An Efficent Security Farmework Design for Cloud Computing using Artificial Neural Networks

Anshika Negi
M.Tech. Student
Department of Computer Science
Krishna engineering college
Ghaziabad, India

Mayank Singh, PhD
Department of computer science
Krishna engineering college
Ghaziabad, India

Sanjeev Kumar
Department of Computer Science
Gurukula Kangri
Vishwavidayalaya
Haridwar, India

ABSTRACT
Cloud Computing is an alluring technology which provides elasticity, scalability and cost-efficiency over a network. In recent years, Data security is considered as the measure issue leading towards a hitch in the adoption of cloud computing. Data privacy, Integrity and trust issues are few severe security concerns leading to wide adoption of cloud computing. The proposed model has sufficient functionalities and capabilities which ensures the data security and integrity. The proposed Framework focuses on the encryption and decryption approach facilitating the cloud user with data security assurance. The proposed solution only talks about the increased security but does not talk about the performance. The solution also includes the functioning of forensic virtual machine, malware detection and real time monitoring of the system. In this paper, a survey of different security issues and threats are also presented. A data security framework also provides the transparency to both the cloud service provider and the cloud user thereby reducing data security threats in cloud environment.

Keywords
Data security, Privacy, Integrity, Trust, Cloud Computing; counter propagation network, cryptography, artificial neural network.

1. INTRODUCTION
Cloud computing is the name given to a recent trend in computing service environment. It is considered as the future paradigm for enabling convenient, on demand network access to the shared computing resources. The technologies behind the success of Cloud computing is Virtualization, Service Oriented computing , Utility Computing , Load balancing, Multi-tenant environment, the ability of pay per use of computing resources reducing large capital expenditures and operational overhead [1]. In spite of having several benefits of cloud computing data security, privacy, integrity and trust are few major hindrances for the wide acceptance of cloud computing [2]. Cloud user requires the safety of their sensitive data from tampering or an unauthorized access. The cloud computing platform faces the internal and external security threats, various outages and security threats to the cloud services from time to time. Various algorithms and protocols have been designed in the past (MD5, RSA, PDP, PoR) and are implemented in order to maintain the issues related to data privacy, integrity and trust. [9], [10].

The Objective of this research paper is to provide the protection of data from various data security threats such as data privacy, data integrity, and data trust lying in cloud environment. In this proposed paper the Symmetric key cryptography for the Encryption and decryption of the sensitive data which scare the prospective consumer and the organization to use cloud computing services their sensitive data. The primary point of cryptography is to deal with information secure from intruders. The inverse procedure of getting back the first information from encoded information is Decryption, which restores the first information. To scramble information at distributed storage both symmetric-key and Asymmetric key calculations can be utilized.

The proposed data security model provides a better security to the data of the cloud user using counter propagation neural networks. Authentication of data at various levels will lead to more data security. The real time monitoring, use of forensic virtual machine and various encryption techniques will lead to data security, data privacy, data integrity and trust.

2. RELATED WORK
This section illustrates the related work on data security. There are few approaches and models earlier proposed by various authors for ensuring the data security in a compliant ways. The author of the Paper [15] proposed an adaptive privacy management system where some of the highly sensitive was encrypted by using predefined privacy policies. In paper [14] author proposed Anonymity based algorithm for cloud computing services which process the micro data also sending the anonymous data to the cloud provider for integrating the data with additional information and can get the result.

In paper [8] Temper proof cryptographic coprocessor which is configured by trusted third party are also proposed by author. Temper proof facilitates a secure execution domain in cloud computing that is physically and logically protected from unauthorized access. In paper [5] the author talked about RACS technique which is redundant array of cloud storage technique

to avoid vendor lock-in and also reduce the cost. The author of the paper [6] presented the privacy manager for protecting the data being stolen or misused and also assisting the cloud computing provider to conform the privacy law by describing the privacy architecture to protect private data. The above approaches are good for providing the security to the data but somewhere the performance is compromised.

In paper [7] the author proposes an approach for public audit and preserve data at cloud. The author talked about the public availability of cloud stored data for security. Third party auditor (TPA) talks about auditing the cloud data storage with no additional on-line burden to the cloud user also bringing no vulnerabilities towards user data privacy.

3. DATA SECURITY AND SECURITY ISSUES IN CLOUD

In traditional data security, various techniques were used for processing and protecting the sensitive data. To secure outsourced data, Encryption technique was commonly used technique for data security. Downloading all the data and decrypting it at local site is not very cost effective as huge bandwidth is required for decrypting at local site associated with the process. Another major security concern arises in outsourcing data is the "proof of ownership" which prevents the user from the exposure to his own data. The Outsourced data is handed over to the remote service provider but the owner himself is not aware about the storage of the data. Other challenging security problem is the disaster recovery. It depends on the service provider handling of the data in case of disaster which can occur in case of the remote hard drive failures due to vulnerabilities on cloud [2]. As the data to be stored is increasing day by day diminishing the security mechanism, the traditional security techniques are not that useful. The provider is handling critical and sensitive data of a customer, which does not always guarantee the data integrity, privacy and trust [11]. According to the author of the paper [4] the top threats to cloud computing are: abuse and nefarious use of cloud computing, insecure interfaces and APIs, malicious insiders, shared technology issues, data loss or leakage, account or service hijacking and unknown risk profile.

There are number of security issue in clued computing environment given as follow:

3.1 Data Privacy

The data is expanding day by day leading towards several security issues in which data privacy is one of the security challenge associated with cloud computing. The privacy threats faced by cloud computing are the complexity associated with the risk assessment, growing industry demands the emergence of timely delivery of new business models and its implications on consumer privacy , various regulatory compliance, data privacy issues in design leading towards poor data quality and also lack of transparency [13]. The

Privacy Impact Assessment (PIA) to the cloud users is carried out by the Information Commissioner Office in United Kingdom (ICO) is responsible for using protocols and standards for accessing and using of the personal information in the cloud [16]. Data privacy protocols are related to the data and software transfer protocols, data processing protocols will influence the privacy of the data on cloud [17].

3.2 Data Integrity

The data integrity is useful for the validity of data and also promising the reliability and uniformity of data. Lack of Integrity is a major threat in the cloud environment; there are many security risks and attacks due to the data Integrity issues. Data integrity assures the user that no modification or tampering of the data will be done without users' knowledge. Data integrity is at risk when the intruder or anonymous user gains access over the stored data. The attack done on the user data can be data modification attack, data leakage attack and Tag forgery attack. Integrity monitoring of data is essential for avoiding data corruption and data crash in the data centers. In cloud computing the architectural design sometimes lead to the integrity issue [18]. Various mechanisms are adopted for preventing data integrity attacks on the cloud environment such as cooperative provable data possession (CPDP) which is the combination of hash indexing hierarchy and Homomorphism verifiable response [19],[20].

3.3 Data Trust

Trust is the major concern is and it breaks if two issues are not handled properly one of them is lack of transparency and other is due to breach in security and privacy. The cloud service providers offer flexibility to the use of resources which attracts consumers of cloud computing to get benefitted from the service by involving their sensitive data at risk. The consumers are unaware of the technology involved and control of the data as they are solely dependent on contracts and trust mechanism. Trust is a complex term and it is based on the positive approach or behavior of other. Trust is based on the security which the cloud service provider gives to its customers. Reputation also plays an important role in building the trust in the relation between the cloud vendor and the cloud consumer. Furthermore, trust mechanisms need to be propagated right along the chain of service provision [12]. Trust can be enhanced if the cloud provider isolates the data without violating the integrity and the privacy issues in the multi tenant environment. Transparency in storing of data and hiding the unnecessary information from the user will built a level of trust and understanding between the cloud provider and the user [12].

3.4 Governance

Administration suggests administration and oversight by the association over methodology, principles and approaches for application advancement and information innovation administration obtaining, likewise on the grounds that the style, usage, testing, utilize, and watching of sent or connected with administrations[14].

3.5 Malicious Insiders

This danger is surely understood to most associations. 'Vindictive insiders' effect on the association is significant. Malicious insiders are dangerous which has admittance to the information or data about the association being an individual from the association. As cloud shoppers application information is put away on distributed storage gave by cloud supplier which additionally has the entrance to that information [18], [19], [20].

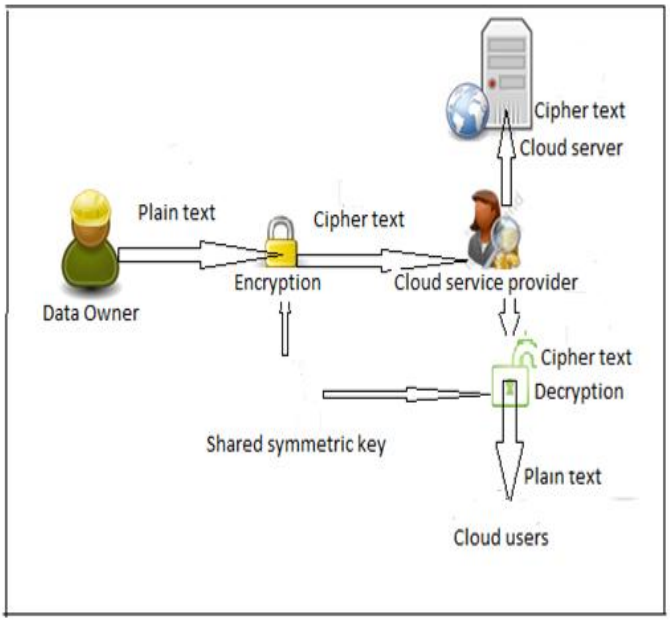


Fig.1. Security in cloud coumputing.

4. OVERVIEW OF ARTIFICIAL NEURAL NETWORK

Artificial Neural networks (ANN) were first introduced by Mc Culloch Pitts in 1943, inspired from biological neurons. An ANN

basically consists of very small computing units called neurons. Each neural neuron contains four basic components known as dendrites (accept inputs), soma (process the input), axons (Turn the processed inputs into outputs), and Synapses (the electrochemical contact between neurons).ANN is an engineering model of biological neuron that tries to simulate the behavior of biological neurons and their interconnections. Each connection link is associated with a weight which represents the input information that is used by the neurons net to solve a particular problem. It has number of inputs and only one output. ANN also contains various processing units and layers that are interconnected with each other, which usually operate in parallel manner and configured in regular architecture [21],[22].ANN networks are non-linear, simple, adaptive and robust in nature. The adaptive nature of ANN has the capability to change the system parameters during the training phase, after that ANN parameters are fixed and a system is developed to solve the problem instantly and the non-linear processing unit of ANN provides the system flexibility to achieve practically any desired input/output map. ANN divided in to two categories.

Supervised learning: In supervised learning, the model work over the input and produce the output that is predefined or known.

Unsupervised learning: In contrast of supervised learning the unsupervised learning doesn't have the known output. So that its work only on input by itself.

The propose a Neural Cryptography techniques and mechanism useful for implementing a highly protected environment is developed to secure the cloud data from the authorized user using counter propagation neural networks.

5. COUNTER PROPAGATION NEURAL NETWORKS

It was firstly introduced by R. Hecht-Nielsen, 1987. CPN is a network that learns a bidirectional mapping. The CPN consist of three layers: Input layer, Kohonen layer and Grossberg layer. The CPN are of two types [25]

1. Full CPN

2. Forward Only CPN

The basic structure of the CPN is shown in the figure below:-

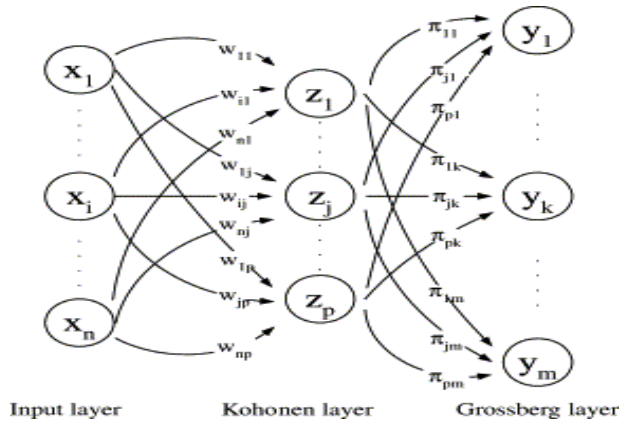


Fig 2: Structure of CPN

CPN is a composite learning scheme. It's a combination of supervised and unsupervised learning scheme. In the unsupervised learning the target in unknown on the other hand the output is predefined. Kohonen layer works on unsupervised learning scheme and the Grossberg layer work over supervised learning scheme. The weights are change according to the learning process automatically [21, 26].

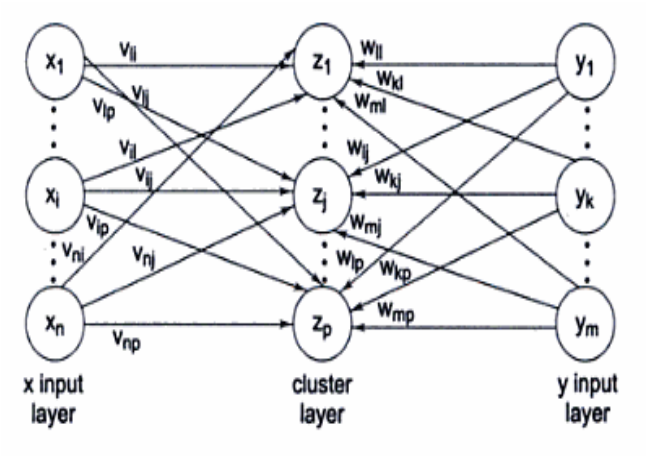


Fig 3: Structure of first phase 1 of CPN

The learning Process :

Phase 1 :(Kohonen unsupervised learning)

(1) Calculate the Euclidean distance between input vector & the weights of each hidden node.

(2) Detect the winner node with the shortest distance.

(3) Modified the weights that connected to the winner node in hidden layer with

Sij (New) =Sij (old) + α [Xi-Sij (old)] i= 1 to n

Tkj (New) =Tkj (old) + β [Yk-Tkj (old)] k= 1 to n

Where

x= input training vector

y= target output

Vij= weight from X-input layer unit

Wkj= weight from Y-input layer unit

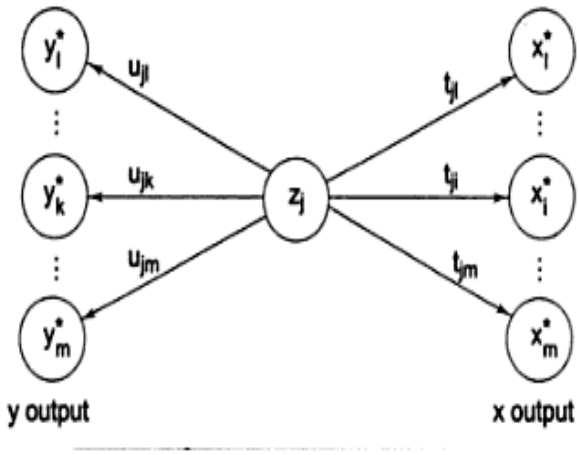


Fig 4: Structure of second phase 2 of CPN

Phase 2 :(Grossberg supervised learning)

(1) Calculate the Euclidean distance between input vector & the weights of each hidden node.

(2) Detect the winner node with the shortest distance.

(3) Let the link connected to the winner node to output node is set as 1 and the other are set to 0.

(4) Adjust the weights using

$$U_{jk}(New) = U_{jk}(old) + \alpha [Y_j - U_{jk}(old)] \qquad k = 1 \text{ to } m$$

$$V_{ji}(New) = V_{ji}(old) + \beta [X_i - V_{ji}(old)] \qquad i = 1 \text{ to } n$$

Where

U_{ik}= weight from cluster layer unit to y output layer

V_{kj}= weight from cluster layer unit to x output layer

6. PROPOSED SECURITY MODEL IN CLOUD COMPUTING

In this section a new model for data security in cloud computing environment using counter propagation neural (CPN) networks. This paper enhances traditional data security model for cloud computing. The proposed data security model divided into two phase architecture. The software encrypts and protects data at various levels by using various security techniques and security algorithms. The proposed model ensures that protection of the user confidential information by ensuring faster retrieval of the data using symmetric cryptography based on counter propagation method (CPN).

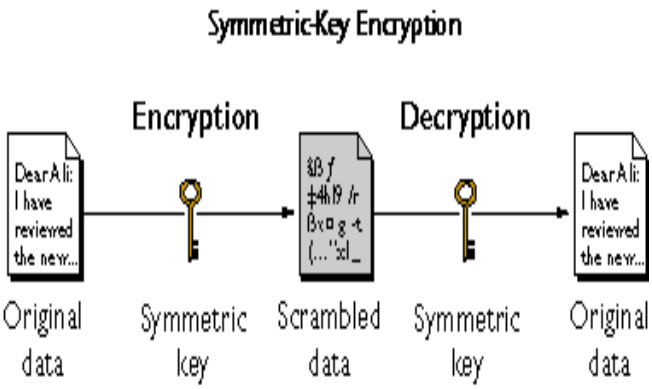


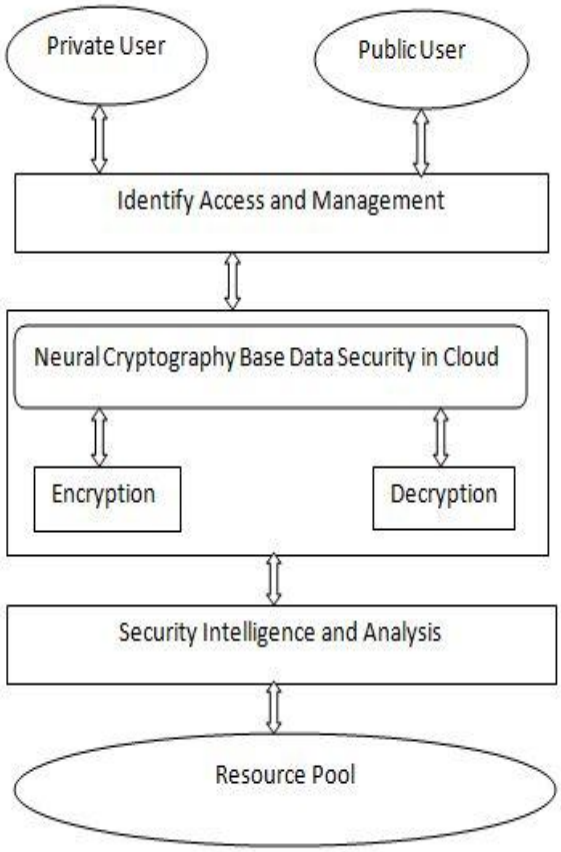
Fig 5: symmetric key encryption process

The proposed model consist of two main phase which will interact with each other to provide data security. First phase is responsible for authentication of the user by applying symmetric encryption process. Second phase communicate with first phase to make sure that only authorized user can send the receive data. This phase has performed decryption process. Encryption and decryption methods are used in the proposed data security framework to achieve a practical preferred solution for data security in cloud computing. In the encryption process the input pattern are converted into ASCII format after that ASCII format converted into binary value. Use this binary value as target input in the first phase (Khonen layer) of CPN. In the decryption process the target input value is applied to the second phase (Grossberg network) of CPN which convert binary value into ASCII value and the ASCII to original input pattern. In the second phase by applying decryption process the proposed technique identify the authorize user and processes entering in the cloud environment.

7. CONCLUSION AND FUTURE WORK

Cloud computing is common these days and more and more users are adding to the cloud environment leading towards security issues related to the data. This paper presents an overview on the data security problem associated with the cloud computing. This paper talked about various threats associated with data security in cloud computing describing briefly. The model is proposed talks about three level authentication mechanisms for improving security to the data as compared to the old traditional system. In this paper we propose encryption and decryption process using counter propagation neural networks for improving security to data as compare to the old traditional system. The proposed system provides helps in building highly secure data security system for all the three layers of the cloud services which are offered to the cloud user by the cloud provider. The future issue of data security in cloud opens new challenges such as Data locks by cloud provider, fault tolerance and disaster recovery mechanisms in cloud computing.

8. FLOW CHART FOR PROPOSED SECURITY MODEL



9. REFERENCES

[1] D Meng, 2013. Data security in Cloud Computing, Computer Science and Education (ICCSE), 8th International conference, pp 810-813.

[2] A. Shawish and M. Salama, 2014. Cloud Computing: Paradigms and Technologies, F. Xhafa and N. Bessis (eds.), Inter-cooperative Collective Intelligence: Techniques and Applications, Studies in Computational Intelligence 495, DOI: 10.1007/9783-642-35016-0_2, Springer-Verlag Berlin Heidelberg.

[3] R. Yadav, N. Yadav, Monika and A. Seharawat, 2015. "Cloud Computing: Flowing Model in IT Services,"

International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 3.

[4] Babcock and Charles, 2015. 9 Worst Cloud Security Threats Leading Cloud Security Group Lists the "Notorious Nine Top Threats to Cloud Computing in 2013; Most Are Already Known but Defy 100% Solution," Information Week..

[5] A.Libdeh, L. Princehouse, and H. Weatherspoon, 2010. RACS: A Case for Cloud Storage Diversity, SoCC 10:Proc. 1 First ACM Symposium on Cloud Computing, PP 209-240.

[6] S. Pearson, Y. Shen and M. Mowbray, 2009. A Privacy Manager for Cloud Computing, Cloudcom2009, LNCS 5931, PP 90-106, Springer.

[7] D.Prasad, B. R. Singh, M. Akuthota and M. Sangeetha, 2014. An Etiquette Approach for Public Audit and Preserve Data at Cloud," International Journal of Computer Trends and Technology (IJCTT) volume 16 number.

[8] W. Itani, A. Kayssi and A. Chehab, 2009. Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures, Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing.

[9] S. Subashini and V. Kavitha, 2011. A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, 34(1): p. 1-11.

[10] C. Ning., et al. 2011. Privacy-preserving multi-keyword ranked search over encrypted cloud data, INFOCOM, 2011 Proceedings IEEE.

[11] B. Goswami, and Dr..S.N. Singh, 2012. Enhance security in cloud computing using public key cryptography with matrices, International Journal of Engineering Research and Applications, vol.2, issu.4, pp.339-344.

[12] S. Pearson and A. Benameur, 2010. Privacy, Security and Trust Issues Arising from Cloud Computing, 2nd IEEE International Conference on Cloud Computing Technology and Science, Cloudcom- PP 693-702.

[13] D. Chen, 2012 .Data security and Privacy Protection issues in Cloud Computing, Computer Science and Electronics Engineering (ICCSEE) International Conference, PP 647-651.

[14] D W. Chadwick and K. Fatema, 2012. A privacy preserving authorization system for the cloud, Journal of Computer and System Sciences, PP 1359-1373.

[15] C. Mont, and Pearson, 2005. An Adaptive Privacy Management System for Data Repositories, Trust, Privacy and Security in digital business, Volume 3592, pp 236-245.

[16] S. Pearson, 2009. Taking Account of Privacy when Designing Cloud Computing Services, ICSE'09 workshop, Vancouver, Canada, 978-1-4244-3713-9-09, IEEE, Page no 44-52.

[17] C.Saravanakumar and C.Arun, 2014. Survey on Interoperability, Security, Trust, Privacy Standardization of Cloud Computing, Contemporary Computing and Informatics (IC3I), pp 997-982.

[18] S. Meena, E Daniel and Dr. NA. Vasanthi, 2013. Surveyon Various Data Integrity Attacks in Cloud Environment and the Solutions, International Conference on Circuits, Power and Computing Technologies [ICCPCT], pp 1076-1081.

[19] Y. Zhu, H. Hu, G. Ahn, and M. Yu, 2012. Cooperative provable data possession for integrity verification in multi-c1oud storage, IEEE Transactions on Parallel and Distributed Systems, no. 99.

[20] A. Jaberi, 2014. M.F Data integrity and Privacy model in cloud computing, Biometrics and Security Technologies (ISBAST), PP 280-284.

[21] Sanjeev Kumar, Krishan Kumar and Anand pandey, 2014. A Comparative Study of Call Admission Control in Mobile Multimedia Networks using Soft Computing, International Journal of Computer Applications (0975 – 8887) Volume 107 – No. 16, December.

[22] Sanjeev kumar, Krishan kumar and pramod kumar, 2015.Mobility based call admission control and resource estimation in mobile multimedia networks using artificial neural networks,1st IEEE International Conference on Next Generation Computing Technologies, Dehradun

[23] Vikas sagar and krishan kumar, 2014. A Symmetric Key Cryptographic Algorithm Using Counter Propagation Network (CPN), ACM sponsored International Conference on Information and Communication Technology for Competitive Strategies.

[24] Fi-John Chang, Yen-Chang Chen, 2001. A counter propagation fuzzy neural network modeling approach to real time stream flow prediction, journal of hydrology, ELSEVIER.

[25] Vikas Gujral, 2009. Cryptography using artificial neural network, Engineering National Institute of Technology Rourkela-769008 Orissa.

[26] Jacek M Zurada, 1992. Introduction to Artificial Neural Systems, West publishing company, St. Paul New York Los Angeles San Francisco.