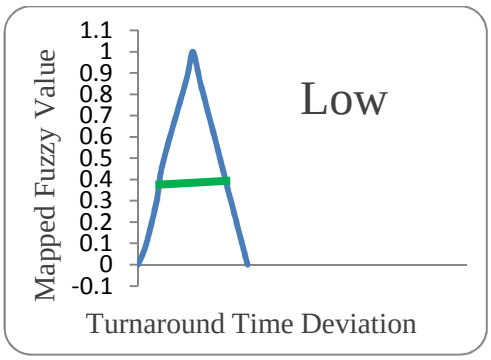

Figure 5.6 Turnaround Time Value

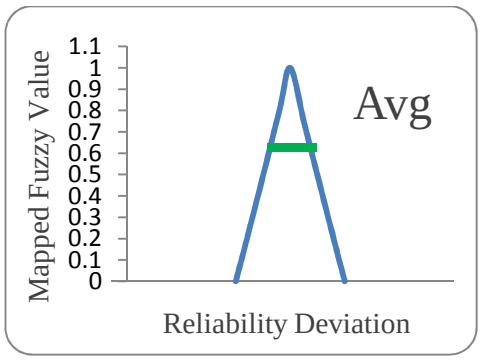

Figure 5.7 Reliability Value

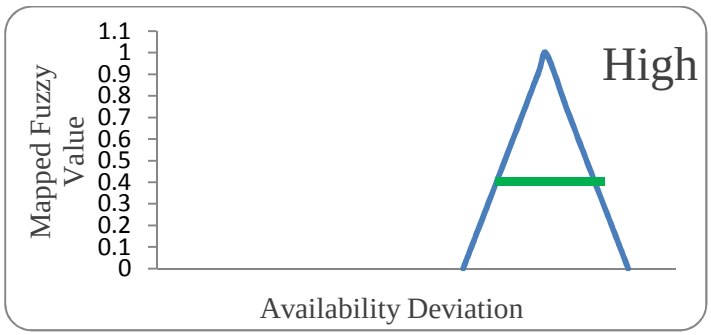

Figure 5.8 Availability Value

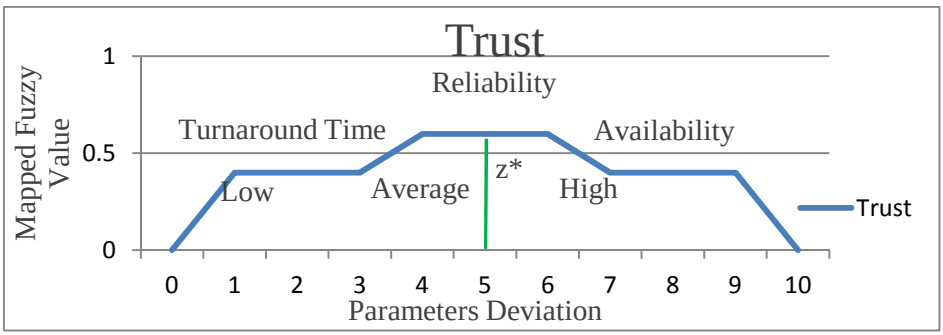

Figure 5.9 Trust Value Calculations

z*=

$$\left[\int_0^1 (0.4z).zdz + \int_1^3 (0.4)zdz + \int_3^4 \frac{(z-0.4)}{2}.zdz + \int_4^6 (0.6z).zdz + \int_6^7 \frac{(z-0.4)}{2}dz + \int_7^9 (0.4z)dz + \int_9^{10} (0.4z).zdz\right]$$

$$\div\left[\int_0^1 (0.4)z.dz + \int_1^3 (0.4z)dz + \int_3^4 \frac{(z-1)}{2}.zdz + \int_4^6 (0.6z)dz + \int_6^7 \frac{(z-1)}{2}.zdz + \int_7^9 (0.4)dz + \int_9^{10} (0.4z)dz\right]$$

= 4.94

So trust lies in the average membership set. Hence, the Trust is average for that provider. So this is how the crisp value of trust is calculated. Trust manager calculates trust values for each cloud provider and then these values are forwarded to the SLA manager. Similarly, trust values are computed for other values as shown in table 5.3. These values can be viewed using fuzzy toolkit available in MATLAB. Rule Viewer is a GUI which shows all the values generated using the Centroid Method. Any value within the range can be passed as an input to the viewer.

Table 5.3 Calculated Trust Values

Turnaround Time	**Availability**	**Reliability**	**Trust Value**
40 (low)	3(low)	0.3(low)	3.51(low)
70(high)	2(low)	0.5(avg)	5.24(Avg)
72.9(high)	6.33(avg)	0.669(avg)	6.4(Avg)
80(high)	7(high)	0.9(high)	8.27(high)
37.95(low)	6.325(avg)	0.668(high)	5.25(avg)
50(avg)	7.0(avg)	0.8(high)	5.24(avg)
47(avg)	3.0(low)	0.65(avg)	5.24(avg)

5.2.4. Experimental Results of rule base:

Fuzzy Inference System (FIS) is implemented using Matlab. The Triangular membership function is selected to define fuzzy sets of all the three parameters and Centroid method of defuzzification is selected using the Matlab fuzzy tool. The range of values for all the parameters is given using the membership function editor tool in Matlab. *Trimf* function is selected to plot a graph. The figure 5.10 shows the membership function editor having range and parameter selector. After that the Inference rules are defined using rule option in edit menu item.

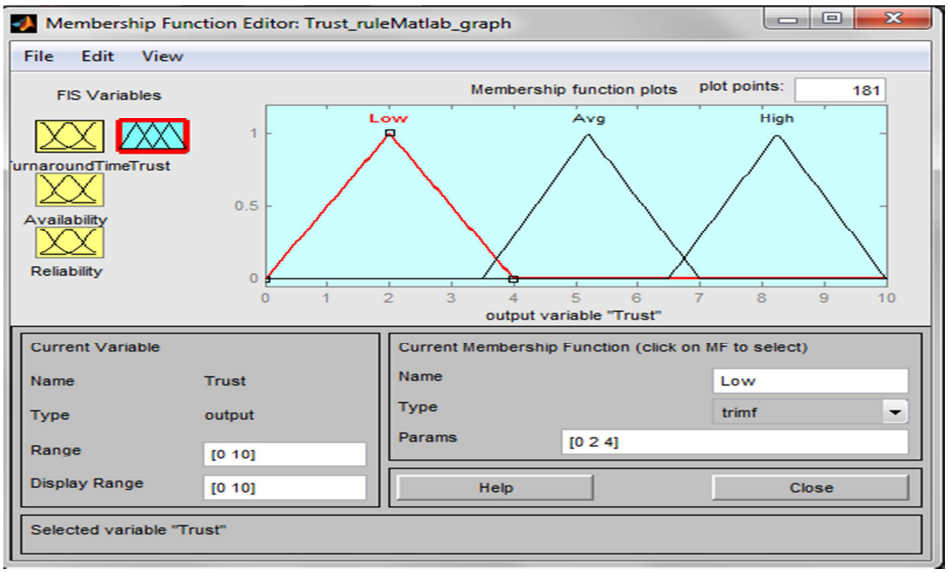

Figure 5.10 Membership Value of Trust

5.2.5 Fuzzy Inference Rules:

Fuzzy Inference Rules are defined below:

Rule -1: If Turnaround time is Low and Availability is Low and Reliability is Low then Trust is Low.

Rule -2: If Turnaround time is Low and Availability is Low and Reliability is Avg then Trust is Avg.

Rule -3: If Turnaround time is Low and Availability is Avg and Reliability is Low then Trust is Low.

Rule -4: If Turnaround time is Low and Availability is Avg and Reliability is Avg then Trust is Avg.

Rule -5: If Turnaround time is Avg and Availability is Low and Reliability is Low then Trust is Low.

Rule -6: If Turnaround time is Avg and Availability is Low and Reliability is Avg then Trust is Avg.

Rule -7: If Turnaround time is Avg and Availability is Avg and Reliability is Low then Trust is Avg.

Rule -8: If Turnaround time is Avg and Availability is Avg and Reliability is Avg then Trust is Avg.

Rule -9: If Turnaround time is High and Availability is Low and Reliability is Low then Trust is Low.

Rule -10: If Turnaround time is High and Availability is Low and Reliability is Avg then Trust is Avg.

Rule -11: If Turnaround time is High and Availability is Avg and Reliability is Low then Trust is Avg.

Rule -12: If Turnaround time is High and Availability is Avg and Reliability is Avg then Trust is Avg.

Rule -13: If Turnaround time is Low and Availability is High and Reliability is Low then Trust is Avg.

Rule -14: If Turnaround time is Low and Availability is High and Reliability is Avg then Trust is Avg.

Rule -15: If Turnaround time is Avg and Availability is High and Reliability is Low then Trust is Avg.

Rule -16: If Turnaround time is Avg and Availability is High and Reliability is Avg then Trust is Avg.

Rule -17: If Turnaround time is Low and Availability is Low and Reliability is High then Trust is Low.

Rule -18: If Turnaround time is Low and Availability is Avg and Reliability is High then Trust is Avg.

Rule -19: If Turnaround time is Avg and Availability is Low and Reliability is High then Trust is Avg.

Rule -20: If Turnaround time is Avg and Availability is Avg and Reliability is High then Trust is Avg.

Rule -21: If Turnaround time is High and Availability is High and Reliability is Low then Trust is Avg.

Rule -22: If Turnaround time is High and Availability is High and Reliability is Avg then Trust is High.

Rule -23: If Turnaround time is Low and Availability is High and Reliability is High then Trust is Avg.

Rule -24: If Turnaround time is low and Availability is Low and Reliability is Low then Trust is Low.

Rule -25: If Turnaround time is High and Availability is High and Reliability is High then Trust is High.

Rule -26: If Turnaround time is High and Availability is Low and Reliability is High then Trust is Avg.

Rule -27: If Turnaround time is High and Availability is Avg and Reliability is High then Trust is Avg.

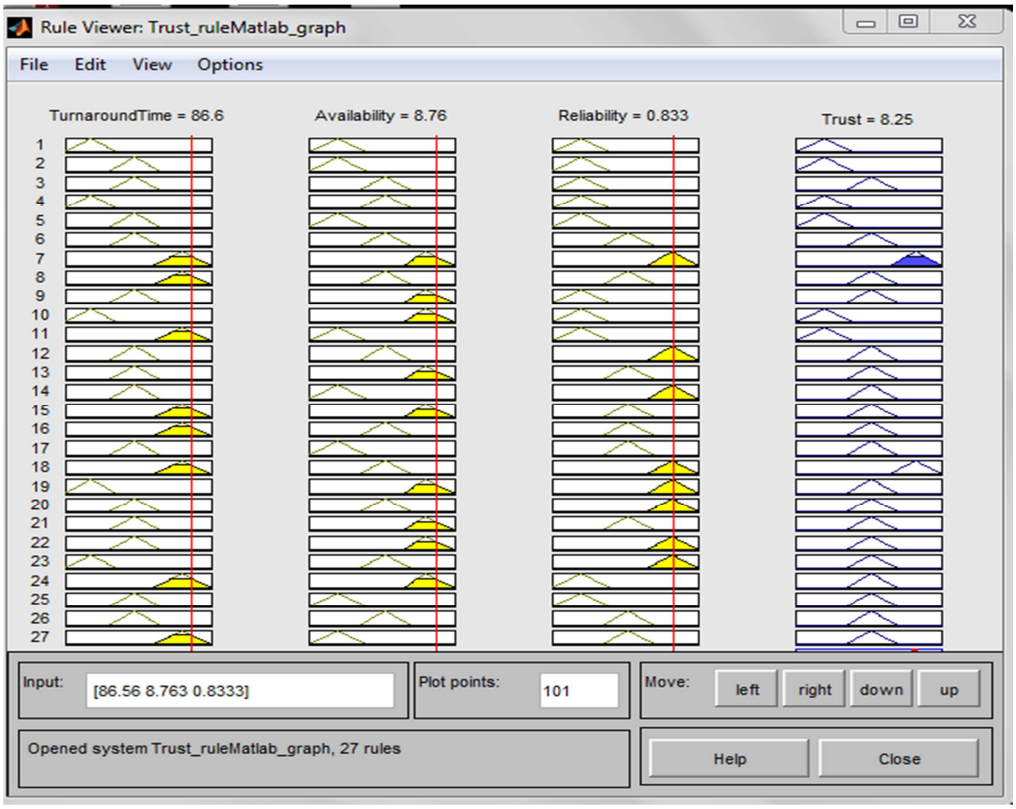

Figure 5.11 Values of QoS Parameters and Trust

The above rules are defined using fuzzy toolkit and saved it in .fis file. Go to View and select rule to see Rule Viewer. The figure 5.11 shows Rule Viewer. Calculated Trust value is also shown and membership also presented in the figure.

5.2.6 FIS Analysis

The Figure 5.12 shows the variation of trust with respect to Reliability and Turnaround time. The figure shows that when Turnaround Time and Reliability goes in low range, the value of trust also goes down. Trust is maximized when the Reliability and Availability is in high range.

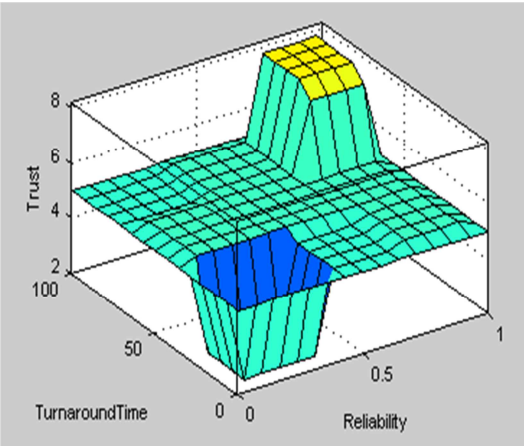

Figure 5.12 Variation of Trust w.r.t. Reliability and Turnaround Time

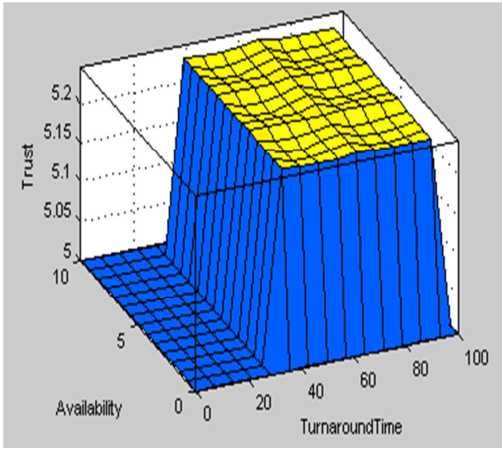

Figure 5.13 Variation of Trust w.r.t Availability and Turnaround time

Similarly, Surface graph is shown for trust w.r.t Availability and Turnaround time in figure 5.13 and Figure 5.14 shows the variation of trust w.r.t Reliability and Availability.

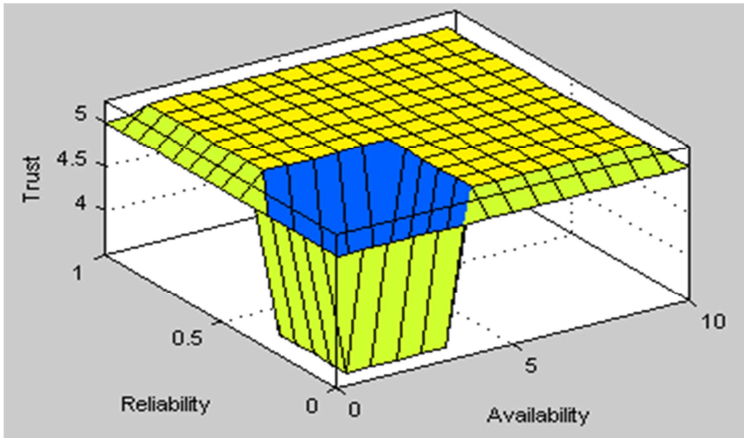

Figure 5.14 Variation of Trust w.r.t Reliability and Availability

5.2.7 Simulation Analysis:

The graphs given below show the variation of QoS parameters w.r.t number of virtual machines, cloudlets and other system configurations. The Reliability of the system is estimated using CloudSim. The figure 5.15 shows that the variation of reliability w.r.t to number of virtual machines. Reliability of the system is first decrease, but after a threshold value the reliability value becomes constant.

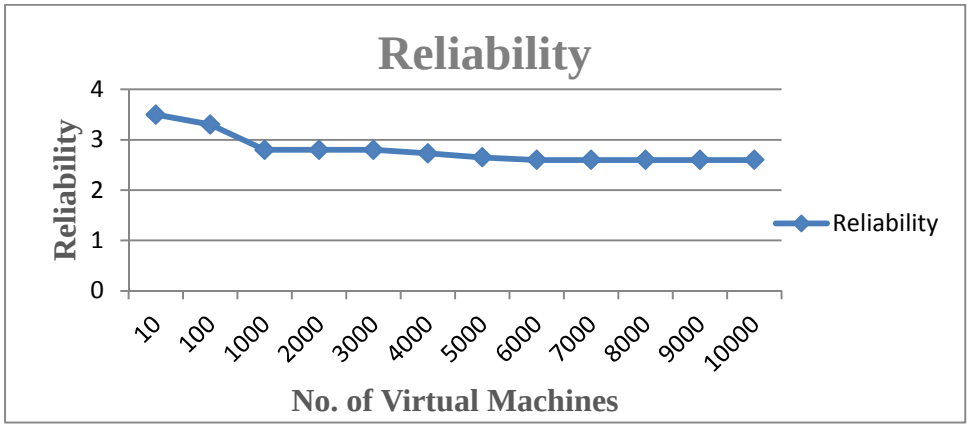

Figure 5.15 Variation of Reliability w.r.t No. of Virtual Machines for Fuzzy Based Approach and Weighted Approach

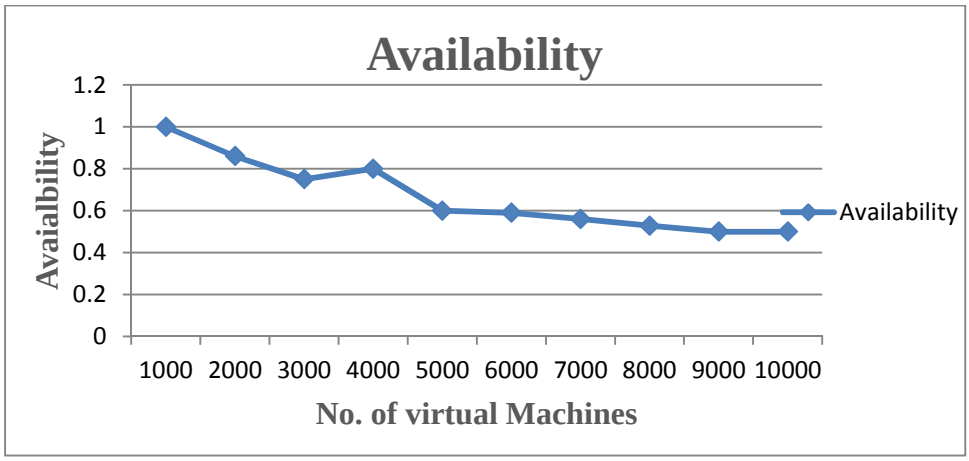

Figure 5.16 Variation of Availability w.r.t No. of Virtual Machines for Fuzzy Based Approach and Weighted Approach

The figure shows that Turnaround time increases with increasing number virtual machines. The values are calculated using CloudSim. CloudSim takes time to create a number of virtual machines on Datacentres and this time increases when the quantity of the virtual machines increases.

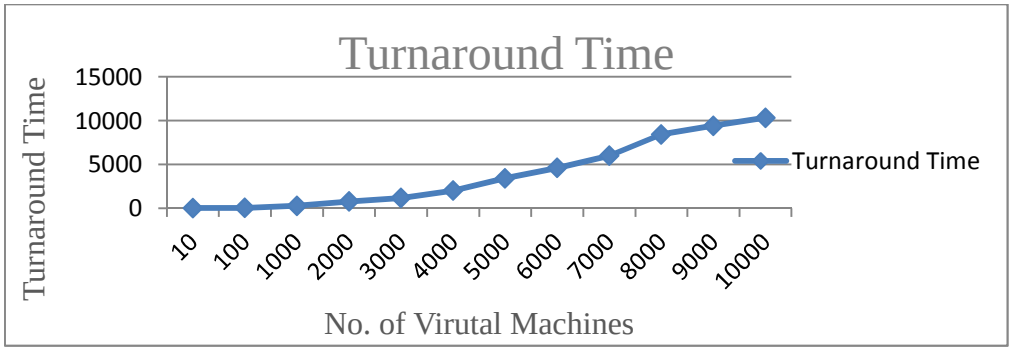

Figure 5.17 variation of Turnaround Time w.r.t No. of Virtual Machines

For Fuzzy Based Approach and Weighted Approach

5.3 Comparison with Weighted Approach

This section presents the comparison between the proposed model and the weighted model, in which the trust is calculated by assigning weights to different parameters without fuzzy logic. The figure 5.18 shows the comparative graphs by taking into account the number of successful transactions in both the models. Our model has a better successful rate than the weighted model, when malicious requests are added to the system. In case of malicious requests, the trust value becomes low and the user will not rely on that provider.

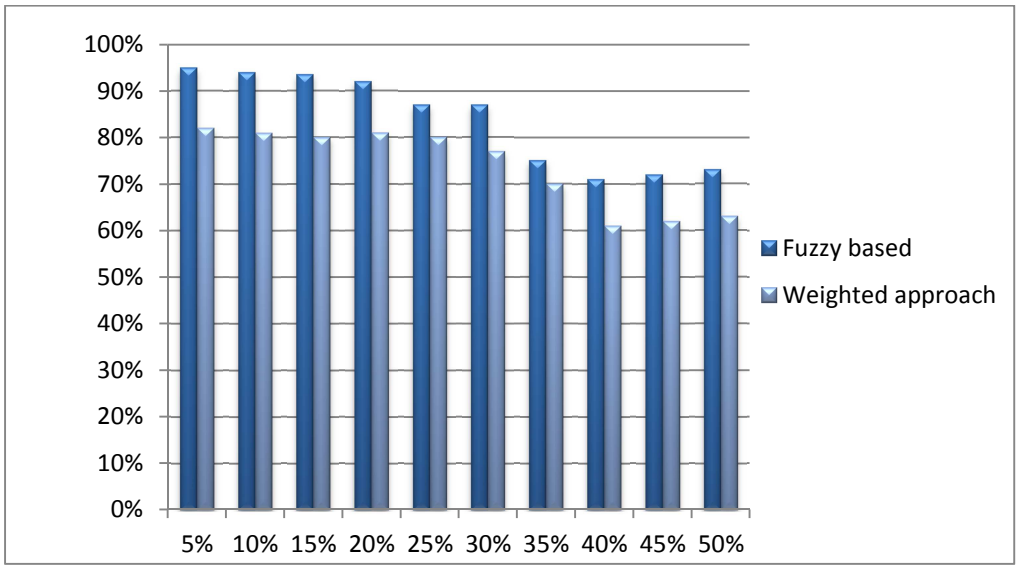

Figure 5.18 Compariosn of Successful Rate between

Fuzzy Based Model and Weighted Trust Model

Chapter 6

Conclusion & Future Scope

6.1 Conclusion

Trust model in cloud computing is the most in-demand mechanism to provide security in cloud computing. In this thesis, a novel model for calculating trust is introduced for cloud computing. The trust value of homogeneous resources, available on the cloud, is calculated on the basis of QoS parameters using a fuzzy logic system.

The simulation and results have shown how the system's reliability is decreased when some malicious task are performed by any user. It is also shown that different configurations and number of cloudlets has an effect on reliability, availability and turnaround time. Finally a comparison is done between our model and Weighted Trust Model by presenting the completed transaction rate and accuracy of output.

6.2 Thesis contribution

In this thesis, the following contributions are presented:

- Different strategies for evaluating trust in cloud atmosphere have been discussed in this thesis.
- A novel trust model is presented which estimate the value of trust using Fuzzy Logic on Quality of Service (QoS) parameters.
- Inference Rules are generated to create a Rule Base for the fuzzy module.
- Both linguistic and real values of trust are generated using this model.
- Trust variation with the QoS parameter is generated using Matlab.
- Variation of QoS parameter with increasing number of virtual machines is analyzed.
- This trust model is compared with the weighted approach and it has given a better performance in terms of trust values.

6.3 Future work

- In the future, we can widen this work to employ in multiple domain cloud atmosphere.

- We can introduce a non-centralized model that would work for a homogeneous set of cloud providers.
- We can employ some other security features to prevent the system from different attacks using separate techniques.
- There are some other parameters to involve in our suggested model in future for optimizing the rules. These parameters are Price comparison, allocation rate, Probability of selection, and security.

Video Presentation

Video Presentation Link → https://youtu.be/E4cNFSx1uXI

References

[1] Cloud Computing Tutorial, [Online], Available: http://www.tutorialspoint.com/cloud_computing/cloud_computing_tutorial.pdf.

[2] R. N. Calheiros, R. Ranjan, A. Beloglazov, C.A. De Rose, and R. Buyya., " CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," *Software: Practice and Experience*, vol. 41(1), pp.23-50, 2011.

[3] R., Buyya, C.S. Yeo, S. Venugopal , J. Broberg, I. Brandic., " Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*; vol. 25(6), pp. 599–616, 2009.

[4] Q. Zhang, L. Cheng, and R. Boutaba., "Cloud computing: state-of-the-art and research challenges," *Journal of internet services and applications*, vol. 1(1), pp.7-18, 2010.

[5] J. Huang and D.M. Nicol., "Trust mechanisms for cloud computing," .*Journal of Cloud Computing*, vol. 2(1), pp.1-14, 2013.

[6] J. Huang, and D.M. Nicol., "A formal-semantics-based calculus of trust," *Internet Computing, IEEE, 14*(5), pp.38-46, 2010.

[7] J. Huang and M.S Fox., "An ontology of trust: formal semantics and transitivity." *In Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet*, pp. 259-270, ACM, 2006.

[8] Zadeh, L.A., 1996., "Fuzzy logic= computing with words." *Transactions on Fuzzy Systems*, IEEE, vol. *4*(2), pp.103-111.

[9] M. Firdhous, O. Ghazali, and S. Hassan., "Trust management in cloud computing: a critical review," *The International Journal on Advances in ICT for Emerging Regions, 2012*

[10] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A Survey of Trust and Reputation Management in Cloud Systems in Wireless Communications", IEEE, vol. 98, pp. 1755-1772, 2010.

[11] Z. Gan, J. He, and Q. Ding, "Trust relationship modelling in e-commerce-based social network," *In proceedings of International conference on computational intelligence and security*, Beijing, China, vol. 1, pp. 206-210, 2009.

[12] D. McKnight and N. Chervany, "Conceptualizing Trust: A Typology and E-Commerce Customer Relationships Model," *In proceedings of 34th Hawaii International Conference on System Sciences*, Island of Maui, HI, USA, 2001.

[13] D. Paoli, Stefano and Gangdharan, G.R. and Kerr, Aphra and D'Andrea, Vincenzo and Serrano, Martin and Botvich, Dmitri, "Toward trust as result: An interdisciplinary approach," *In Proceedings of ALPIS, Sprouts: Working Papers on Information Systems*, vol. 10(8), pp. 1-6, 2010.

[14] M. Akhoondi, J. Habibi, and M. Sayyadi, "Towards a model for inferring trust in heterogeneous social networks," in *Second Asia International Conference on Modelling & Simulation*, Kuala Lumpur, Malaysia, pp. 52-58, 2008.

[15] H. Huang, G. Zhu, and S. Jin, "Revisiting trust and reputation in multi-agent systems," *ISECS International Colloquium on Computing, Communication, Control, and Management*, Guangzhou, China, vol. 1, pp. 424-429, 2008.

[16] L. Mui, "Computational models of trust and reputation:agents, evolutionary games, and social networks," Boston, MA, USA, PhD Thesis 2002.

[17] Q. Zhang, T. Yu, and K. Irwin, "A Classification Scheme for Trust Functions in Reputation-Based Trust Management," *In International Workshop on Trust, Security, and Reputation on the Semantic Web*, Hiroshima, Japan, 2004.

[18] S.K. Chong, J. Abawajy, M. Ahmad, and I.R.A. Hamid., "Enhancing Trust Management in Cloud Environment," *Procedia-Social and Behavioral Sciences*, vol. 129, pp.314-321, 2014.

[19] I. Foster, Y. Zhao, I. Raicu, and S. Lu., "Cloud computing and grid computing 360-degree compared," *Grid Computing Environments Workshop, GCE*, IEEE, pp. 1-10, 2008.

[20] Z. Liu, S.S. Yau, D. Peng, and Y. Yin., "A flexible trust model for distributed service infrastructures," *In proceedings of 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC)*, IEEE, pp. 108-115. 2008.

[21] S. Spitz and Y. Tuchelmann., "A trust model considering the aspects of time." *In Second International Conference on Computer and Electrical Engineering,* ICCEE. vol. 1, pp. 550-554, IEEE, 2009.

[22] X. Wu, J. He, and F. Xu.,"An enhanced trust model based on reputation for P2P networks," *In proceedings of IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing., SUTC'08,* IEEE, pp. 67-73, 2008.

[23] S. Chhabra, E. Damiani, S.D.C di Vimercati, S. Paraboschi, and P. Samarati., "SupP2PRep: A Protocol for Reputation Management via Polling in P2P Networks with SuperPeers".

[24] J. Hu, Q. Wu, and B. Zhou., "FCTrust: a robust and efficient feedback c redibility-based distributed P2P trust model." *In proceedings of the 9th International Conference for Young Computer Scientists, ICYCS* ,IEEE, pp. 1963-1968, 2008.

[25] X. Li, J.S. Valacich, and T.J Hess., "Predicting user trust in information systems: A comparison of competing trust models." *In Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 2004.*IEEE, pp. 10, 2004.

[26] L. Wen, P. Lingdi, L. Kuijun, and C. Xiaoping., "Trust model of users' behavior in trustworthy internet," *In proceedings of WASE International Conference on Information Engineering, ICIE'09,* IEEE, vol. 1, pp. 403-406, 2009.

[27] W. Yang, C. Huang, B. Wang, T. Wang and Z. Zhang., "A General trust model based on trust algebra," *In proceedings of International Conference on Multimedia Information Networking and Security*, IEEE, pp. 125-129, 2009.

[28] S. Dorri Nogoorani, and R. Jalili., "Uncertainty in probabilistic trust models," *In proceedings of 26th International Conference on, Advanced Information Networking and Applications (AINA),* IEEE, pp. 511-517, 2012.

[29] P. Manuel., "A trust model of cloud computing based on Quality of Service." *Annals of Operations Research*, vol. 233(1), pp. 281-292, 2015.

[30] Guo, Q., Sun, D., Chang, G., Sun, L. and Wang, X., January., "Modeling and evaluation of trust in cloud computing environments," *In proceedings of* 3rd *International Conference on Advanced Computer Control (ICACC) IEEE, pp.* 112-116, 2011.

[31] Li, X. and Du, J., "Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing," *Information Security, IET*,vol. 7(1), pp. 39-50, 2013.

[32] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani., "An efficient distributed trust model for wireless sensor networks," *In Transactions on Parallel and Distributed Systems*, IEEE, vol. 26(5), pp. 1228-1237, 2015.

[33] P.D. Manuel, S.T Selvi, and M.E Barr., "Trust management system for grid and cloud resources," *In proceedings of First International Conference on Advanced Computing, ICAC*, pp. 176-181, IEEE, 2009.

[34] P. Varalakshmi, S.T. Selvi, A.J Ashraf, and K. Karthick., "B-tree based trust model for resource selection in grid," *In proceedings of International Conference on Signal Processing, Communications and Networking, ICSCN'07,* pp. 222-227, 2007.

[35] G. Theodorakopoulos and J.S Baras., "On trust models and trust evaluation metrics for ad hoc networks," *In proceedings of Journal on Selected Areas in Communications*, IEEE, vol. 24(2), pp.318-328, 2006.

[36] J. Luo, X. Liu, and M. Fan, "A trust model based on fuzz recommendation for mobile ad-hoc networks," *In Journal of Computer Networks*, vol. 53(14), pp. 2396-2407, 2009.

[37] J. Abawajy., "Establishing trust in hybrid cloud computing environments," *In proceedings of 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom),* IEEE, pp. 118-125, 2011.

[38] W. Han-Zhang and H. Liu-Sheng., October., "An improved trusted cloud computing platform model based on DAA and privacy CA scheme," *In proceedings of International Conference on computer Application and System Modeling (ICCASM),* IEEE, vol. 13, pp.13-33, 2010.

[39] K. Hwang, S. Kulkareni, and Y. Hu. ,"Cloud security with virtualized defense and reputation-based trust management," *In proceedings of Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, DASC'09,* IEEE, pp. 717-722, 2009.

[40] Q. Zhang, L. Cheng, and R. Boutaba., "Cloud computing: state-of-the-art and research challenges," *The Journal of Internet Services and Applications*, pp. 7-18, 2010.

[41] S. Pearson., "Privacy, security and trust in cloud computing," *In* proceedings *of Privacy and Security for Cloud Computing*, Springer London. pp. 3-42, 2012.

[42] D. Zissis, and D. Lekkas, "Addressing cloud computing security issues," *Future Generation computer systems*, vol. 28(3), *pp.* 583-592, 2012.

[43] M. Firdhous, O. Ghazali, and S. Hassan., "Trust management in cloud computing: a critical review," *In the International Journal on Advances in ICT for Emerging Regions.2012*

[44] J. Huang and D.M. Nicol., "Trust mechanisms for cloud computing," *.Journal of Cloud Computing: Advances, Systems and Applications*, vol. 2(1), pp. 1-14, 2013.

[45] X. Sun, G. Chang and F. Li, "A trust management model to enhance security of cloud computing environments," *In proceedings of Second International Conference on Networking and Distributed Computing (ICNDC) IEEE,* pp. 244-248, 2011.

[46] L. Gu, C. Wang, Y. Zhang, J. Zhong, and Z. Ni., "Trust Model in Cloud Computing Environment Based on Fuzzy Theory," *International Journal of Computers Communications & Control*, vol. 9(5), pp. 570-583, 2014.

[47] H. Xia, Z. Jia, and E.H. Sha., "Research of trust model based on fuzzy theory in mobile ad hoc networks." *Information Security, IET*, vol. 8(2), pp. 88-103, 2014.

[48] S. Wang, L. Zhang, N. Ma, and S. Wang., "An evaluation approach of subjective trust based on cloud model," *In proceedings of International Conference on Computer Science and Software Engineering*, IEEE, vol. 3, pp.1062-1068, 2008.

[49] I.B. Türkşen., "Fuzzy logic: review of recent concerns," *In proceeding of International Conference on Computational Cybernetics and Simulation Systems, Man, and Cybernetics*, IEEE, vol. 3, pp. 2975-2978, 1997.

[50] D. Ramot, Friedman, M., Langholz, G. and Kandel, A, "Complex Fuzzy Logic," *Fuzzy Systems, IEEE Transactions on*, vol. 11(4), pp.450-461, 2003.

[51] J. Yen., “Fuzzy logic-a modern perspective,” *Knowledge and Data Engineering, IEEE Transactions on*, vol 11(1), pp.153-165.

[52] T.P Hong and C.Y. Lee, “Induction of fuzzy rules and membership functions from training examples,” *Journal of Fuzzy sets and Systems*, vol. 84(1), pp. 33-47, 1996.

[53] W. Pedrycz., “Why triangular membership functions?.” *Fuzzy sets and Systems*, vol. 64(1), pp.21-30, 1994.

[54] Y.M. Wang., “Centroid defuzzification and the maximizing set and minimizing set ranking based on alpha level sets,” *Computers & Industrial Engineering*, vol. *57*(1), pp.228-236, 2009.

List of Publications

Ritu and Dr. Sushma Jain, “A Trust Model in Cloud Computing based on fuzzy Logic”, 2016 Recent Trends in Electronics, Information & communication Technology (RTEICT), IEEE Explore,2016, [**To be published**]