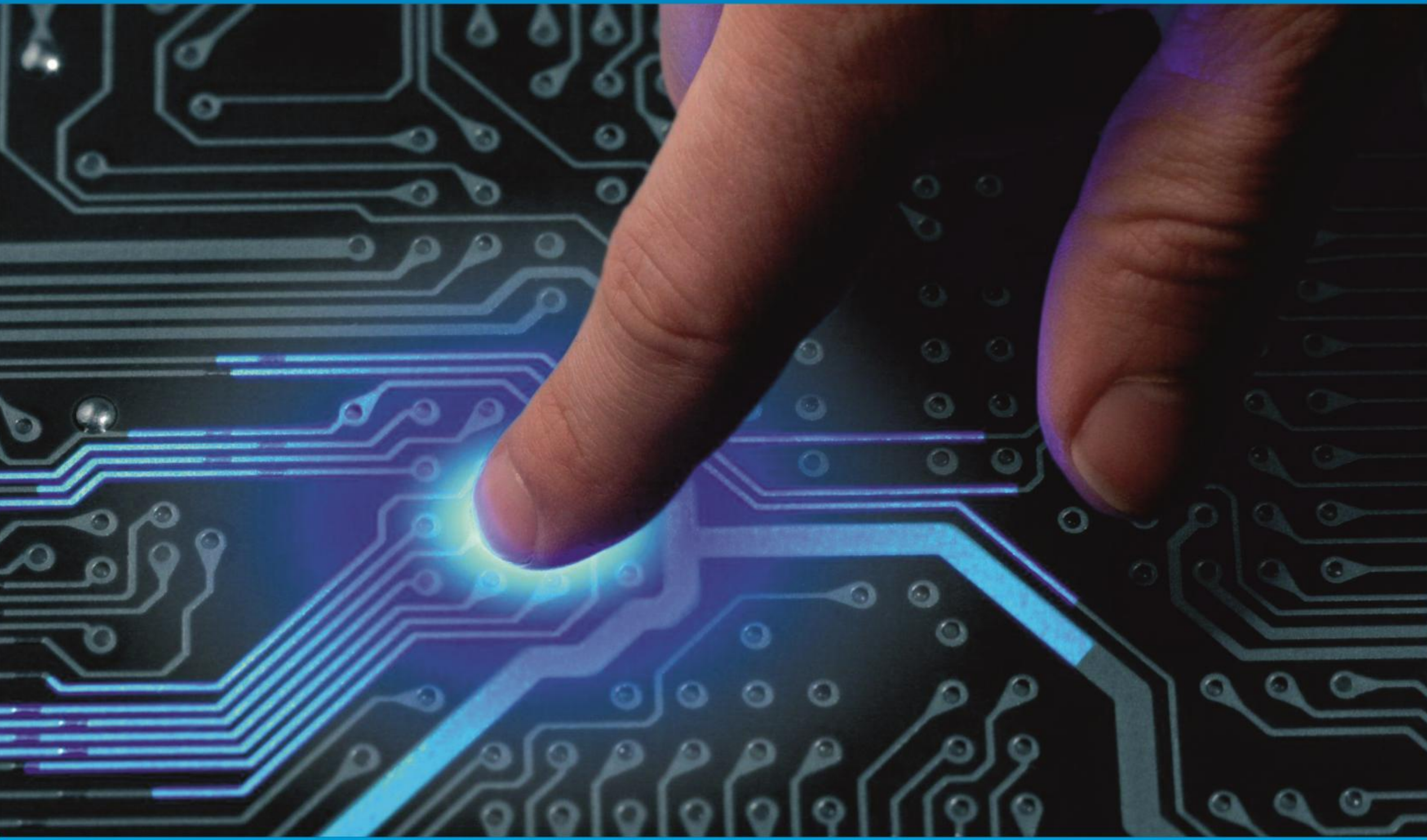
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 1, January 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 1, January 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0901010 |

Secure Transfer of Symmetric Key in an Unsecure Channel Using Artificial Neural Network

Megha Sharma, Pankaj Rathi

Research Scholar, M.Tech. (Digital Communication), SITE, Nathdwara, India

Assistant Professor, Dept. of Electronics and Communication, SITE, Nathdwara, India

ABSTRACT: An Artificial Neural Network is a technique which is designed for modelling the way in which the brain performs a particular task. The network is implemented by using hardware, software and firmware. The brain is a highly complex, nonlinear and parallel information processing system. It has the capability to organize its structural constituents, known as neurons, so as to perform certain computations many times faster than the fastest digital computer.

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. It uses mathematical techniques for information security. Information security is now a compulsory component of commercial applications, military communications and also social media implementation. This is a result of the many threats and attacks that can be made to these networks by people with malicious intent.

I. INTRODUCTION

For first few decades, university researchers mainly used computer networks to send e-mails, while company employees mainly used computer networks to share printers. In this case, security has not attracted much thought. But now that millions of regular citizens are using the Internet for banking, shopping or tax proceeds, hidden dangers to network sanctuary are becoming more serious.

In the last few decades before prevalent use of data dispensation apparatus, requirements for information security in organizations have undergone major changes. With preface of computers, need for mechanical tools to protect files or other information accumulate on computers became obvious. This is particularly true for shared systems such as time-sharing systems, or need for systems accessible via public telephones or data networks is even more urgent. The collective term for collecting tools used to protect data and prevent hackers is "computer security". [1]

II. BIOLOGICAL MODEL

The human nervous structure can be wrecked down into 3 theatre that may be symbolize as follows:

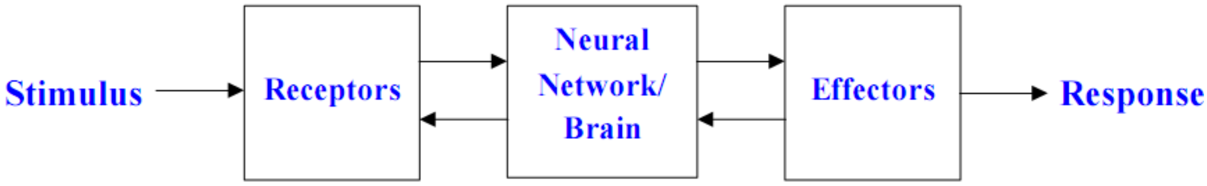


Fig 1: Block Diagram of a Human Nervous System.

The receptor collects information from atmosphere. The effector interacts with situation, for example. Activate strength. The flow of information / activation is indicated by arrows. There is an intertwined organizational hierarchy:

Molecules and ions
2. Synapse
3. Neuron microcircuits
4. Dendritic wood
5. Neurons
6. Local circuit

7. Interzone circuits
8. Central nervous system

III. ANN STRUCTURE

An reproduction neural system consists of a set of plain processor units that converse by distribution signals to each other over a great number of prejudiced associations. [5] A number of key feature of artificial neural network are:

- A set of treatment units ("neurons", "cells");
- The activation mode Yk for each device corresponds to the output of the device;
- Connectivity between devices. In general, each compound is definite by a weight Wjk which conclude influence of signal from unit j on unit k;
- Reproduction rules that determine the unit's effective input Sk from external input.
- Activation meaning Fk, which conclude new activation level according to valid input Sk (t) or modern activation Yk (t) (ie update);
- External input (aka bias, bias) θk for each device, a process of information assembly (learning rules);

- The situation in which the system is to operate, provide input signals or provide error signals when necessary.

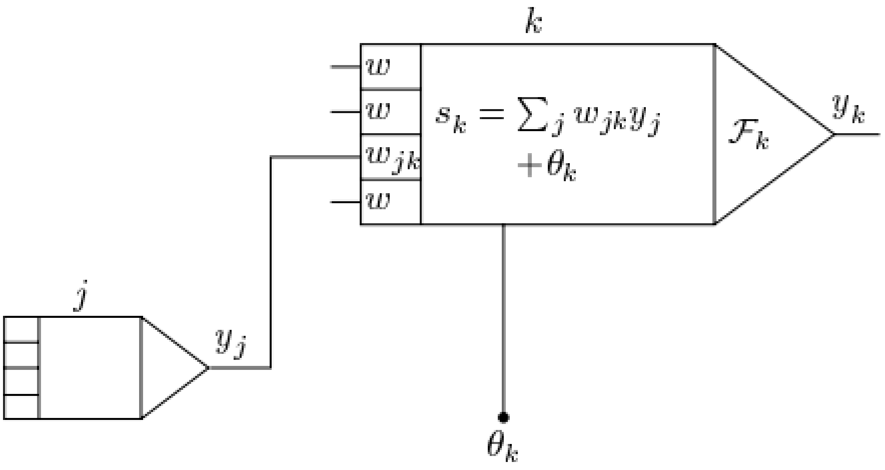


Fig 2: The basic components of an artificial neural network

TWIN NEURAL NETWORK

officially, a neural network consists of a group of neurons mass in input or output layers and single or many hidden layers. These neurons are initialized with chance weights. As neural system learns from the education examples, weights are modernized using update rules based on error minimization methods (such as gradient tumble). Through iteration, these weights converge to their optimum values, allowing effective predictions on test samples, and this example simply run through the network to obtain category forecasts. The optimal weight is used to calculate the activation of neurons in midway layer and the expected value of the last layer to reach the test point. This makes neural system scalable to great datasets. though, it has been shown that neural system often suffer from over-assembly or poor simplification aptitude.

IMPLEMENTATION

In this section, how to program neural machine or how to use MATLAB is been described.
DESIGNING OF A SIMPLE NEURAL NETWORK FOR ENCRYPTION AND DECRYPTION-
For designing of a simple neural network, for encryption of keys consists of four fundamental parts-

- The key that we need to encrypt.
- Key obtained after encryption process.
- Neural network required for encryption process.
- The Backpropagation algorithm used to train neural network.

Performance (plotperform): It plots graph between error vs epoch for the training, validation, and test performance of the training record. The plot performance chart shows the best verification performance in a given period. Training stops when the mean square error (MSE) of the validation test begins to increase.

Training mode (plottrainstate): The graph of plottrainstate shows the state of the system after training according to the default values for various input parameters.

Regression (plot regression): The plot regression diagram shows the curves between 0-output data and training examples, between output data and verification examples and between output data and test examples (R-value shows the relationship between output and target value).

- For Encryption
    - Plotperform

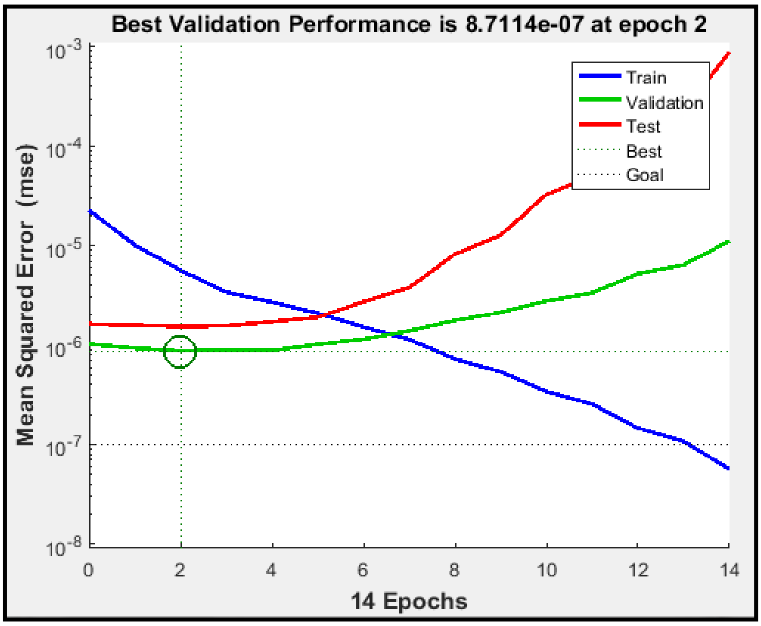


Figure 3 : Performance Plot for Encryption

IV. CONCLUSION

We have tested behaviour of neural network for the encryption and decryption process. The proposed neural network has been experienced for different statistics of education iteration or for changed number of hidden neurons and input data. The reproduction result has shown a very good consequence, with comparatively better presentation than conventional encryption technique.

The algorithm used for training neural network was Scaled Conjugate Gradient. The reason behind using this algorithm over other training algorithm was that firstly, it gives better result when used for larger data sets. Secondly, it avoids the time consuming line search which is performed in other algorithms and thirdly, this algorithm unite model-trust region advance (used in Levenberg-Marquardt algorithm) with conjugate gradient advance.

REFERENCES

[1] M.Bishop. (19 February, 2003). "What is Computer Security". *IEEE Security and Privacy* (pp. 67-69). IEEE.

[2] M.Guizani. (23 January, 2006). "Computer and Network Security". *Global Telecommunication Conference.* St. Louis, MO, USA: IEEE.

[3] A.Eskicioglu, & L.Litwin. (February, 2001). "Cryptography". *IEEE Potentials. 20*, pp. 36-38. IEEE.

[4] N.Ferguson, & B.Schneier, T. (2010). In *"Cryptography Engineering: Design Principles and Practial Applications".* Wiley Publishing.

[5] Kumar, P., & Sharma, P. (2014). "Artificial Neural Network - A Study". *International Journal of Emerging Engineering Research and Technology (IJEERT) , 2* (2), 143-148.

[6] Kinzel, W., & Kanter, I. (05 June, 2003). "Neural Cryptography". *IEEE*, (pp. 1-4). Singapore.

[7] R.Mislovaty, E.Klein, I.Kanter, & W.Kinzel. (2004). Security of Neural Cryptography. *IEEE*, (p. 3).

[8] T.Godhavari, Alamelu, N., & Soundararajan, R. (2005). Cryptography Using Neural Network. *IEEE*, (p. 4).

[9] E.C.Laskari, G.C.Meletiou, D.K.Tasoulis, & M.N.Vrahatis. (5 December, 2005). "Studying the Performance of Artificial Neural Network on Problems Related to Cryptography". *Nonlinear Analysis: Real World Application.* Elsevier.

[10] T.Schmidt; H.Rahnama; A.Sadeghian (09 December, 2008). "A Review of Applications of Artificial Neural Network in Cryptosystem". *Automation Congress. WAC 2008. World.* Hawaii, USA: IEEE

[11] Yu, H., & M.Wilamowski, B. "Levenberg-Marquardt Training".

[12] A.Forouzan. (2007). "Cryptography and Network Security". USA: McGraw-Hill.

[13] S.R.Subramanya. (05 July 2006). "Digtal Signature". *IEEE Potentials* (pp. pages 5-8). IEEE.

[14] Sheshasaayee, A. (13 July 2017). "Digital Signatures Security Using Cryptography for Industrial Application". *Innovative Mechanisms for Industry Applications.* Banglore, India: IEEE.

[15] *Digital Signature*. (n.d.). Retrieved from Search Security: http://searchsecurity.techtarget.com/

[16] Volna, E., Kotyrba, M., Kocian, V., & Janosek, M. "Cryptography Based on Neural Networks". *26th European Conference on Modelling and Simulation.*

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING