JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 104 - 111
https://publishoa.com
ISSN: 1309-3452

A Heuristic Secure Resource Sharing Method In Internet Of Things Environment

C Kamalanathan
Associate Professor
Department of Electrical Electronics and Communication Engineering
GITAM School of Technology, GITAM Deemed to be University, Bengaluru Campus, Karnataka, India
Corresponding author kamalanadhan@gmail.com

S Karthick
Associate Professor, Department of Electrical, Electronics and Communication Engineering
GITAM School of Technology, GITAM Deemed to be University, Bengaluru Campus, Karnataka, India

Sunita Panda
Assistant Professor, Department of Electrical,Electronics and Communication Engineering
GITAM School of Technology, GITAM Deemed to be University, Bengaluru Campus, Karnataka, India

S Raja Gopal
Assistant Professor, Department of Electronics and Communication Engineering
KL Deemed to be University, Vaddeswaram, Andhra Pradesh, India

D V Soundari
Assistant Professor, Department of Electronics and Communication Engineering
Sri Krishna College of Engineering and Technology, Coimbatore, India.

ABSTRACT

In recent times one of the emerging and intelligent tool is Cloud Computing. It has developed a leading model of computing and IT service delivery. Cloud Computing is characterized by three-layered basic service forms such as, Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS) and Infrastructure-as-a Service (IaaS). Pushing information into the cloud extends larger closeness since users are not necessary to be concerned about the storage capacity, storing techniques, hardware management, or data maintenance. A key problem that requires specific consideration is security of clouds. Existing approaches for secured outsourcing of information and random calculations are either support on a single tamper-proof hardware, or based on homomorphic encryption. To overcome existing issues a novel approach is proposed to focus on security experiments in cloud computing and to provide solutions. To provide unfailing security to the users, the purpose of this paper is in three folding. 1) To design a mathematical model for trust and reputation calculation. 2) To propose TR-SS algorithm for calculation of security score. 3) To compare the security score of trust and reputation factors by Fuzzy Logic System, Neural Network. This work is focused on controlling the security issues in cloud environment by means of trust and reputation factors using mathematical model, Trust and Reputation Security Score (TRSS) algorithm, Fuzzy Logic System, Neural Network in Internet of Things applications.

Keywords: Internet of things, Cloud Computing, Resource Center, Trust and Reputation, Neural network

INTRODUCTION

Cloud computing is a paradigm for supporting pervasive network access, shared tend to focus on shared pool of configurable computing resources to expanding the effectiveness. Cloud computing involves providing services through the internet and the services are largely classified into three types: IaaS, PaaS, SaaS. Authenticated communications amid of hosts and users are focusing on security conditions in cloud computing environment. The cloud computing requires advanced and secured resource management systems for effective utilization. The degree, in which the resources are trusted, reputation and allocation of resources can be used for trust calculation. The major problems indicating the reputation systems are the trust metric, i) modelling, computing the trust and management, ii) Security and efficient retrieval of the required data required. A cloud computing based Trust and Reputation factor secure resource allocation model were developed by considering the problems. A fuzzy-neuro secured resource allocation method were proposed to protect resource center. There are several security problems in cloud computing covers many technologies with memory management networks, OS, databases, virtualization, resource scheduling, networks, load balancing etc.

A neuro fuzzy method is proposed to achieve this security issues during resource allocation.To solve the security issues and in order to provide trust in the cloud environment during resource allocation, a fuzzy logic, neural network and rough set theory based trust and reputation model has been introduced in this proposed research.

LITERATURE SURVEY

Based on the cloud on demand model for multi-clouds novel framework for secure and dynamic Internet of Things is proposed by Muhammad Kazim et al.(2018). The system provides little overhead compare to standard authentication protocols.

Chuan Pham et al(2018) implemented an anti-phishing gateway as software at the edge of the network and phishing detection Fi-NFN model using embedded robust machine learning technique. It provides stable and accurate results in fog computing environment.

Hongliang Zhu et al(2019) proposed ZSS signature algorithm which by allowing trusted third party provides public auditing and privacy protection. This technique reduces adaptive chosen-message attacks with enhanced safety and efficiency.

Kalka Dubey et al(2019) Ideal Distribution Algorithm (IDA) is proposed for virtual machines to schedule the workflow tasks. To provide the load balancing with deadline constraints and to improve monetary cost Enhanced IDA is adopted.

Yang et al.(2010) is proposed a BNBTM(Bayesian Network Based Trust Management) methods, which utilize a each dimension is estimate by means of a single Bayesian network distributes the trust value and multidimensional function specific trust value which are represented by beta probability distribution function (PDF) based on the relations history.

The truth is that cloud computing has simplify by technological feature of building computer systems, but the numerous confront facing IT environment still remain proposed by Chaisiri et al. (2012). Organizations which take up cloud based services and also realize the numerous problems of information policy, reliability, security, privacy, access and regulation.

Muhammad Awais Shibli et.al. (2013) is proposed VM migration is a valuable feature for Cloud environment. It also introduces new security concerns such as modification of VM content during migration. VM migration which offers robust security features such as authorization of migration operation, mutual authentication between confidentiality, integrity of VM content and Cloud Providers.

A broker based totally architecture become supplied to choose appropriate cloud provider from numerous issues. The dealer calculate every cloud company and prioritizes of the great based on the requester proposed by Raghavendra Achar & Santhi Thilagam P (2014). In the direction to distinguish from one to every other cloud service provider, the Service Measurement Index (SMI) has advanced by way of Cloud Services Measurement Initiative Consortium (CSMIC).

Raghavendra Achar & Santhi Thilagam P (2014), author proposed SMI is the standard methods to evaluate cloud service based on requester in essential business desires.

There are some high level attributes are taken into consideration like Performance, Accountability, Assurance, Agility, Privacy and Security, Integrity, Cost, Usability Raghavendra Achar & Santhi Thilagam P (2014) author become proposed. Pick out a apposite cloud provider from numerous, interdependent dating and cloud provider involves numerous criterion amid them. It is Multiple Criteria Decision- Making (MCDM) hassle. Author proposed the Technique for Order Preference by way of Similarity to Ideal Solution (TOPSIS) based rating approach to pick out service offer. The selection of cloud issuer involves 3 steps. 1) Suitable Criteria Identification 2) Evaluation of the load of standards via AHP 3) Ranking cloud vendors by means of TOPSIS.

Soft computing includes (Tian 2010; Vivekananth 2010) neural networks, fuzzy good judgment, genetic algorithms and probabilistic reasoning. To layout an intelligence system, strategies or a set of strategies from these kinds of regions are used.

Zohre Raghebi & Mahmoud Reza Hashemi (2013), Trust level is verified by means of past knowledge of earlier customers of this cloud service with every each latest customer, therefore a new trust evaluation scheme was proposed for this cloud service. An adaptive method introduces that aid discriminate amid malicious and reliable customer feedbacks

Mehrnoosh Monshizadeh et.al (2015), proposed a new approach for building federations of clouds providers, which is based on algorithms and on an architectural model that describe the relations amid the entities of the model. The proposed model makes use of a global entity that is conscientious for the search and share of resources in the federation on behalf of the cloud user.

An imperative drift in decision support for internet arbitrate service condition for trust and reputation systems was proposed by Jsang et al. (2007).

Xu Wu (2015) an adaptive trust management model explains capable of estimate the cloud provision based on its numerous trust aspect. Adaptive modelling tools is classified into two category such as induced ordered weighted averaging (IOWA) and rough set are applied to knowledge discovery and trust data mining.

PROPOSED SYSTEM

Fuzzy logic is one of the key methods that is to achieve high level security. It holds non-linear mapping abilities and agreement with uncertainties parameters in the systems. The fuzzy systems convert fuzzy rules to their equivalent mathematical values. The fuzzy logic system is comprising with three stages viz., Fuzzification, Evaluation of Rules and Defuzzification. Fuzzy inference systems consist of several conditional ‘if-then’ rules which are called as fuzzy logic models. The fuzzy sets are having different degrees of membership. The proposed system overall process is the scheduling manager is allocate the resource center once users give a task to access the block of resource. The manager schedule and verifies given path to corresponding resource center and resource block where it is placed. After accessing the block of resource, the user gives the attribute values for the trust and the reputation factors.

Resource Center trust factor

Resource center is the addition of consider aspect in each resource blocks of the resource center. Some of the attributes we considered for the trust factor are Contact us, Firewall, Anti-virus,About us, Copyright,Policy, Corporate logos, Secure Job execution

Trust factor can be calculated by

$$Trust\ factork\ (Resource\ block) = Prob \sum_{1}^{m} \left(\sum_{1}^{users} \frac{Each\ user\ TF\ \ * Weight\ of\ TF\ attribute}{Total\ weight} \right) \ - (1)$$

where,

Trust factor (Resource block) - Trust Factor of resource block

Prob - Probability of users used the resource block

m - Total number of attributes considered for trust factor

Total weight value of the attributes is calculated, with sum of every weight values of characteristic.

$$Total\ weight = \sum_{1}^{m} Weight\ value\ of\ each\ trust\ factor\ attribute \quad - (2)$$

The trust factor of a resource center is calculated as by the use of the under equation

$$Trust\ factor\ (Resource\ center) = \sum_{1}^{N} Trust\ factor\ of\ resource\ block\ - (3)$$

where,

N - Total useful resource blocks in a resource center

Table 1. Weight values assigned for Attributes

Sl No	Attributes	Weight value

1.	Anti-virus	0.85
2.	Copyright	0.70
3.	Firewall Capabilities	0.90
4.	Corporate Logo	0.65
5.	Secure Job Execution	0.75
6.	About us	0.50
7.	Policy	0.80
8.	Business Address	0.60

Resource Canter Reputation factor

Reputation is defined as a measure of reliability. Reputation of a system offers a structure for creating trust through societal control deficient trusting third parties.

Attacker Model

Reputation systems are in general vulnerable to attacks, and many types of attacks are possible.

Scenarios of attack

The system would affect by various attack scenario such as Self-promoting, Whitewashing, Slandering, Orchestrated, Denial of Service. To determine the reputation factor some of the attributes are considered that are Consistency, Contents look current, Rapid Response, Confidentiality, Trust symbols, Robustness, Return Policy. Reputation factor is computed through user about their earlier experiences the feedback. The feedback is a value between 0 to 1.

The resource center reputation factor is calculated by:

$$Reputation\ factor\ (Resource\ Center) = \sum_{k=1}^{N} Reputation\ factor\ of\ each\ resource\ block\ in\ Resource\ center\ \ -(4)$$

where,

N - Total useful resource blocks in a useful resource center

To determine the reputation factor of a resource center, the formula is used to estimate as

$$Reputation\ factork\ (Resource\ block) = Prob \sum_{1}^{m} \left(\sum_{1}^{users} \frac{Each\ user\ RF\ * Weight\ of\ RF\ attribute}{Total\ weight} \right)\ \ -(5)$$

The computation of total weight value L of the characteristic is given underneath

$$Total\ weight = \sum_{1}^{m} Weight\ value\ of\ each\ Reputation\ factor\ attribute\ \ -(6)$$

Fuzzy System

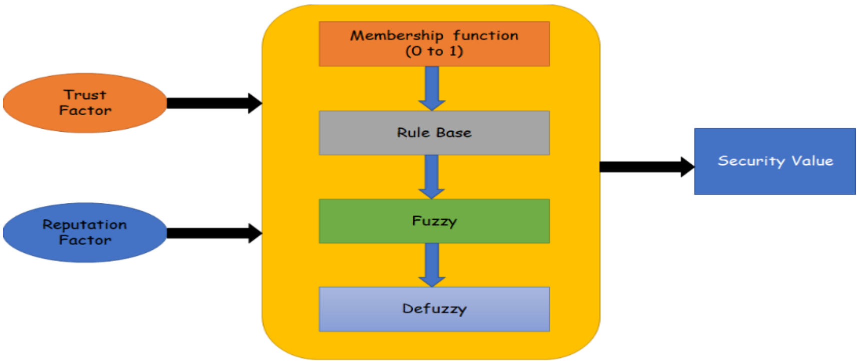


Figure1.Fuzzy Logic (FL) System in proposed technique

To compute the resource center security score is by giving reputation factor and trust factor input for the fuzzy system. In this proposed method, a fuzzy logic system usedfor fuzzification and defuzzification. For computing the security score,

$$I = Trust\ factor\ (Resource\ center) * Reputation\ factor\ (Resource\ center)\ \ -(7)$$

where, I - Security Score output from FL system

Rule for Fuzzy logic and Security Score (TF – Trust Factor & RF – Reputation Factor)

Rule 1: TF is extreme or RF is high, in that case the high score.
Rule 2: TF is low or RF is high, in that case the high score.
Rule 3: TF is low or RF is low, in that case the low score.
Rule 4: TF is extreme or RF is extreme, in that case the extreme.

Neural Network Model

Neural Network is an artificial computing system. It recognizes, highly interconnected processing elements which process data to external inputs by their dynamic state response.

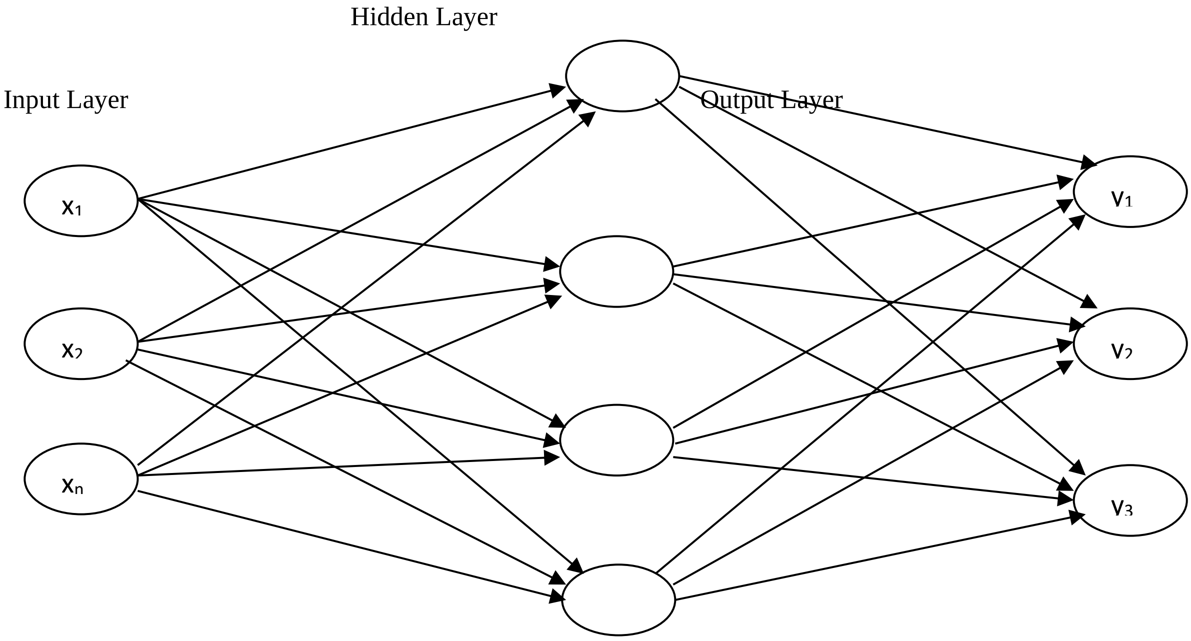


Figure 2 Neural Network Structure

The trust and the reputation factor value are applied to the neural network to achieve the security score from the fuzzy logic system. To train a neural network, a backpropagation method is used. The neural network learn a defined to pairs of input and output. An input has been given as a stimulus to the first layer and it is pass on to higher layer till an output is formed. The output pattern is subsequently matched towards required output, and for each output unit an error signal is processed. The error signals are then pass on rearward from output layer.

The proposed security score for the resource center is

$$Security\ Score = \frac{Weight\ value\ (Fuzzy) \times Score\ (I) + Weight\ value\ (Nural) \times Neural\ Network\ Score}{2} - (8)$$

RESULTS

This phase illustrates the proposed works. It consists of experimental setup, fuzzy result and performance analysis of our proposed technique.

Experimental Setup

The proposed technique is employed in jdk 1.6 (java)and system configuration is i5 processor with 4GB RAM. Financial, Medical and RDB are the different datasets used.

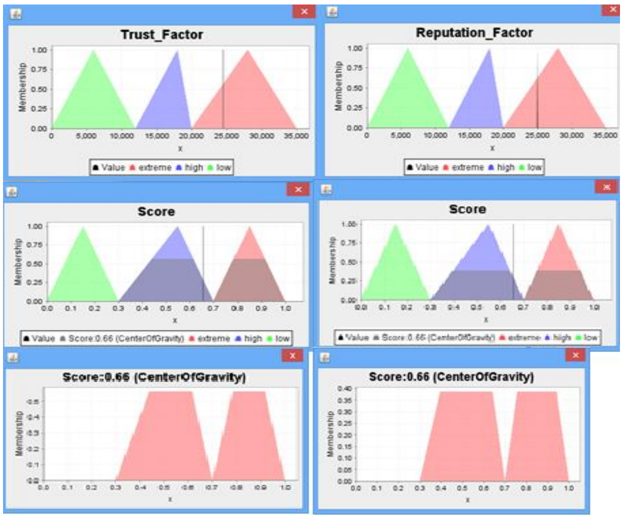


Figure 3 Fuzzy Logic System Score value

Fuzzy System and Neural Network Model Results

Table 2.Score values from fuzzy system results

S. No	Resource Centre	Level	Range	Security score value	Centre of Gravity
1	Trust factor	Low	0 to 11000	0.0 to 0.2	0
		High	11000 to 19000	0.3 to 0.6	0.66
		Extreme	19000 to 40000	0.6 to 1.0	0.66
2	Reputation factor	Low	0 to 11000	0.0 to 0.2	0
		High	11000 to 19000	0.3 to 0.6	0.66
		Extreme	19000 to 40000	0.6 to 1.0	0.66

Performance Analysis

The trust and reputation managers are used to gather the attribute values for accessing the resource to calculate the reputation factor and trust factor. Threshold values of attributes are considered from 0 to 1. This segment explains the shows our proposed technique. To verify the implementation, two secured resource center and two in-secured resource center are used also this system mechanism based on the users feedback. This systems implementation is verified with different users. In this segment, the depiction 'High' and 'Low' in the figure denotes secured resource center and in-secured resource center respectively. The justification of the performance achieved from the proposed technique.

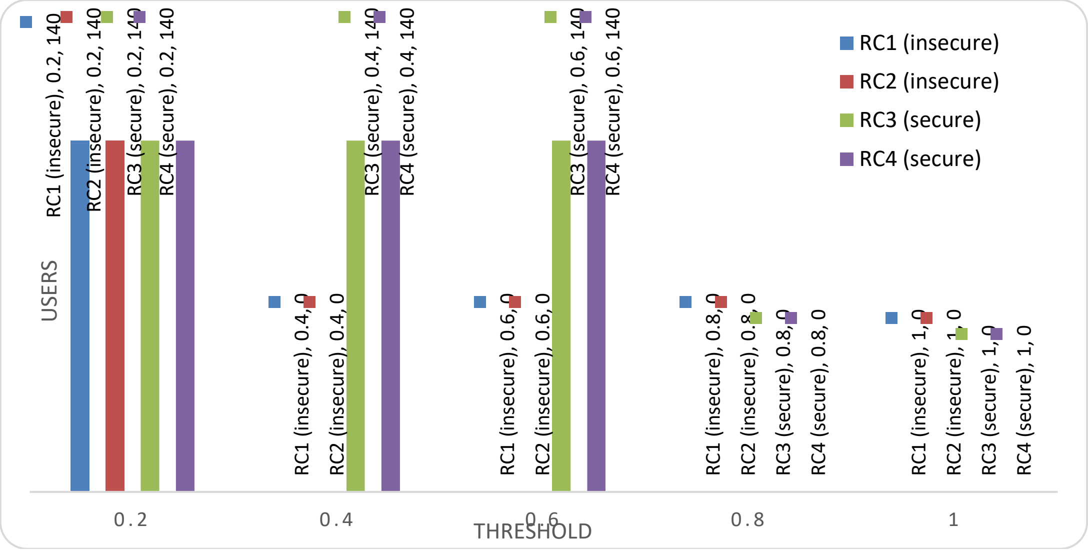


Figure 4 Representation with 150 users feedback

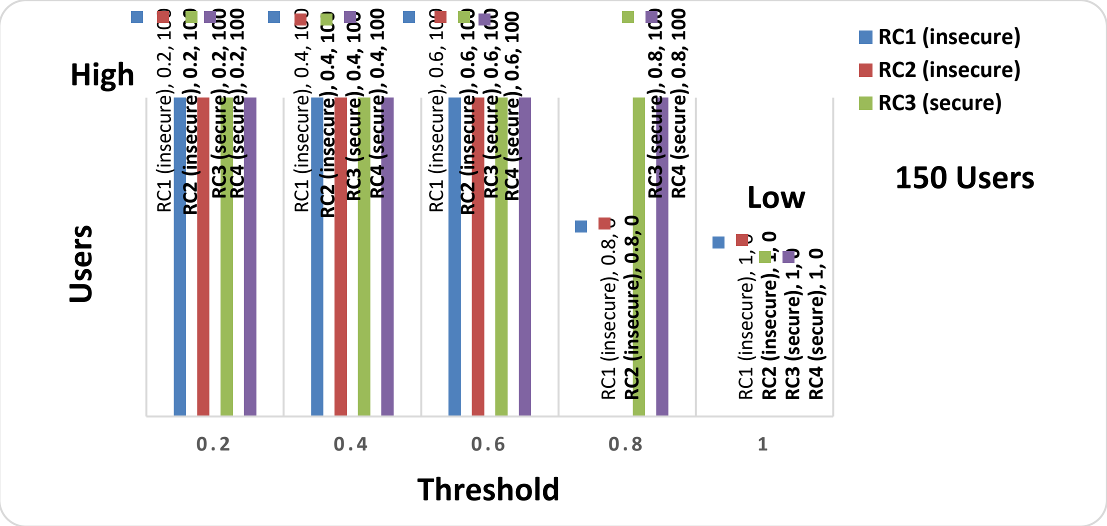
Figure 4 shows, implementation of proposed technique, represented with Hundred and Fifty users feedback by varying threshold. Fuzzy Logic system decides, a resource center is security level. The result of the resource center after the feedback

Table3.Performance analysis of different resource centers using fuzzy (50,100 & 150 users)
Table4.Dissimilar resource centers Score values using fuzzy

Th* RC*	0.2	0.4	0.6	0.8	1.0
RC1	Secured	In-secured	In-secured	In-secured	In-secured
RC2	Secured	In-secured	In-secured	In-secured	In-secured
RC3	Secured	Secured	Secured	In-secured	In-secured
RC4	Secured	Secured	Secured	In-secured	In-secured
U* RC*	50	100	150	200	250
RC1	0.3526	0.3526	0.3593	0.3577	0.3590
RC2	0.3593	0.3594	0.3584	0.3581	0.3590
RC3	0.6550	0	0.6587	0.6558	0.6587
RC4	0.6512	0.6429	0.6420	0.6588	0.6284

Security score of reputation factor between 0.0 to 0.2 the system provides low security, for high security the values between 0.2 to 0.6 and the values between 0.6 to 1.0 is extremely good security. The CoG ranges are taken from 0.0 to 1.0. The ranges of 0.3 to 0.7 and 0.7 to 1.0 which is extremely high trust and reputation factor security values. The center of gravity is more between the range of 0.3 to 0.7 and the center of gravity score value is 0.65.

This segment defines the proposed method. To validate the presentation, two secured and in-secured resource centers are used. Based on the feedback from users, the first two resource centers are kept as in-secured and next two resource centers are considered secure. Initially 50 users have been taken and different users like 100,150,200 and 250 users were considered



Performance analysis with 150 users feedback

Table5.Performance analysis of different resource centers after neural (150 users)

Th* RC*	0.2	0.4	0.6	0.8	1.0
RC1	Secured	In-secured	Secured	In-secured	In-secured
RC2	Secured	In-secured	Secured	In-secured	In-secured
RC3	Secured	Secured	Secured	Secured	In-secured
RC4	Secured	Secured	Secured	Secured	In-secured

Table 6. Score values for different resource centers after neural

U* RC*	0.2	0.4	0.6	0.8	1.0
RC1	0.0670	0.0401	0.0671	0.0671	0.0671
RC2	0.0671	0.0401	0.0671	0.0671	0.0671
RC3	0.0818	0.0541	0.0817	0.0745	0.0807
RC4	0.0817	0.0548	0.0817	0.0791	0.0492

CONCLUSION AND FUTURE WORK

The proposed method implemented to calculate trust and reputation model for cloud computing secure resource allocation with neural network and fuzzy logic. Resource center security score is discovered by neuro fuzzy model. Different number of users were considered and implemented with different threshold values for decided the resource center is secured or not. In Future, this work may be prolonged to address the various dynamic security problems and attacks in cloud computing by developing asymmetric encryption algorithms in Internet of Things protocol stack application layer to provide security for the exchanging of message with different medical datasets.