Development of a Highly Secured and Scalable Network Security Framework using Secured Neural Network Algorithm

[1]Ohaneme, L.C., [2]Ibiejugba, M.A. and [3]Adejo, B.O

[1]Department of Computer Science, Federal Polytechnic, Oko Anambra State

[2, 3] Department of Mathematical sciences, kogi State University, Anyigba kogi State

Abstract--- The vulnerability of transmitted data in computer network has brought untold hardship to network users and operators. The loss of data due to network insecurity in the recent times has made the information system less reliable and prone to attacks. Therefore, this work tries to develop highly secured and scalable network security framework that will guarantee optimum security to network users using secured neural network algorithm. In this work NeuroSec+ is proposed using neural network back propagation supervisory learning algorithm to train automatically stored encrypted passwords. The proposed method can solve the security problems in computer network system and can be used to store the users' profiles and access controls in smart home networks.

Keywords: Network security, neural network algorithm, framework

I. INTRODUCTION

The authentication and authorization of users in smart environment are the key factors in the security of home networks users. Authentication has been traditionally based on PIN, password, key, cryptography, smart card or biometrics. It is widely used to identify legitimate users, because passwords are cheap, easy and reasonably accurate. These methods use some encryption algorithms to prevent the passwords from being revealed, but they are still vulnerable. An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack [1]

To lessen the vulnerability of the computer to the network there are many products available. The tools used in tackling security are encryption, authentication mechanisms, intrusion-detection, security management and firewalls. Networks running businesses throughout the world are using a combination of some of these tools to combat network security vulnerabilities. In most cases, Intranets are both connected to the internet and reasonably protected from it. The internet architecture itself leads to vulnerabilities in the network when closely observed. Understanding the security issues of the data centre and internet design greatly assists in developing new security technologies and approaches for networks with internet access and internet security itself.

Besides, the types of attacks through the data centre and internet need to also be studied to be able to detect and guard against them. Intrusion detection systems (IDS) are established based on the types of attacks most commonly used on these networks.

Typical security currently exists on the computers connected to the network for the enterprise market segments. In existing works, security protocols sometimes usually appear as part of a single layer of the Open System Interconnection (OSI) network reference model. The use of traditional passwords has its drawbacks with respect to authentication in data centre networks, etc, [2] viz:

- User password difficult to memorize.
- User cannot freely choose is password
- User cannot change his password
- It cannot withstand forgery attack

The word neural network is referred to a network of biological neurons in the nervous system that process and transmit information. Artificial neural network is an interconnected group of artificial neurons that uses a mathematical model or computational model for information processing based on a connectionist approach to computation. They made of interconnecting artificial neurons which may share some properties of biological neural networks. Literally, it is a network of simple processing elements (neurons) which can exhibit complex global behavior, determined by the connections between the processing elements and element parameters. Therefore, neural network can be defined as an artificial representation of the human brain that tries to simulate its learning process.

The essence of neural networks is to learn the behavior of actors in the system (e.g. security policies). Neural networks use its learning algorithms to learn about the relationship between input and output vectors and to generalize them to extract new input/output relationships. The advantage of using neural networks over statistics is its ease in expressing and learning nonlinear relationships between variables. Experiments using neural networks will result in accurately predicting the behavior of security policies in the data center network core. In this research, the use of Secured Neural Network Algorithm to structure a proposed NeuroSec+ is presented.

II. REVIEW OF RELATED LITERATURE

According to [3], following the contemporary world of hackers and malware, the resiliency and security of computerized control systems such as the Supervisory Control and Data Acquisition (SCADA) or systems used in nuclear plants are of relevant concern. The computer systems used within critical infrastructures are susceptible to various threats of cyber attacks and are potentially vulnerable. As a matter of fact, in many cases they might be even more vulnerable than common information technology systems. While many intrusion detection systems have been already proposed, they do not always suit the needs of critical infrastructure control system. Rather, these systems were typically developed using publicly available datasets such as the KDD CUP 1999 [4].

Therefore, tailoring such an intrusion detection system to the specific needs of critical infrastructures can significantly improve their security. This is mainly due to the fact that these systems are often composed of interconnected computer-based sub-systems exchanging crucial information via the computer network.

The original idea of an intrusion detection system goes back to 1980 and an early intrusion detection model was proposed by Denning in 1987 [5]. An intrusion can be defined as follows: Having a system performing predefined legal tasks, an intrusion is anything that differs from the allowed operations and was in most cases generated with the intention of compromising or misusing the informational system. Consequently, the intrusion detection system (IDS) attempts to detect and trace such an inappropriate, incorrect and illegal or anomalous activity within the computer network. Generally, there are two kinds of IDS, the anomaly based and the signature based IDS. The training process of a signature based IDS require a database of known and labelled intrusion instances [6], every input vector is assigned either to the normal or to the intrusion class. The main advantage of such system is its capability to correctly recognize intrusion attacks that match previously seen signatures. However, the main drawback of signature based IDS is the inability to recognize previously unseen intrusion vectors. These intrusions will deceive the system and they will generate a significant number of false negatives (intrusions labelled as normal behaviour).

One of the main contributions of the presented research work is the use and analyses of real network data (data recorded from an existing critical infrastructure) to ascertain quality of service performance under existing security implementations.

The work in [7] presented an analysis of Artificial Neural Networks (ANN) being used in the development of effective Intrusion Detection Systems for computer systems and computer networks. In their work, the ANNs technologies, which were discussed, were designed to detect instances of the access of computer systems by unauthorized individuals and the misuse of system resources. The authors reviewed the foundations of Intrusion Detection Systems and other ANNs, while deriving a comparative analysis of different ANNs in Intrusion Detection.

The authors in [8] opined that password authentication is a common approach to the system security as well as an important procedure for gaining access to user resources. Unlike in the conventional password authentication methods where a server has to authenticate the legitimate user, in their proposed method, users can freely choose their passwords from a defined character set or they can use a graphical image as password and that input will be normalized.

Consequently, the work proposed a method for password authentication using alphanumeric password and graphical password. In this regard, the work used Back Propagation algorithm (see Figures 2.1 and 2.2) for both alphanumeric (Text) and graphical password by which the level of security can be enhanced. The work concludes along with test results that by converting user password in to Probabilistic values, this will enhance the security of the system.

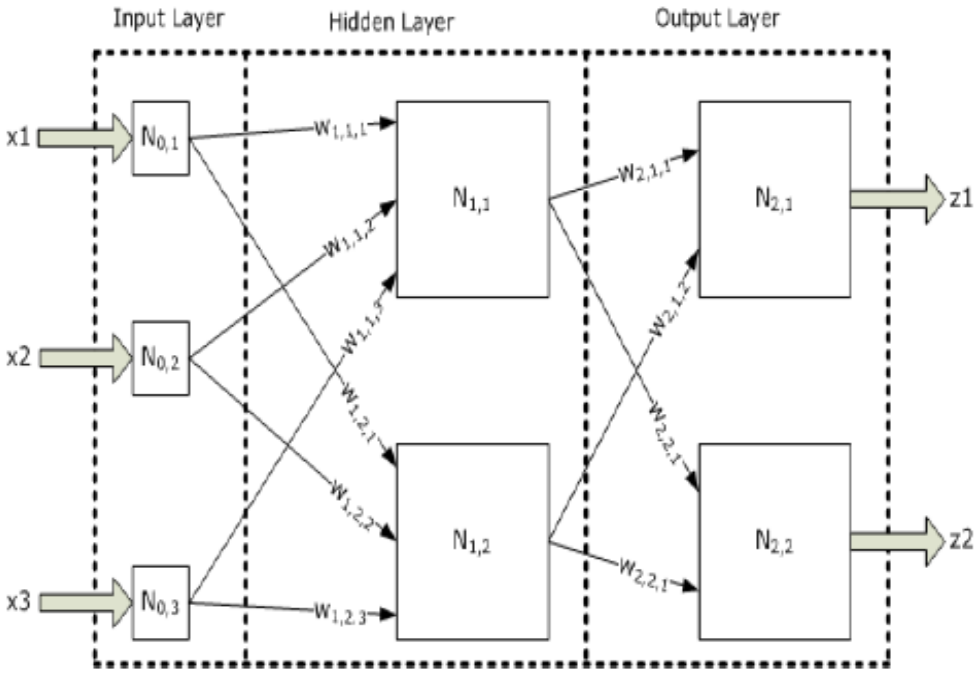

Figure1: Back propagation [8]

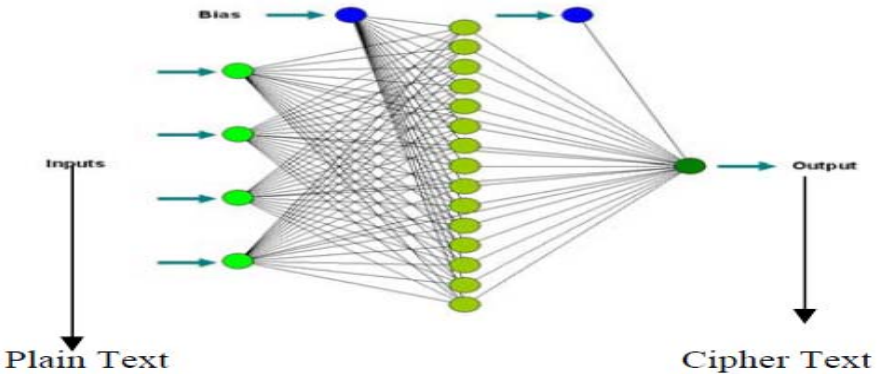

Figure 2 Feed forward Network [8]

The authors in [9], proposed the use of neural network and machine learning as the approaches through which security intrusion challenges can be overwhelmed. The work opined that anomaly in the Anomaly based Intrusion Detection System can be detected using various Anomaly detection techniques. The work argued that Dimension Reduction can be done using Principle Component Analysis while the Support Vector Machine can be used to specify the classifier construction problem for high network security. Figure 2.3 shows the classifications of IDS as studied in [9]

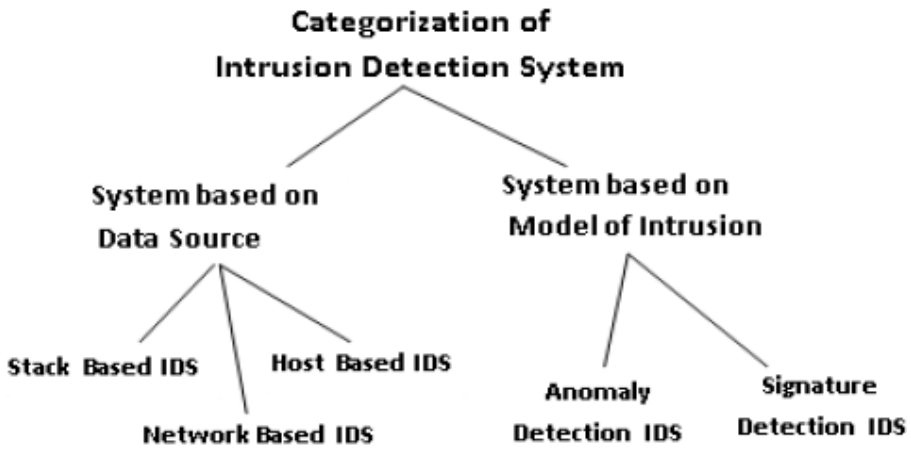

Figure 3 Categorization of Intrusion Detection System [9]

In the work of [10], the authors focused on intrusion detection in computer and network systems.

While discussing on detection as a major part of any security tool viz: Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Adaptive Security Alliance (ASA), check points and firewalls, the authors then adopted its schemes for probing attacks in computer networks. Their approach leveraged supervised neural network phenomenon that is majorly used for detecting security attacks while taking into account Multiple Layered Perceptron (MLP) architecture and resilient back propagation for its training and testing in their proposed model.

The work of [11] proposed an enhanced password based security system based on user typing behaviour, which will attempt to identify authenticity of any user failure to login in first few attempts by analysing the basic user behaviours/activities and finally training them through neural network and classifying them as genuine or intruder. In their experiments, data were collected in real time and analysed using Visual Basic 6.0 as a front end and Microsoft Access 2003. Figure 2.4 shows the feed forward architecture with two outputs.

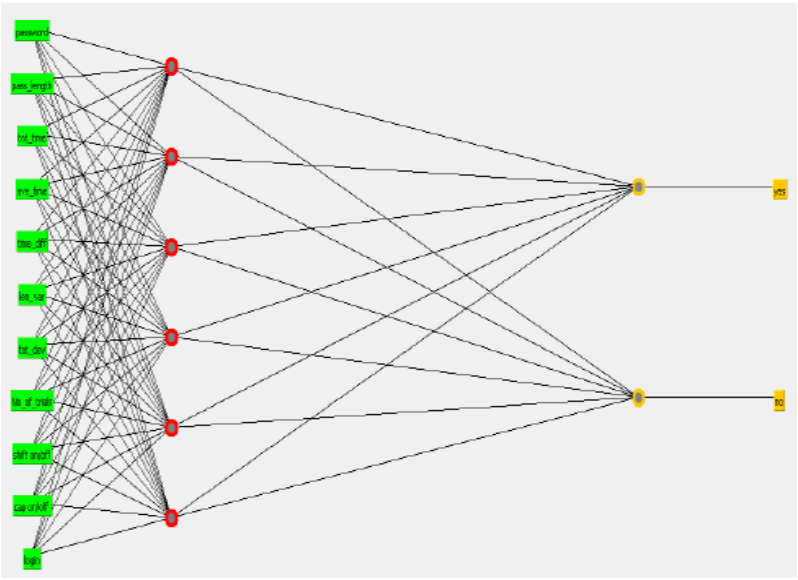

Figure 4. Feed forward Architecture with two outputs

A multi-agent system that incorporates an Artificial Neural Networks based Intrusion Detection System (IDS) has been defined to guaranty efficient computer network security architecture. The proposed system facilitates the intrusion detection in dynamic networks. The work proposed a structure of the Mobile Visualization Connectionist Agent-Based IDS that is flexible and adaptable.

The contribution of their system includes the introduction of deliberative agents that use the artificial neural network to identify intrusions in computer networks.

The works in [12] proposed a new way of applying neural networks to detect intrusions. In their work, it was asserted that a user leaves a 'print' when using the system; and then, a neural network can be used to learn this print and identify each user much like detectives use thumbprints to place people at crime scenes. A back propagation neural network called NNID (Neural Network Intrusion Detector) was trained in the identification task and tested experimentally on a system of 10 users. The work concluded with its results suggesting that learning user profiles is an effective way for detecting intrusions.

In their work, since security of computer networks plays a strategic role in modern computer systems, their work proposed a pattern matching IDS for network security. The work opined that many network security applications rely on pattern matching to extract the threat from network traffic. Also, the increase in network speed and traffic may make existing algorithms to become a performance bottleneck. This, necessitating the development of a faster and more efficient pattern matching algorithm in order to overcome the troubles on the network performance. A general pattern recognition system is shown in Figure 2.5.

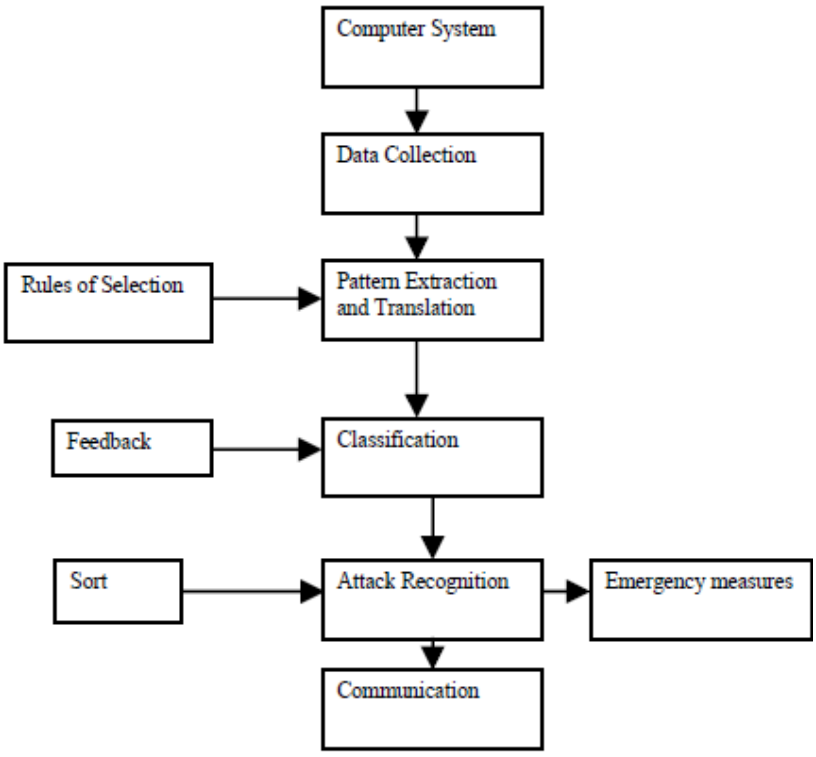

Figure 5. Block diagram of the general pattern recognition system [10]

Some of the identified Pattern recognition methods developed for many years in numerous applications in different fields includes: statistical pattern recognition, data clustering, fuzzy set, artificial neural networks, structural pattern recognition, Support Vector Machine (SVM), approximate reasoning approach to pattern recognition, and a logical combinatorial approach to Pattern Recognition. A representative sample of works on neural networks viz-viz computer network security was also studied.

III. METHODOLOGY

The work uses an artificial neural network which is the powerful feed-forward neural networks trained using Back-propagation algorithm. In this approach, a neural network is trained with back-propagation algorithm to store the userIDs (samples) and the corresponding encrypted passwords on the computer network switch. In this case, the system stores the weights of the trained neural network. The proposed system has the following learning rule:

- **Supervised learning:** In supervised learning, or learning with a "teacher," the network is provided with a correct answer

(output) for every input pattern. Weights are determined to allow the network to produce answers as close as possible to the known correct answers.

- **Reinforcement learning:** (i.e. learning with limited feedback) is a variant of supervised learning in which the network is provided with only a critique on the correctness of network outputs, not the correct answers themselves.
- **Unsupervised learning:** (i.e. learning with limited feedback) unsupervised learning, or learning without a teacher, does not require a correct answer associated with each input pattern in the training dataset. It explores the underlying structure in the data, or correlations between patterns in the data, and organizes patterns into categories from these correlations.

The ability to learn is a fundamental trait of intelligence. Although a precise definition of learning is difficult to formulate, a learning process in the ANN context can be viewed as the problem of updating network architecture and connection weights so that a network can efficiently perform a specific task. The network usually must learn the connection weights from available training patterns. Performance is improved over time by iteratively updating the weights in the network. ANNs' ability to automatically learn from examples makes them attractive and exciting. Instead of following a set of rules specified by human experts, ANNs appear to learn underlying rules like input-output relationships) from the given collection of representative examples. This is one of the major advantages of neural networks over traditional expert systems.

To understand or design a learning process it must first have a model of the environment in which a neural network operates, that is, it must know what information is available to the network. It refers to this model as a learning paradigm.

IV.SYSTEM ANALYSIS AND DESIGN

Basically, back propagation is a common method of training artificial neural networks used in conjunction with an optimization method such as gradient descent. The method calculates the gradient of a loss function with respects to all the weights in the network. The gradient is fed to the optimization method which in turn uses it to update the weights, in an attempt to minimize the loss function. This requires a known, desired output for each input value in order to calculate the loss function gradient (user samples). It is therefore usually considered to be a supervised learning method and it is a generalization of the delta rule to multi-layered feed forward networks, made possible by using the chain rule to iteratively compute gradients for each layer. This works and requires that the activation function used by the artificial neurons (or switch "nodes") be differentiable. This back propagation learning algorithm is divided into two phases: propagation and weight update.

Phase 1: Propagation

Each propagation involves the following steps:

1. Forward propagation of a training pattern's input through the neural network in order to generate the propagation's output activations.
2. Backward propagation of the propagation's output activations through the neural network using the training pattern target in order to generate the deltas of all output and hidden neurons.

Phase 2: Weight update

For each weight-synapse the following steps are taken:

1. Multiply its output delta and input activation to get the gradient of the weight.
2. Subtract a ratio (percentage) of the gradient from the weight.

This ratio (percentage) influences the speed and quality of learning; it is called the learning rate. The greater the ratio, the faster the neuron trains; the lower the ratio, the more accurate the training is. The sign of the gradient of a weight indicates where the error is increasing; this is why the weight must be updated in the opposite direction.

Repeat phase 1 and 2 until the performance of the network is satisfactory. Consider Algorithm for a 3-layer network (only one hidden layer):

Initialize network weights (often small random values)

Do

for Each *training example ex*

Prediction = neural-net-output (network, ex) // forward pass

Actual = teacher-output (ex)

Compute error (prediction - actual) at the output units

Compute for all weights from hidden layer to output layer // backward pass

Compute for all weights from input layer to hidden layer // backward pass continued

Update network weights

***Until** all examples classified correctly or another stopping criterion satisfied*

***Return** the network*

As shown, the samples errors (network issues) propagate backwards from the output nodes to the input nodes. This calculates the gradient of the error of the network regarding the network's modifiable weights. This entire procedure encompasses both the calculation of the gradient and its use in stochastic gradient descent. It furthermore, allows quick convergence on satisfactory local minima for error in the kind of networks to which it is suited.

Recall that back propagation networks are multilayer perceptrons (usually with one input, one hidden, and one output layer). In order for the hidden layer to serve any useful function, multilayer networks must have non-linear activation functions for the multiple layers: a multilayer network using only linear activation functions is equivalent to some single layer, linear network. Let's consider the more functional algorithm below

1. *Initialize the weights to small random values*
2. *Randomly choose an input pattern X(α)*
3. *Propagate the signal forward through the network*
4. *Compute δ_i^l in the output layer ($0_l=y_i^l$)*

   $\delta_i^l=g^l(h_i^l)\{0^{i+j}-y_i^l\}$

   where h_i^l represents the net input to the i^{th} unit in the i^{th} layer, and g' is the derivative of the activation function g
5. *Compute the deltas for the preceding layers by propagating the errors backward;*

   $\delta_l{}'=g'(h_i^l)\Sigma w_0^{i+j}\ \ \delta_i^{l+I}$

   for all I =(t-1),.....,1
6. *Update weights using*

   $\Delta w_j = \eta\delta_i^j\ y_j^{j-1}$
7. *Go to step2 and repeat for the next pattern until the error in the output layer is below a prespecified threshold or a maximum number of iteration is reached.*

V. Result

During the training process, the weights (user workloads or end users) are adjusted in order to make the actual outputs (predicated) close to the target (measured) outputs of the network. In this work, 8000 data samples (traffic density) were used for 23 input sources with 7 hidden layers in the training.

The next step was to test the performance of the developed switch model. At this stage, unseen reference data are exposed to the switch model. For the case study, the packets data generated from the input sources are used for testing the NN switch model. Afterwards, throughput, stability and delay plots are obtained.

In order to evaluate the performance of the developed NN switch model for computer network quantitatively and verify whether there is any underlying trend in its performance, statistical analysis involving the coefficient of determination *(R),* the Root Mean Square Error (RMSE), are conducted and captured in the model. RMSE provides information on the short term performance which is a measure of the variation of predicated values around the measured data.

VI. Conclusion

The neural network showed that after training the artificial neural networks, it can be used effectively as a security function. Essentially, the neural network in this work is a massively parallel-distributed processor made up from simple processing units, which has a natural propensity for storing experiential knowledge and making it available for use. The use of neural network offers the Input-Output Mapping property and capability. The ANNs learning algorithms were considered more particularly in two main groups, viz: Supervised (or Associative learning) and unsupervised (Self-Organization) learning. Supervised learning learns based on the target value or the desired outputs. During training the network tries to match the outputs with the desired target values. It is presented with an example picked at random from the set and the synaptic weights of the network are modified to minimize the difference between the desired response and the actual response of the network produced by the input signal in accordance with an appropriate statistical criterion. The training of the network is repeated for many times in the set until the network reaches a steady state, where there are no further significant changes in the synaptic weights. This by defaults maps the security of the connected sample inputs.

The previously applied training example may be re-applied during the training session but in a difference order. Thus the network learns from the examples by constructing an input-output mapping for the problem at hand. Unsupervised learning method is not given any target value. A desired output of the network is unknown.

During training the network performs some kind of data compression such as dimensionality reduction or clustering. The network learns the distribution of patterns and makes a classification of that pattern where, similar patterns are assigned to the same output cluster. The Kohonen Self-Organizing Map (SOM) network was shown to be the best example of unsupervised learning network. SOM has been used to provide a graphical representation of the analysis, highlighting outliers that may suggest suspicious activity. In our cryptography process, a feed-forward network is used in implementing the back propagation algorithm.

References

[1] Bhavya Daya, "Network Security: History, Importance, and Future",

http://web.mit.edu/~bdaya/www/Network%20Security.pdf.

[2] Behrouz A. Forouzan, and Sophia Chung Fegan "Data Communications and Networking"

4th Edition McGraw-Hill of the Americas, New York

[3]. H. S. Kim, J. M. Lee, T. Park, W. H. Kwon, "Design of networks for distributed digital control systems in nuclear power plants," Intl. Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies (NPIC&HMIT 2000), Washington, DC, November 2000.

[4]. J. P. Anderson, Computer security threat monitoring and surveillance, Technical report,James P. Anderson Co, 1980.

[5]. S. Zhong, T. Khoshgoftaar, N. Seliya, "Clustering-based network intrusion detection",Intl. Journal of Reliability, Quality and Safety, Vol. 14, pp. 169-187, No. 2, 2007.

[6]. G. Stein, B. Chen, A. S. Wu, K. A. Hua,"Decision Tree Classifier For Network

Intrusion Detection With GA-based Feature Selection", Proceedings of the 43rd ACM Southeast Conference, Kennesaw, GA, March 2005.

[7]. ASN Chakravarthy, P S Avadhani, "A Probabilistic Approach for Authenticating Text Or Graphical Passwords Using Back Propagation", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.5, May 2011

[8].Deepika P Vinchurkar, Alpa Reshamwala, "A Review of Intrusion Detection System Using Neural Network and Machine Learning Technique", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, November 2012, pp.54-63

[9]. Iftikhar Ahmad, Azween B Abdullah, Abdullah S Alghamdi, "Application of Artificial Neural Network in Detection of Probing Attacks",IEEE Symposium on Industrial Electronics and Applications (ISIEA 2009), October 4-6, 2009, Kuala Lumpur, Malaysia

[10]. Preet Inder Singh, Gour Sundar Mitra Thakur, "Enhanced Password Based Security System Based on User Behavior using Neural Networks", I.J. Information Engineering and Electronic Business, 2012, 2, Pp.29-35

[11]. Álvaro Herrero, Emilio Corchado, María A. Pellicer, and Ajith Abraham, "Hybrid Multi Agent-Neural Network Intrusion Detection with Mobile Visualization", Innovations inHybrid Intelligent Systems, ASC 44, pp. 320–328, 2007.

[12]. V. K. Pachghare, Parag Kulkarni, "Network Security Based On Pattern Matching: An Overview", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, October 2008.