# Interfacing of Neural Network in Cryptography and Security Mechanisms of System

**Dr. Aruna J. Chamatkar[1], Prof. Sachin Y. Zade[2] and Dr. Pradeep K .Butey[3]**

[1] Associate Prof., MCA Department, Kamla Nehru Mahavidyalaya, Nagpur

[2]Assistant Prof., MCA Department, Kamla Nehru Mahavidyalaya, Nagpur

[3]HOD, Department of Computer Science, Kamla Nehru Mahavidyalaya, Nagpur

## Abstract

*The main issue with wireless network security is its simplified access to the network compared to traditional wired networks such as Ethernet. With wired networking it is necessary to either gain access to a building, physically connecting into the internal network, or break through an external firewall. Most business networks protect sensitive data and systems by attempting to disallow external access. Thus being able to get wireless reception provides an attack vector, if encryption is not used or can be defeated. One most important Artificial Neural Network (ANN) has its adaptive in nature and hence many existing paradigms can be fused into it easily. Pattern mapping technique of artificial neural networks is also useful in generating the encrypted passwords without going with any standard encryption algorithm. ANN can easily be utilized for establishing the relationship between the input pattern in the form of password code and output pattern in the form of encrypted password. In this paper we review on security issues and challenges in IT and studies how neural network is interfacing cryptography. Methods of security like cryptography and how neural networks are effective in terms of reducing complexity and increasing speed and accuracy in a security system. Neural networks provide a number of advantages in the detection of these attacks.*

**Keywords:** ANN, Cryptography, Neural Network, Computer Security.

## 1. INTRODUCTION

There are various strategies and techniques used to design security systems. However, there are few, effective strategies to enhance security after design. That way even if an attacker gains access to one part of the system, fine-grained security ensures that it is just as difficult for them to access the rest. There are many aspects to secure many applications ranging from secure in many firms like payments to private communication and protecting password. One of such aspect for secure communication is that of cryptography. Cryptography is the science of writing in secret codes and is an ancient art. Cryptography is a technique to encrypt simple message into cipher text for secure transmission over any channel. The training of the network has been done using the input output set generated by the cryptosystem. Cryptosystem is the system where we are implementing the cryptographic system.

Artificial Neural Networks can easily be utilized for establishing the relationship between the input patterns in the form of password code and output pattern in the form of encrypted password. Pattern mapping technique of artificial neural networks is also useful in generating the encrypted passwords without going with any standard encryption algorithm. This relationship can be made with proper training of feed forward neural network for different combinations of the input pattern with output pattern pair. Different types of neural network can also deciding more secure and complex structure of NN with their description so we can apply that type of NN.

In this paper we go through various challenges in security in IT field, as well as we review the studies of cryptography mechanisms. Also we are mainly focus on how Neural Network providing interfacing in cryptography.

## 2. SECURITY CHALLENGES AND ISSUES

a. **Technology with Weak Security –** New technology is being released every day. More times than not, new gadgets have some form of Internet access but no plan for security.

**b.** **Social Media Attacks –** Users of internet (attacker) are leveraging social media as a medium to distribute a complex geographical attack.

**c.** **Mobile Malware –** Security experts have seen risk in mobile device security since the early stages of their connectivity to the Internet far less concerned than they should be.

**d.** **Third-party Entry –** Cybercriminals prefer the path of least resistance. Target is the poster child of a major network attack through third-party entry points.

**e.** **Neglecting Proper Configuration –** Companies continue to neglect the importance of properly configuring security settings.

**f.** **Outdated Security Software –**Software is developed to defend against known threats. That means any new malicious code that hits an outdated version of security software will go undetected.

**g.** **Social Engineering –**. They have turned to reliable non-technical methods like social engineering, which rely on social interaction and psychological manipulation to gain access to confidential data.

**h.** **Lack of Encryption –** Protecting sensitive business data in transit and at rest is a measure few industries have yet to embrace, despite its effectiveness requires every computer to be encrypted.

**i.** **Corporate Data on Personal Devices –** Whether an organization distributes corporate phones or not, confidential data is still being accessed on personal devices.

**j.** **Inadequate Security Technology –**The software is designed to send alerts when intrusion attempts and alerts are only valuable if someone is available to address them.

Here we are listing some security issues in information technology that are important to studies while Considering security mechanisms of system. By studying this challenges we need to focus towards the different aspects of security.

## 3. CRYPTOGRAPHY

The goal of any cryptographic system is to exchange of information among the intended users without any leakage of information to others who may have unauthorized access to it. A common secret key could be created over a public channel accessible to any opponent. Neural networks can be used to generate common secret key. In case of neural cryptography, both the communicating networks receive an identical input vector, generate an output bit and are trained based on the output bit. The two networks and their weight vectors exhibit a novel phenomenon, where the networks synchronize to a state with identical time-dependent weights. The generated secret key over a public channel is used for encrypting and decrypting the information being sent on the channel.

There are some basic terms used in cryptography are as follows:

- Plain text – The original message to be transferred to the other person.
- Cipher text – The secret version of the plain text which is used for transferring.
- Key – A secret code which is used to lock or unlock the plain text and the cipher text respectively.
- Encryption – The process of converting plain text to cipher text.
- Decryption – The process of converting cipher text to plan text.

## 4. NEURAL NETWORK

An Artificial Neural Network is an information processing paradigm that is inspired by the way biological nervous systems, such as the brain, process information. The key element of this paradigm is the novel structure of the information processing system. It is composed of a large number of highly interconnected processing elements (neurons) working in unison to solve specific problems.

The structured of neural network consist of different types layers

i) Input Layer-It contains those units (artificial neurons) which receive input from the outside world on which network will learn, recognize about or otherwise process.

ii)Hidden Layer-These units are in between input and output layers. The job of hidden layer is to transform the input into something that output unit can use in some way.

ii)Output Layer-It contains units that respond to the information about how it's learned any task.

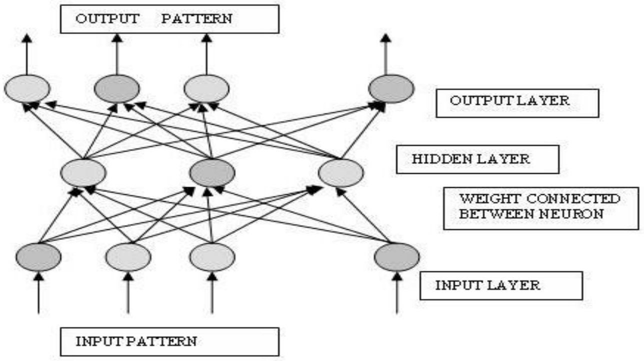


**Figure 1 : Basic structure of Neural Network**

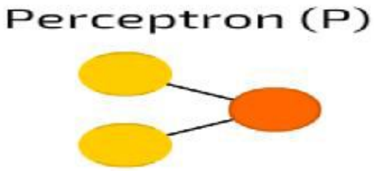
## 4.1 FEATURES OF ANN

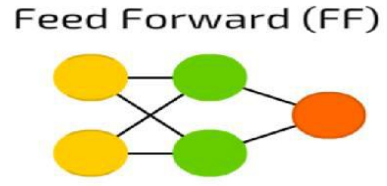
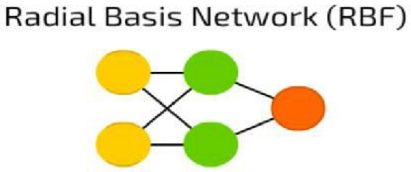
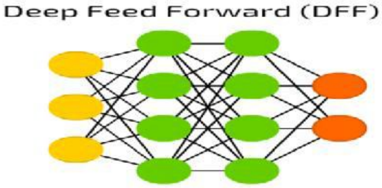
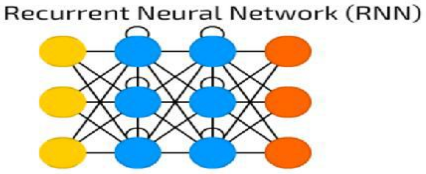
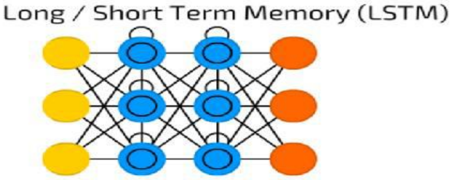
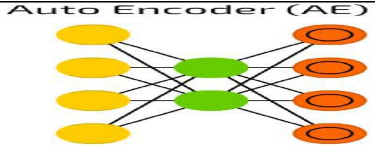
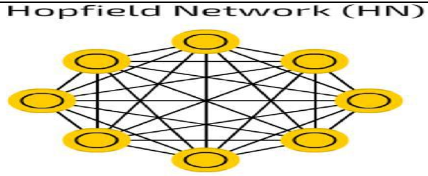
**i) Adaptive learning:** An ability to learn how to do tasks based on the data given for training or initial experience.
ii) **Self-Organization:** An ANN can create its own organization or representation of the information it receives during learning time.
iii) **Real Time Operation:** ANN computations may be carried out in parallel, and special hardware devices are being designed and manufactured which take advantage of this capability.
iv) **Fault Tolerance via Redundant Information Coding:** Partial destruction of a network leads to the Corresponding degradation of performance. However, some network capabilities may be retained even with major network damage.

## 4.2 TYPES OF NEURAL NETWORK

We go through the many types of neural networks available or that might be used in the development stage. They can be classified depending on their: Structure, Data flow, Neurons used and their density, Layers and their depth activation filters etc.

**Table 1: Different types of neural network with their description**

| **Sr. No.** | **Types of Neural Network** | **Description** |
|---|---|---|
| 1. |  | The simplest and oldest model of Neuron, as we know it. Takes some inputs, sums them up, applies activation function and passes them to output layer. |

| | | |
|---|---|---|
| 2. |  | In single layer network, 'single layer' refers to the output layer of computation nodes<br>1. all nodes are fully connected<br>2. activation flows from input layer to output, without back loops<br>3. there is one layer between input |
| 3 |  | The Radial Basis Network is same as the Feed forward NNs only in use radial basis function as activation function instead of logistic function |
| 4 |  | DFF neural networks consist of FF NNs, but with more than one hidden layer. |
| 5 |  | Type of neural network in which hidden layer neurons has self-connections. Recurrent neural networks possess memory. At any instance, hidden layer neuron receives activation from the lower layer as well as it previous activation value |
| 6 |  | This type introduces a memory cell, a special cell that can process data when data have time gaps (or lags). Memory cells are actually composed of a couple of elements called gates, that are recurrent and control how information is being remembered and forgotten. |
| 7 |  | Auto encoders are used for classification, clustering and feature compression. |
| 8 |  | Hopfield networks are trained on a limited set of samples so they respond to a known sample with the same sample.<br>Each cell serves as input cell before training,as hidden cell during training and as output cell when used. |

## 5.HOW NEURAL NETWORK INTERFACES IN CRYPTOGRAPHY

Neural cryptography deals with the problem of key exchange using the mutual learning concept between two neural networks. The two networks will exchange their outputs (in bits) so that the key between the two communicating parties is eventually represented in the final learned weights and the two networks are said to be synchronized. Security of neural synchronization depends on the probability that an attacker can synchronize with any of the two parties during the training process, so decreasing this probability improves the reliability of exchanging their output bits through a public channel.
Artificial neural networks are used to classify functional blocks from a disassembled program as being either cryptography related or not. The resulting system, referred to as NNLC (Neural Net for Locating Cryptography). When training a neural network it is tempting to experiment with architectures until a low total error is achieved. The danger in doing so is the creation of a network that loses generality by overlearning the training data; lower total error does not necessarily translate into a low total error in validation. The resulting network may keenly detect the samples used to train it, without being able to detect subtle variations in new data.

### 5.1 SECURE PASSWORD

Passwords are at present the most common method for verifying the identity of a user. This is a defective method; systems continue to use passwords because of their ease of use and ease of implementation. Among many problems are the successful guessing of user‘s passwords, and the intercepting of them or uncovering them online. When a particular user submits his login credentials, his username is given as input to network and we check whether the output of network and specified password are equal or not, if both are equal the user is authorized and rejected otherwise. A method is presented for choosing the best neural network architecture for a given data set based on observation of its accuracy, precision, and mean square error.

### 5.2 PSEDOCODE

**Following PSEDOCODE is used to encode secure password USERID and PASSWORD**

```
Step I.   START
Step II.  INPUT USERID AND PASSWORD
Step III. TRAIN THE NEURAL NETWORK FOR GIVEN USERID AND PASSWORD
Step IV. USER SIGNIN BY TYPING USERID AND PASSWORD
Step V.  USERID IS ENCODED AND ACCEPTED BY NETWORK AS INPUT
Step VI. OUTPUT OBTAINTED FROM NETWORK AND ENCODED PASSWORD ENTERED BY USER
ARE COMPAIRED
Step VII. IF NETWORK OUTPUT = PASSWORD THEN LOGIN SUCCESSFUL
ELSE LOGIN FAILED
END IF
StepVIII. END
```

### 5.3 REPRESENTATION OF FLOW

The method, based on, relies on k-fold cross validation to evaluate each network architecture k times to improve the reliability of the choice of the optimal architecture. The need for four separate divisions of the data set is demonstrated (testing, training, and validation, as normal, and a comparison set). Instead of measuring simply the total error the resulting discrete measures of accuracy, precision, false positive, and false negative are used. This method is then applied to the problem of locating cryptographic algorithms in compiled object code for two different CPU architectures to demonstrate the suitability of the method.

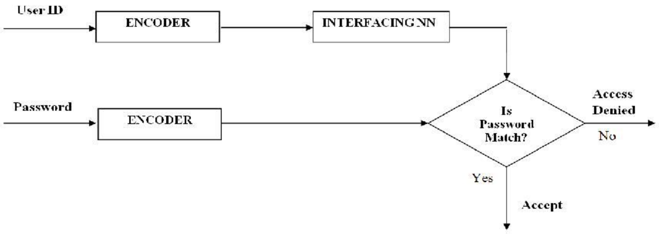


**Figure 2: Flowchart to represent Encoding Secure Password**

## 6. CONCLUSION

In this paper we basically focusing review on security issues and challenges in IT as well as study the terms used in cryptography. For implementing the concept we studied the number of different types of Neural Network. We consider a Hopfield Neural Network of fully interconnected N neurons. In this network, we present N patterns of N bit each of bipolar nature. The associative memory property of the Hopfield Model will generate the associative pattern for every presented input pattern. Trained the neuron by providing known valued. It is used to Cryptographic Algorithm to secure Local Area Networking models of Neural Network.

## 7. References

[1] S.Z. Reyhani, M. Mahdavi, "User Authentication Using Neural Network in Smart Home Networks," International Journal of Smart Home, Vol 1 no 2, pp147, July 2007.

[2] Jacek M. Zurada- " Introduction to Artificial Neural Network" Jaico Publishing House, 1999

[3] Arvandi M., Wu S., Sadeghian A., Melek W. W., Woungang I.: Symmetric Cipher Design Using Recurrent Neural Networks.International Joint Conference on Neural Networks, pp.2039–2046, 2006.

[4] Chi-Kwong C., Cheng L. M.: The convergence properties of a clipped Hopfield network and its application in the design of key stream generator. IEEE Trans. Neural Networks, 12, pp. 340–348, 2001.

[5] Godhavari T., Alainelu N. R., Soundararajan R.: Cryptography Using Neural Network. IEEE Indicon 2005 Conference,, (I), pp. 11–13, 2005.

[6] Guo D., Cheng L.-M., Cheng L. L.: A new symmetric probabilistic encryption scheme based on chaotic attractors of neural networks. Appl. Intell., 10(1), pp. 71–84, 1999.

[7] Hagan M. T., Beale M. H., Demuth H. B.: Neural Network Toolbox User's Guide. TheMathWorks, Inc, 2009.

[8 ] Stuart J. Russell and Peter Norvig ]"Artificial Intelligence A Modern Approach "

[9] http://www.garykessler.net /crypto.html

[10] ITSecurity. (2007) Network Security Threats for SMBs.

**AUTHORS**

Dr. Aruna J. Chamatkar is Associate Professor at Kamla Nehru Mahavidyalaya, Nagpur. She has done PhD in Computer Science from RTM Nagpur University, Nagpur under the guidance of Dr. Pradeep K. Butey. Her research area is Data Mining and Neural Network.

Prof. Sachin Y. Zade is Assistant Professor at Kamla Nehru Mahavidyalaya, Nagpur.
Currently pursuing PhD from RTM Nagpur University, Nagpur under the guidance of Dr. Pradeep K. Butey. His research area is Network Security and Neural Network.

Dr. Pradeep K Butey is Associate Professor and HOD of Computer Science Department at Kamla Nehru Mahavidyalaya Nagpur. He is research supervisor for the subject of Computer Science and has guided many students of RTMNU Nagpur University. His area of interest is Fuzzy Logic, Neural Network, and Theoretical Computer Science.