

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

Dr. Aruna J. Chamatkar<sup>1</sup>, Prof. Sachin Y. Zade<sup>2</sup> and Dr. Pradeep K .Butey<sup>3</sup>

<sup>1</sup> Associate Prof., MCA Department, Kamla Nehru Mahavidyalaya, Nagpur

<sup>2</sup> Assistant Prof., MCA Department, Kamla Nehru Mahavidyalaya, Nagpur

<sup>3</sup> 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