

TR-SS Algorithm for Secure Resource Allocation in Cloud Computing

¹C.Kamalanathan, ²Dr.R.S.Valarmathi, ³S. Karthick and ⁴R.Nirmalkumar.

¹Assistant Professor (Sl.G), Department of Electronics and Communication Engineering,
Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India.

²Senior Professor, Department of Electronics and Communication Engineering,
Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India.

³Assistant Professor (Sr.G), Department of Electronics and Communication Engineering,
Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India.

⁴Assistant Professor (Sr.G), Department of Electronics and Communication Engineering,
Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India.

¹kamalanadhan@gmail.com, ²atrmathy@gmail.com, ³karthickapplied@gmail.com,
⁴nirmalkumarr@bitsathy.ac.in.

Abstract: Cloud Computing is one of the vibrant technologies in recent times. It has become a prominent paradigm of computing and IT services delivery utility due to its advantages of high computing power, low cost services, high performance, scalability, accessibility and easy availability. In recent years, the demand for cloud computing has forced the development of new market offerings involved in various cloud service and delivery models. Moving data into the cloud offers greater convenience since users are not required to be aware about the storage capacity, storing techniques, hardware management, or data maintenance. Online storage services of the cloud offers flexible and customizable services that make data storage and management much easier and more accessible. Cloud computing has widely adapted by both the enterprises and individuals where several security issues have to be solved. To design and develop a fuzzy logic and neural network based TR model for safe resource allocation in cloud computing is the most important objective of this research. The TR model is the trust manager and reputation manager employed in our proposed approach.

Keywords: Fuzzy Logic, Security, Threshold, Resource Block, Resource Center.

1. Introduction

In recent years, With the advancement in dynamic distributed technology, deliberation of security in resource allocation is a major part of the research on cloud computing[. Cloud computing is an internet-based comprehensive computing solution that delivers IT as a service where resources are shared. Service delivery model provides internet based services, computing and storage for users mostly in financial, health care and government. The cloud computing flexibility is how to allocate available resources on demand[4]. Cloud computing can provide organizations

with the means and methods needed to ensure financial stability and high quality service. There must be global cooperation if the cloud computing process is to attain optimal security and general operational standards. With the advent of cloud computing it is considered to be very important revolution for all but this revolution needs to be strongly protected. In cloud computing, there are numerous security issues as it covers a lot of technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, the security issues for some of these

systems and technologies are not dealt up to the limit. To launch the patterns and trends to improve the quality, there is an essential necessity to securely store, manage, share and examine large amount of complex information. Due to the critical nature of the applications, it is essential that the clouds to be protected[6]. Cloud computing is a model for enabling ubiquitous network access tend to focus on maximizing the effectiveness of the shared pool of configurable computing resources. A key issue that needs special attention is security of clouds. These issues arise during the deployment of mostly public cloud because in public cloud infrastructure, customer is unaware of the location and nature of the data stored on the internet. There are many security threats at different levels, such as threats at Cloud Service Provider (CSP) Level, Network Level and User/Host Level. Existing approaches for secured outsourcing of data and arbitrary computations are either based on a single tamper-proof hardware, or based on recently proposed fully homomorphic encryption. The hardware based solutions are not scalable, and fully homomorphic encryption is currently only applicable theoretically interest and hence inefficient. The proposed research addresses security challenges in cloud computing and provide solutions to overcome these drawbacks. To give reliable security to the users, this work provides a coherent framework for research in the field of large scale data analysis on cloud computing systems using trust and reputation factors. There are many security threats at different levels, with the a cloud computing has become a highlight for the IT specialists due to the potentiality to transform. To execute this technology, immense steps had been taken.

For secure resource allocation in cloud computing, a fuzzy logic and neural network based trust and reputation model is proposed. Trust and reputation manager's is used to gather the characteristic values for the trust and reputation factors from the users after employing a resource. At first, users will present a task through the scheduling manager. The scheduling manager after receiving the user's request, it expresses to the related resource center which the task necessitates to complete. The user requires accessing a resource block in a resource center to execute a task. After carrying out the task, a form will be given to the user to fill the characteristics values for the trust factor and reputation factor based on the experience. These characteristic values are applied to work out the security. The trust factor value and the reputation factor value for the resource center is calculated based on the characteristic values and given as input to the fuzzy logic system. The fuzzy logic system offer the score value for the resource center based on the trust factor and reputation factor we present as input. From the score value we make a decision whether a resource center is protected or not.

This work involves with two objectives is as follows:

- To develop a mathematical model for computing the trust and reputation factor's based on the attribute values.

- To propose a TR-SS algorithm i.e. trusts and reputations based security score algorithm.

2. Related Works

This segment demonstrates a few of the researches seen in the literature for trust based secure model and trust reputation system in cloud computing and grid computing environment. For different distributed system, a trust model has been suggested by Mohamed Firdhous *et al.* [1]. The trust management systems suggested for cloud computing had been examined with particular emphasis on their ability, applicability in sensible heterogonous cloud environment and implementability. It was found that not any of the systems was based on solid theoretical foundation during the assessment of those systems and furthermore does not take any superiority of service characteristic for forming the trust scores. Therefore, solid theoretical groundwork for building trust models for cloud computing was necessary. A physical cloud computing security architecture has been proposed by Alok Tripathi and Abhinav Mishra [2]. Cloud security was turning into a chief differentiator and aggressive edge amid cloud providers. They have discovered the security issues that happen in a cloud computing frame work. It spotlighted on technical security aspect arising from the practice of cloud services and in addition offered a summary of main security aspect related to cloud computing with the outlook of a secure cloud architecture environment. Proactive enterprises and service providers used this security on their cloud infrastructure, to attain security so that they were taken benefit of cloud computing in front of their competitors.

Safwan Mahmud Khan and Kevin W. Hamlen [3] have offered and assessed Hatman: the first full- scale, data-centric, reputation depended trust management system for Hadoop clouds. By distinguishing the job replica effects for steadiness, Hatman vigorously estimates node integrity. These capitulated agreement feedbacks for a trust manager rely on EigenTrust. Low overhead and high scalability had been attained by creating both consistency-checking and trust management as secure cloud computations; as a result, the cloud's disseminated computing power was influenced to make stronger its protection. For a cloud computing marketplace, a multi-faceted Trust Management (TM) system structural design has been proposed by Sheikh Mahbub Habib *et al.* [5]. This system offers to identify the trustworthy cloud providers based on different characteristics (e.g., security, performance, compliance) estimated by abundant sources and roots of trust information.

Shanshan Song *et al* [7] have suggested that trusted Grid computing stress robust resource allotment with security assurance at all resource sites. By lack of security guarantee from isolated resource sites, Large-scale Grid applications were being holdedup. They have formed a security-binding system through site reputation measurement and trust integration across

Grid sites. They didn't take care of the trust factor deterministically. As a substitute, they have employed fuzzy theory to deal with the fuzziness or uncertainties following all trust characteristics. The combining was reached by repeated replace of site security information and matchmaking to please user job demands. PKI-based trust system assists Grids in multi-site verification and single sign-on operations. On the other hand, cross certificates were not sufficient to review local security conditions at Grid sites. For disseminated trust aggregation, they have proposed a fuzzy-logic trust system through fuzzification and integration of security characteristics. They have brought in the trust index of a Grid site, which was resolute by site reputation from its track record and self-defense potential attributed to the risk conditions and hardware and software defenses arranged at a Grid site.

Vivekananth.P [8] has suggested that grid system was a vibrant environment where all things shared the resources issued by the other entities. The system permits the synchronized and aggregated apply of geographically disseminated resources, often owned by independent organizations, for working out large-scale issues in science, engineering. Conversely, application composition, resource management and scheduling in those environments were a complex process. Before beginning any transaction, the resource provider as well as the user should be convinced. Mutual trust must be created among the user and the provider. Trust was built on repute. The idea of reputation was eye-catching in peer to peer networks. However, yet it was not flawless in grid computing. They have offered an outline of available reputation based systems for resource selection.

Bao Rong Chang, Hsiu-Fen Tsai, Chia-Yen Chen, & Yun-Che Tsail [15] have proposed the two benchmark Enterprise Resources Planning systems such as in-house ECC 6.0 and in-cloud. By designing an Access control authentication design in the cloud computing system to prevent the service-oriented hosts from external fraud or intrusion. They introduced high availability architecture to build an in-cloud services solution to overcome the crucial problem of unexpected down-time or system failure that will cause data loss and system termination.

Berstein, D, Ludvigson, E, Sankar, K, Diamond, S & Morrow M [16], Different protocols and formats which are required to be standardized to solve some specific use cases in cloud computing interoperability was attempted. One use case involving a physical metaphor (server, disks, network segment etc) and another use case involving an abstract metaphor (message queue, blob storage, email functions etc.). Authors also detail specific technology which can be applied to cloud computing interoperability. Some of the protocols and technologies highlighted are Location Identity Separation Protocol for addressing, IPA for naming, identity and trust, XMPP for presence and messaging, Virt-Image, OVF and Libvirt for virtual machines and AMQP based message bus for Reliable Application Transport.

Ignacio Aransay, Marina Zapater, Patricia Arroba, and Jose M. Moya, [17], Energy challenge by a temperature-aware VM allocation policy based on a Trust-and- Reputation System is attempted. A TRS meets the requirements for inherently distributed environments such as data centers, and allows the implementation of autonomous and scalable VM allocation techniques. The increasing success of Cloud Computing applications and online services has contributed to the unsustainability of data center facilities in terms of energy consumption. The relationships between the different computational entities, synthesizing this information in one single metric were proposed. This metric, called reputation would be used to optimize the allocation of VMs in order to reduce energy consumption. The VM allocation problem can be seen as a decision making process to take the best option in order to meet different objectives, i.e., maximizing QoS, minimizing energy consumption.

Raghavendra Achar & Santhi Thilagam P [18], a broker based architecture for selecting suitable cloud provider from multiple providers is proposed. The broker measures the quality of each cloud provider and prioritizes them based on the needs of the requester. In order to differentiate one cloud provider from another, Cloud Services Measurement Initiative Consortium (CSMIC) has developed the Service Measurement Index (SMI).

The SMI is a framework and method for computing relative index, which can be used by the requester to distinguish one cloud service from others (Raghavendra Achar & Santhi Thilagam P 2014). SMI is one of the standard methods to measure cloud service based on requester's critical business requirements. Measures are being defined which enable the use of cloud service providers data for cloud service selection decision.

Raghavendra Achar & Santhi Thilagam P [19], There are some high level attributes are considered like Accountability, Agility, Cost, Performance, Assurance, Security and Privacy, Integrity, Usability. By Selecting a suitable cloud provider from multiple cloud providers involves multiple criteria and interdependent relationship between them. It is Multiple Criteria Decision- Making (MCDM) problem. Author proposed the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) based ranking mechanism in order to select a suitable cloud provider. The selection of suitable cloud provider involves 3 steps. 1) Identifying the suitable criteria 2) Evaluating the weight of criteria using AHP 3) Ranking cloud providers using TOPSIS.

3. Requirement for Security in Resource Allocation of Cloud Computing

To improve the quality of the database, there is a necessity to securely store, manage, share and examine large amount of complex information. Based on the nature of applications, it is important that the

clouds to be secured. The key aspect of the security of the cloud system is that the owner of the data may not know the location of the data, where the data is situated. The cause is that if one need utilizing the benefits of cloud computing, one should besides utilize the resource allocation and scheduling presented by clouds. Consequently, it is required to protect the data in the middle of third party process location. The emerging cloud computing system challenges to deal with the growth of internet connected tools and manage huge amount of data. To simplify the vast quantity of data on commodity hardware, Google has offered the MapReduce framework. HDFS is (Apache's Hadoop allocated File System) emerging superior software component for cloud computing combined with MapReduce. The necessity to enhance the human intellectual clarification and conclusion makes abilities that have produced in the development of semantic web which is an idea that efforts to convert the web from its current, only human readable form to machine processable form. This in turn has produced in numerous social networking sites with massive amount of information to be shared and managed.

For cloud computing, there are numerous security issues as it covers a lot of technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, the security issues for some of these systems and technologies are related to cloud computing. For example, the networks that intertwine the systems in a cloud have to be safe. Besides, the virtualization paradigm in cloud computing consequences in a number of security concerns. For design, mapping the virtual machines to the physician machines has to be executed firmly. The protected resource allocation in cloud computing can offer the user to browse decisively. The user can moreover keep their information safe. By this novel method user can judge about a resource center whether protected or not based on the security score.

4. Proposed Resource Allocation in CC

Fuzzy and Neural network based trust and reputation model for the allocation of resource in cloud computing technique is proposed. The Fig.1 shows structure of our proposed model. It comprise users, a scheduling manager (SM), a trust manager(TM), a reputation manager (RM) and resource centers (RC's) that has number of resource blocks. To access the resource block, the users proposed a task which is in the resource center through the scheduling manager. The scheduling manager makes sure the location of the resource block and where it is situated, the scheduling manager provides the path to the related resource center. The user presents the attributes value from (0 to 1) for the trust factor and the reputation factor after access the resource block. The trust and reputation factor value are then given to the fuzzy logic system and then neural network to acquire the security score.

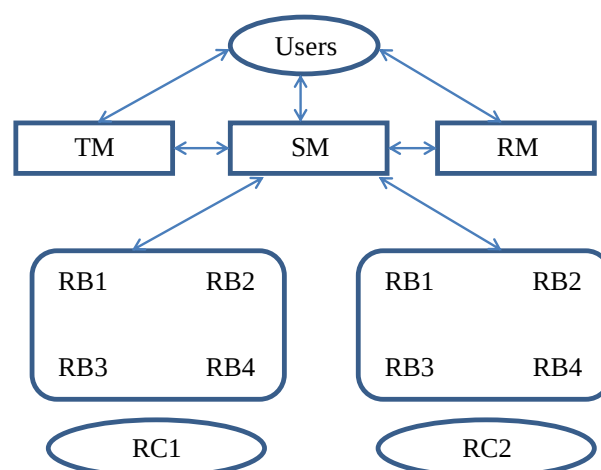


Fig.1 Structure of Proposed Technique

Where, TM – Trust Manager, SM – Scheduling Manager, RM – Reputation Manager, RB1to RB4 – Resource Block 1to 4, RC1 & RC2 – Resource Center 1 & 2.

The proposed approach aims for secure scheduling of incoming request based on the trust factor value in the available resource center. The trust factor value of each resource block is calculated through its trust factor attribute values given by each user and weight value of each trust factor. Based on their contribution to security, a weightage is given to all the security factors and aggregated to compute trust factor. The values of the attributes differ in the range between 0 to 1 and used for calculating the trust factor by trial and error method.

4.1. Trust Factor of Resource Center

The total sum of the resource center is the trust factor of individual resource block in the resource center. Trust is an important factor in both human society and Internet security. Trusting someone is very important when sharing the data. Trust can be termed as assurance that a particular party would work in an expected manner in spite of monitoring or controlling the party. Trust is regarded positive and presents good result in uncertain environments. Generally, there has a grey region in expressing the dependability of a computer site [13]. Related to the human relationship, trust is specified by a verbal term rather numerically. Trust would get fluctuate based on time and environment. Farag Azzedin and Muthucumaru Maheswaran [12] presented the definition for the trust and it is as follows: Trust is a strong opinion in proficiency of an entity to act as expected and the strong opinion is not a fixed value related with the entity but rather it is subject to the entity's attitude and employs only inside a particular context at a specified time. The tough opinion can be described as a dynamic value that is found to distance over a set of values vary from very trustworthy to really untrustworthy. Based on the previous experience and is offered for a particular context, the trust factor is formed. The trust factor is based on the specified time

instance, as the trust level relating two entities is not significant to be similar for today when compared to a year ago. A few of the characteristics we regarded for the trust factor are as follows:

- Anti-virus Capability
- Firewall Capability
- Secured Job Execution
- Copyright date
- Corporate logos
- About Us
- Privacy Policy
- Business Address

Table 1. Weight values for attributes

Attributes	Characteristics	Weight value (w_i)
Anti-virus Capabilities	Capability of the resource to guard against viruses and malicious codes	0.85
Copyright date	Ability to protect the resource from other network accesses	0.70
Firewall Capabilities	Ability of the resources to guarantee the secure implementation of a job	0.9
Corporate logos	Users trust shopping with repeatedly revised websites	0.65

Secured Job Execution	Incorporate the company logos on your website	0.75
About Us	About us page demonstrates the detailed history of the company & user may trust based on history	0.50
Privacy Policy	Includes a considerable degree of trust & respect the customer's personal information	0.80

The trust factor is the sum of each resource blocks in each resource center. The computation of trust factor of each resource block is as follows:

$$TF_k(rb) = p_a \sum_{i=1}^m \left(\sum_{j=1}^u \frac{x_{ij} w_i}{TW} \right) \rightarrow (1)$$

where,

$TF_k(rb) \rightarrow$ Trust Factor of resource block

$p_a \rightarrow$ Probability of users applied the resource block

$x_{ij} \rightarrow$ Trust Factor characteristic values given by each user

$w_i \rightarrow$ Weight value of each trust factor characteristics (0.85, 0.70, 0.90, 0.65, 0.75, 0.50, 0.80)

$TW \rightarrow$ Total weight value

$m \rightarrow$ Total number of characteristics regarded for trust factor

$u \rightarrow$ Total number of users

The total weight value of the characteristics. It is the sum of the weight values of every characteristic.

$$Total\ Weight = \sum_{i=1}^m Weight\ value\ (w_i) \rightarrow (2)$$

To find the trust factor of a resource center is the sum of every resource block in a resource center. The summation of resource blocks in a resource center is the total of trust factor in a resource center. The resource center consist of the resource block, each resource block consist of attribute and its characteristics. For example, in Fig.1, the first resource center has four resource blocks and to locate the trust factor of the first resource center, the trust factor value of all the four resource blocks. The trust factor for the resource center is computed as follows:

$$TF(rc) = \sum_{k=1}^N TF_k(rb) \rightarrow (3)$$

where,

$TF(rc) \rightarrow$ Trust Factor of a resource center

$N \rightarrow$ Total number of resource blocks in a resource center

4.2. Reputation Factor of a Resource Center

The reputation mechanism is one of the most important methods which form the basis for the allocated application and system safety, for its improved scalability and liveness. One can trust another on basis of good reputance since of the fact. Reputation is a measure of trustworthiness in the sense of reliability. For generating trust through social control lacking of trusting third parties, reputation system [14]. The reputation mechanism gives a strategy about the past experience of entities by creating trust through social control by means of the community based feedback. Farag Azzedin and Muthucumaru Maheswaran [12] described that reputation of an entity is an anticipation of its attitude based on other entities examinations or information about the entity's past attitude at a specified time. A few of the reputation characteristics we regarded for reputation factor are as follows:

- Consistency
- Confidentiality
- Robustness
- Contents look current
- Rapid Response
- Trust symbols
- Return Policy

Table 2. Weight values for attributes

Attributes	Characteristics	Weight value (w_i)
Consistency	The ability of the resource to execute the anticipated function for a particular period of time	0.85
Confidentiality	The ability of concealing information from unauthorized users	0.70
Robustness	The ability of the system to stay alive from the assaults	0.9
Contents look current	If the website is in old format, the users will pay no attention to it.	0.65

Attributes	Characteristics	Weight value (w_i)
Rapid Response	The fast reply of a webpage will raise the reputation of the webpage.	0.75
Trust symbols	Trust symbols in the web page demonstrates the users that the web page is guarded against the hackers and viruses	0.50
Return Policy	Provides the users comfort of knowing that they can return the product if it is imperfect or they are sad with it	0.80

The reputation factor of a resource center is computed by the summation of every resource block in a resource center. The reputation factor for the resource center is calculated as below:

$$RF(rc) = \sum_{k=1}^N RF_k(rb) \quad \rightarrow (4)$$

where,

$RF(rc)$ → Reputation Factor of a resource center

$RF_k(rb)$ → Reputation Factor of each resource block in a resource center

N → Total number of resource blocks in a resource center

To find the reputation factor for the resource center, we should find the reputation factor for each resource block in the resource center. The formula to assess the reputation factor for each resource block in a resource center is as follows:

$$RF_k(rb) = P_a \sum_{i=1}^n \left(\sum_{j=1}^u \frac{y_{ij} l_i}{z} \right) \quad \rightarrow (5)$$

where,

P_a → Probability of users applied the resource block

y_{ij} → Reputation Factor characteristics values specified by the user

l_i → Weight value of each reputation factor characteristics

z → Total weight value of the characteristics regarded for reputation factor

n → Total number of characteristics regarded for reputation factor

u → Total number of users

The computation of total weight value z is the sum of the characteristics of the attributes, the reputation factor is specified below.

$$Total\ Weight = \sum_{i=1}^n Weight\ value\ (l_i) \quad \rightarrow (6)$$

4.3. Fuzzy Logic Model

Soft computing tools such as fuzzy logic are one of the important techniques that is to achieve high level security. It possesses non-linear mapping capabilities and can deal with uncertainties in the systems parameters. Although fuzzy logic deals with imprecise information, the information is processed in sound mathematical theory.

The fuzzy logic system is summarized into three main stages namely 1) Fuzzification where membership functions are used to graphically describe a situation, 2) Evaluation of Rules where it represents the application of the fuzzy logic rules and 3) Defuzzification obtains the crisp results. The benefits of fuzzy logic include its simplicity and its flexibility.

The fuzzy logic model, the Trust Factor value $TF(rc)$ and the Reputation Factor value $RF(rc)$ are giving as input to the fuzzy logic system to find out the security score of the resource center. The Fig.2 Input and Output of Fuzzy Logic System used in proposed technique.

Resource Centre	Level	Range	Security score value	Centre of Gravity
Trust factor	Low	0 to 12000	0.0 to 0.3	0
	High	12000 to 20000	0.3 to 0.7	0.66
	Extreme	20000 to 40000	0.7 to 1.0	0.66
Reputation factor	Low	0 to 12000	0.0 to 0.3	0
	High	12000 to 20000	0.3 to 0.7	0.66
	Extreme	20000 to 40000	0.7 to 1.0	0.66

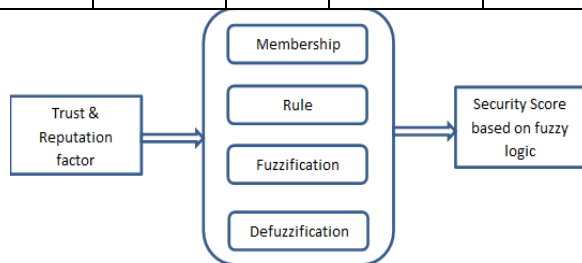


Fig.2 Input and Output of Fuzzy Logic System used in proposed Technique

The membership functions in the fuzzy logic systems are used to map the input variables. The changing of input value to membership value is called fuzzification. The fuzzification in the fuzzy logic system based on the rule and the defuzzification is also based on rule. After defuzzification, to find a single output for the specified number of inputs. In Fig.2, the trust and the reputation factor as input to the fuzzy logic system. The fuzzy logic system at first uses the input values of the membership functions and the fuzzification and defuzzification will be completed based on the rule. The ultimate output we obtain from the fuzzy logic system is the security score based on fuzzy logic system. It is signified by an equation beneath:

$$FL\ Score = TF(rc) \times RF(rc) \rightarrow (7)$$

Where,

$FL_{Score} \rightarrow$ Score attained from fuzzy logic system

$TF(rc) \rightarrow$ Trust Factor as input to fuzzy logic system

$RF(rc) \rightarrow$ Reputation Factor as input to fuzzy logic system

Table 3. Score value from fuzzy system results

Table 3. Shows score value from the fuzzy logic systems, the trust factor and reputation are considered as low, high and extreme levels. When low level, the range is between 0 to 12000, the security score level is from 0.0 to 0.3 and the centre of gravity is attained as 0. Due to the low centre of gravity, providing more security is required.

If the trust factor is low or reputation factor is low, then the score value comes to low, so there is a need of more security requirement for the resource center. If the trust factor is extreme or reputation factor is high, then the score value comes to high, so the resource center is protected.

4.4. Neural Network (NN) Model

Neural Network is an artificial computing system made up of a number of simple, highly interconnected processing elements which process information by their dynamic state response to external inputs. Neural networks are organized as layers. Layers are made up of a number of interconnected elements/nodes which contain an 'activation function'. Input patterns are presented to the network via the 'input layer', which communicates to one or more 'hidden layers' where the actual processing is done via a system of weighted 'connections'.

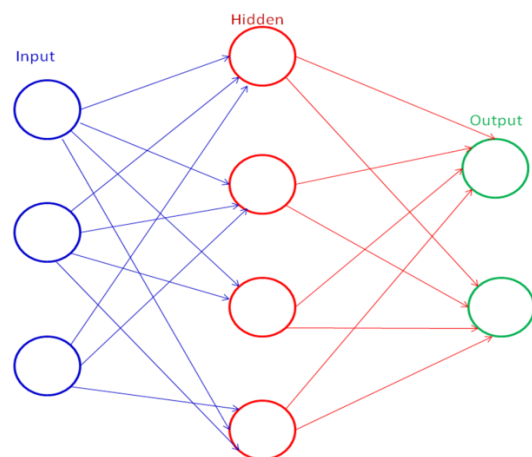


Fig.2 Structure of Neural Network

The trust and the reputation factor values are given to the neural network to get the security score from the fuzzy logic system. To train a neural network Back Propagation method is used. The neural network learns a predefined set of input-output pairs. two input neurons are used in the input layer and four neurons in

the hidden layer and finally one neuron in the output layer. An input pattern has been applied as a stimulus to the first layer of network units, it is propagated through upper layer until an output is generated. The output pattern is then compared to the desired output, and an error signal is computed for each output unit.

The error signals are then transmitted backward from the output layer to each node in the intermediate layer that contributes directly to the output. Each unit in the intermediate layer receives only a portion of the total error signal, based roughly on relative contribution the unit made to the original output. This process repeats layer by layer until each node in the network has received an error signal that describes relative contribution to the total error. Based on the error signal received, connection weights are then updated by each unit to cause the network to converge toward a state that allows all the training patterns to be encoded. The network trains the nodes in the intermediate layers and organizes themselves such that different nodes learn to recognize different features of the total input space. After training, when presented with an arbitrary input pattern that is noisy or incomplete, the units in the hidden layers of the networks will respond with an active output if the new input contains a pattern that resembles the feature the individual units learned to recognize during training. The hidden layer units have a tendency to inhibit their outputs if the input pattern does not contain the feature that they are trained to recognize. The signals propagate through the different layers in the network, the activity pattern present at each upper layer can be identified as a pattern with features that can be recognized by units in the subsequent layer. The output pattern generated can be thought of as a feature map that provides an indication of the presence or absence of many different feature combinations at the input. The adjustment of the weight values are based on the back propagation algorithm. The neural network eventually gives a security score by means of the trust factor value and the reputation factor value given as input. The security scores based on the fuzzy logic system and the neural network is merged to get the security for the resource center.

The security score for the resource center is calculated as follows:

$$SS(rc) = \frac{M \times FL_{Score} + N \times NNS}{2} \rightarrow (9)$$

In the above equation $SS_{(rc)}$ is the security score of the resource center and FL_{Score} is the score obtained based on fuzzy logic system and NNS is the score obtained based on neural network and M is the weight value for fuzzy logic based score and N is the weight value for neural network based score.

5. TR-SS Algorithm

This section makes clear about our TR-SS algorithm. The TR-SS algorithm is a trust factor and reputation

factor based security score algorithm which applies fuzzy logic system.

1. **Input:** Filing the attribute values by the users for trust and reputation factor.
2. For each resource center is used to calculate trust factor and reputation factor.
3. Calculating the probability of number of users accessed a resource block.
4. The trust factor calculation to be determined for each resource block in a resource center.
5. Similarly, the trust factor calculation to be done for next resource blocks in a resource center.
6. **End for**
7. The reputation factor calculation to be done for each resource blocks in a resource center.
8. Similarly, the reputation factor calculation to be done for next resource blocks in resource center.
9. **End for**
10. Calculate the trust factor for resource center.
11. The trust factor for resource center was calculated based on the user trust attributes.
12. Calculate the reputation factor for resource center.
13. The reputation factor for resource center was calculated based on the user reputation attributes.
14. Repeat the steps from two to thirteen for next resource centers.
15. **End for**
16. The trust factor and the reputation factor of resource center values are the input for the fuzzy logic system and neural network system.
17. Fuzzify the trust factor and reputation factor and defuzzify based on rules rule activation and rule accumulation method.
18. Merging the scores obtained from Fuzzy logic system and neural network.
19. **Output:** Obtaining security scores values for resource center.

Rule for Fuzzification, Defuzzification and Security Score values

Rule 1: If Trust factor is extreme or Reputation factor is high, then the score value is high.

Rule 2: If Trust factor is low or Reputation factor is high, then the score value is high.

Rule 3: If Trust factor is low or Reputation factor is low, then the score value is low.

Rule 4: If Trust factor is extreme or Reputation factor is extreme, then the score value is extreme.

6. Results and Discussions

This section shows the outcome of proposed technique. It encompasses the experimental setup, fuzzy design result and the presentation of our proposed technique.

6.1. Experimental Setup

With 4GB RAM, our method is executed in java (jdk1.6) that has the system configuration as i5 processor. For this proposed techniques three dissimilar datasets which are Financial, Medical and RDB are used. The four dissimilar resource centers that have used in three different resource blocks in this method. The datasets are as resource blocks. With different number of users were observed for the proposed technique, because the users will present the attribute values for the trust factor and the reputation factor after they applied the resource.

6.2. Fuzzy System Results

The fuzzy system result is the procedure of giving input and obtaining output from the fuzzy logic system. The Fig.3 shows a score value we attained from the fuzzy logic system for the membership conditions of trust factor and reputation factor.

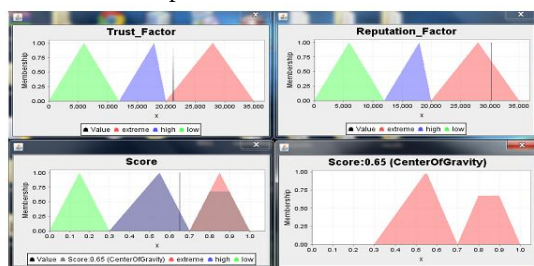


Fig.3 Score value obtained from the fuzzy logic system

6.3 Performance Analysis

The trust and reputation managers are used to collect the attribute values for the trust and reputation factors from the users after accessing the resource. The weight values are given to attributes, for example if the user accessing the attribute of the copyright date. The attributes are having weights, if the user's copyright date is expired, it means the user should renew the copyright form. If the user is accessing the copyright form without renewing it, then the weight factor comes into consideration. If the weight value matches, then the user can access the block. Otherwise the resource center may protect from the user. The threshold values for the attributes are 0 to 1.

This section delineates the performance of the proposed technique. To check the performance, two secure resource centers and two insecure resource centers are used. The first and second resource centers are insecure whereas the third and fourth resource centers are secure and this system works based on the feedback of the users. The performance of this system is checked with different number of users. In this section, the representation 'High' in the graph denotes that the resource center is secured and the

representation 'Low' in the graph denotes that the resource center is not secured.

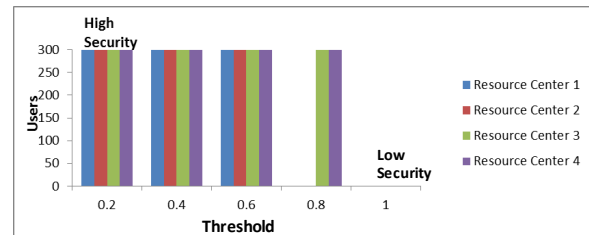


Fig.4 Performance based on feedback of three hundred users

The Figure 4 shows the performance of our technique based on the feedback of three hundred users by varying the threshold. The Fuzzy Logic system decides whether a resource center is secured or not. Here, while setting the threshold value as 0.2, the system shows the entire resource centers that are secured and when setting the threshold value as 0.4, the system shows the third and fourth resource centers as secured. Similarly, while setting the threshold value as 0.6, the system shows the third and fourth resource centers as secured and for the threshold values between 0.8 to 1, the entire resource centers are insecure.

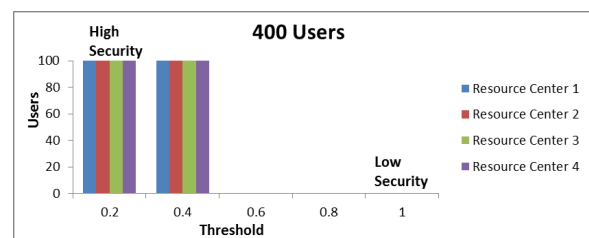


Fig.5 Performance based on feedback of four hundred users

The performance of our system based on the feedback of four hundred users is shown in the Figure 5 for diverse threshold values. Here, the threshold value 0.2 shows that the entire resource centers that are secure and for the threshold values between 0.4 and 0.6, the third and fourth resource centers are secured whereas the first and second resource centers are insecure. When setting the threshold values between 0.8 to 1, the entire resource centers are insecure.

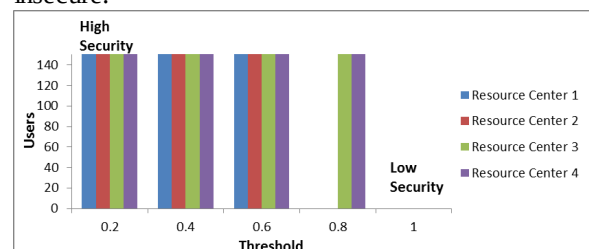


Fig.6 Performance based on feedback of five hundred users

The Figure 6 shows the performance of the system based on the feedback of five hundred users by varying the threshold which decides whether a resource center is secured or not. When setting the threshold value as 0.2, the system shows the entire resource centers used for technique are secured. While setting the threshold value as 0.4, the first and second

resource centers are insecure but the third and fourth resource centers are secured.

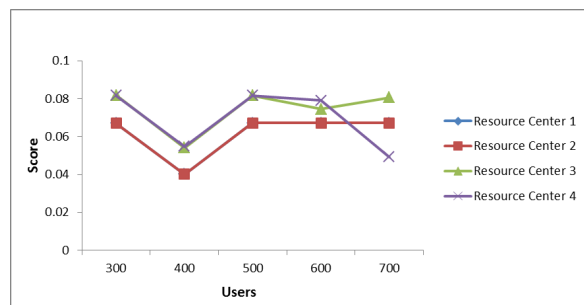


Fig.7 Score Values obtained for different resource centers

The score values attained from the fuzzy logic system together with neural network for the resource centers in our experimentation are illustrated in Figure 7. From the comment of three hundred users, the score value attained from the fuzzy logic system together with neural network system for the first, second, third and fourth resource centers are 0.067087044, 0.067186321, 0.081805798 and 0.081786668 respectively. When reflecting on the comment of four hundred users, the score values attained from the proposed system for the first, second, third and fourth resource centers are 0.040135843, 0.040135843, 0.05410748 and 0.054839521 respectively.

When reflecting on the comment of five hundred users, the score values attained for the first, second, third and fourth resource centers are 0.067146769, 0.067184832, 0.081783037 and 0.081755906 respectively. When the analyzing the comment six hundred users, the score value for the first, second, third and fourth resource centers are 0.067161597, 0.067174059, 0.074504212 and 0.079140074 respectively. When reflecting on the feedback for seven hundred and fifty users, the score values for the first, second, third and fourth resource centers are 0.067118327, 0.067153199, 0.080761123 and 0.049212507 respectively.

7. Conclusion

The proposed technique for secure resource allocation in cloud computing by means of fuzzy logic and neural network based trust and reputation model is implemented. Based on the characteristics values specified by the users, the trust factor and reputation factor is computed and specified to the fuzzy logic system and neural network system to discover the security score of a resource center. With the comment of dissimilar number of users, we have executed the experimentation of proposed technique and with dissimilar threshold values to make a decision whether a resource center is protected or not.

References

[1] Alok Tripathi and Abhinav Mishra, "Cloud Computing Security Considerations", IEEE International Conference on Signal Processing,

Communications and Computing, Vol.4, no.7, pp.1-5,2011.

[2] A. Josang, C. Keser and T. Dimitrakos, "Can we manage trust?" in *iTrust*, Springer, pp. 93-107, 2005.

[3] A. Jsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no.2, pp. 618-644, 2007.

[4] Chaisiri, S. Bu-Sung Lee ; Niyato, D., "Optimization of Resource Provisioning Cost in Cloud Computing", *IEEE Transactions on Services Computing*, vol. 5, no. 2, pp. 164-177, 2012.

[5] Farag Azzedin, Muthucumaru Maheswaran, "Towards Trust-Aware Resource Management in Grid Computing Systems," in *Proceedings of the 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid*, Washington, USA, pp: 452, 2002.

[6] Florin Ogigau-Neamtii, "Cloud Computing Security Issues", *International Journal of Application or Innovation in Engineering*, Vol.1, no.2, pp.1-5,2012.

[7] Mohamed Firdhous, Osman Ghazali and Suhaidi Hassan, "Trust Management in Cloud Computing: A Critical Review", *International Journal on Advances in ICT for Emerging Regions*, Vol.4, no.2, pp.24-26,2011.

[8] R. A. Malaga. "Web-based reputation management systems: Problems and suggested solutions", *Journal of Electronic Commerce Research*, Springer Netherlands, Vol: 1, No: 4, pp: 403-417, 2001.

[9] Safwan Mahmud Khan and Kevin W. Hamlen, "Hatman: Intra-cloud Trust Management for Hadoop", *IEEE International Conference on In Proceedings of IEEE CLOUD*, Vol.9, no.5, pp. 494-501, 2012.

[10] Shanshan Song, Kai Hwang and Yu-Kwong Kwok, "Trusted Grid Computing with Security Binding and Trust Integration", *Journal of Grid Computing*, 2005.

[11] Shanshan Song and Kai Hwang, "Dynamic Grid Security with Trust Integration and Optimized Resource Allocation", in *Proceedings of the International Symposium on High- Performance distributed computing*, Honolulu, 2004.

[12] Sheikh Mahbub Habib, Sebastian Ries, Max Muhlhauser, "Towards a Trust Management System for Cloud Computing", *International Conference on Trust, Security and Privacy in Computing and Communications*, pp.933-939,2011.

[13] S. M. Habib, S. Ries, and M. Muhlhauser, "Cloud computing landscape and research challenges regarding trust and reputation," *Symposia and Workshops on ATC/UIC*, vol. 0, pp. 410-415, 2010.

[14] Vivekananth.P, "Trusted Resource Allocation in Grid Computing by Using Reputation,"

International Journal of Computer Science & Communication, Vol.1, no.2, pp.23-25, 2010.

- [15] Bao Rong Chang, Hsiu-Fen Tsai, Chia-Yen Chen, & Yun-Che Tsai, 'Assessment of In-Cloud Enterprise Resource Planning System Performed in a Virtual Cluster', Hindawi Publishing Corporation Mathematical Problems in Engineering, Article ID 213461, pp. 1-11, 2015.
- [16] Bernstein, D, Ludvigson, E, Sankar, K, Diamond, S & Morrow M 2009, 'Blueprint for the Intercloud-Protocols and Formats for Cloud Computing Interoperability', Proceedings of 4th international conference on Internet and Web Applications and Services, pp. 328-336, IEEE.
- [17] Ignacio Aransay, Marina Zapater, Patricia Arroba, and Jose M. Moya, 2015, 'A Trust and Reputation System for Energy Optimization in Cloud Data Centers', Proceedings of 8th international conference on Cloud Computing, pp. 138-145.
- [18] Raghavendra Achar & Santhi Thilagam P, 'A Broker Based Approach for Cloud Provider Selection', In Proceedings of IEEE, International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp.1252-125,2014.
- [19] Raghavendra Achar, Santhi Thilagam P, Nihal Soans, Vikyath P V, Sathvik Rao and Vijeth A M, 'Load Balancing in Cloud Based on Live Migration of Virtual Machines', Proceedings of Annual IEEE India Conference (INDICON), pp.1-5,2013.

