Neural Network based Intrusion Detection Systems

Sodiya A.S
Department of Computer Science,
Federal University of Agriculture,
Abeokuta, Nigeria

Ojesanmi O.A
Department of Computer Science,
Federal University of Agriculture,
Abeokuta, Nigeria

Akinola O.C
Department of Computer Science,
Federal University of Agriculture,
Abeokuta, Nigeria

Aborisade O.
Department of Computer Science,
Federal University of Agriculture, Abeokuta, Nigeria

ABSTRACT
Recent Intrusion Detection Systems (IDSs) which are used to monitor real-time attacks on computer and network systems are still faced with problems of low detection rate, high false positive, high false negative and alert flooding. This paper present a Neural Network-based approach that combined supervised and unsupervised learning techniques designed to correct some of these problems. The design is divided into two phases namely: Training and Detection. In the training phase, Multiple Self–Organizing Map algorithm (SOM) was constructed to capture a number of different input patterns, discover significant features in these patterns and learn how to classify input. Sigmoid Activation Function (SAF) was used to transform the input into a reasonable value (0, 1). The learning weights were randomly assigned in the range (-1, +1) to obtain the output consistent with the training. SAF was represented using a hyperbolic tangent in order to increase the learning speed and make learning efficient. Momentum and adaptive learning rates were introduced to significantly improve the performance of the back-propagation neural network. The trained lattice of neuron was used as input in the back propagation for the real-time monitoring and detection of intrusive activities. The design was implemented in Visual Basic.Net. An evaluation was carried out using Network Traffic data collected from Defence Advanced Research Projects Agency dataset consisting of normal and intrusive traffic. The training model was performed by means of Root Mean Square (RMS) error analysis using learning rate of 0.70, 4 input layers, 8 hidden layers and 2 output layers. The evaluation result of the new design showed a promising and improved technique when compared with the recent and best known related work.

Keywords
Intrusion, Detection, Attack, Neural network, Security,

1. INTRODUCTION
An intrusion attempt or intrusion can be defined as the potential possibility of a deliberate unauthorized attempt or action to access information, manipulate information or render a system unreliable or unusable [3,21]. Intrusion attempt or intrusion activity may come from external or internal. Its ultimate purpose is to violate a system's integrity, confidentiality and reliability. Intrusion detection system (IDS) is the hardware device or software system which is used in the intrusion detection process to monitor network and host activities including data flows and information accesses etc. and detect suspicious activities. It serves three essential security functions: they monitor, detect, and respond to unauthorized activity by both internal intruders and external intruders. Intrusion detection systems use policies to define certain events that, if detected will issue an alert [1,4, 12, 13, 17].

Currently there are two major approaches to intrusion detection. The first approach, called anomaly detection or behavior detection, is to define and characterize correct static form and/or acceptable dynamic behavior of the system, and then to detect wrongful changes or wrongful behavior. The second approach is misuse detection or signature detection. More commonly known as signature detection, this approach uses specifically known patterns of unauthorized behavior to detect subsequent similar attempts. These specific patterns are called signatures. The misuse detection system monitors for those explicit patterns [2,16].

There are two basic types of intrusion detection based on the range of its detection: host-based and network-based [15] while [19] classified intrusion detection into three including Vulnerability-Assessment i.e Vulnerable attacks are to detect on internal networks and firewalls as the third attack. Each has a distinct approach to monitoring and securing data, and each has distinct advantages and disadvantages, host-based IDSs examine data held on individual computers that serve as hosts, while network-based IDSs examine data exchanged between computers. Both differ significantly from each other, but complement one another well. The network architecture of host-based is agent-based, which means that a software agent resides on each of the hosts that will be governed by the system.

Although network intrusion detection has its merits and certainly must be incorporated into a proper IDS solution, while host-based look more reliable bust always make use of NIDS to complete the defense.

2. LITERATURE REVIEW
Most research on intrusion detection focuses on anomaly detection because its strength in intrusion detection lies in anomaly detection, where the system does not need to depend on a signature before it can detect an attack. There are increases in the use of Neural Network in IDS in the recent times. [18] proposes a multi-level hybrid intrusion detection method that uses a combination of supervised, unsupervised and outlier based methods for improving the efficiency of detection of new and old attacks. This proposed method detecting rare category attacks as well as large-scale attacks of both new and existing attacks when tested with several benchmark and real-life intrusion datasets but still need to create a more effective ensemble approach based on faster and efficient classifiers so as to make a significant contribution in the study of the intrusion detection. [14] developed a hybrid IDS that uses semi supervised method shows better accuracy and reduced false alarm rate. Through this approach the overwhelming problem of using supervised and unsupervised method were be solved this approach has to be done regarding detection of on DOS attacks and corresponding intrusion prevention system must be designed with all necessary security measures. [23] proposed a multi-layer intrusion

detection model to achieve high efficiency and improve the detection and classification rate accuracy. Also the proposed model was improved the detection rate for known and unknown attacks by training the hybrid model on the known intrusion data. Then the model applied for unknown attacks by introducing new types of attacks that are never seen by the training module. [6] proposed hybrid method based neural network algorithm was proposed for speech recognition. The proposed method combines Self-Organizing Map (SOM) which known as unsupervised network and Multilayer Perceptron (MLP) which known as supervised network for Malay speech recognition. [5] applied SOM for a visual approach to analyze network data to support the decision process of a human expert in the field of intrusion detection. A SOM is trained with an unsupervised training algorithm and no prior knowledge of the data being analyzed is needed. The intrusion detection system presented is not able to make classifications but he emphasized that the integration of a human expert allows to detect new sophisticated and structured attacks. [11] used hierarchical back propagation neural network to detect TCP SYN flooding and port scanning intrusions. There is also a combinational approach using back propagation and expert system for an IDS. Nevertheless, visualizing together with classifying intrusion data has not been introduced in any network IDS. [9] worked on the combination of two different approaches to intrusion detection using signature-based systems and anomaly-based system , the approaches was feasible and advantageous when producing NIDS , implementation required minimal system resources and produces high detection rate, but it has no ability to resist attack itself and its dependence on third party software , which apart from the inconvenience, possible problems could result from differences in output between different versions and a possible lack of availability in the future. [7] proposed hybrid model of the SOM and the MLP, in that work, the self-organizing map was combined with the feed-forward neural network. This model was designed to detect the dispersing and possibly collaborative attacks. [25] shown in figure 1.

used a combination of RBF Networks and SOM in the IDS for easy extension so as to automatically adapt to classification results of an human expert without complete re-training, this experiment resulted in very high detection rate but high false rate alarm too. [20] used supervised artificial neural networks to also increase the efficiency further on a network. He later conclude that the same experiments should also be conducted with other types of neural networks to see if these types can improve the detection rate got from the experiments with a back propagation neural network. But the system is still an experimental framework also due to the lack of training examples; the efficacy of the model machine-learning algorithm on other datasets has not been tested. [24] combined the strategy of data mining and expert system to improved detection efficiency by reducing false positive and false negative. This model reduced considerably false alarm but the model suffers from lack of flexibility in the rule-to-audit record representation. Slight variation in an attack sequence can affect the activity rule comparison to a degree that the attack is not detected by the intrusion detection mechanism. In addition, it has no capability for autonomous learning; they require frequent updates by the system administrator.

3. SYSTEM MODEL

3.1 Artificial Neural Network Based IDS Model

This model is split into **sensor**, which gathers information from an information source, and a **detector**, which performs the analysis. The model consists of several sensors and several detectors. For instance, in real life scenario it collects information from several sources that are then analyzed by a single detector. It consists of a detector that recognized known intrusion, learns new types of intrusions, and takes actions based on events that occur, raising an alarm if necessary as

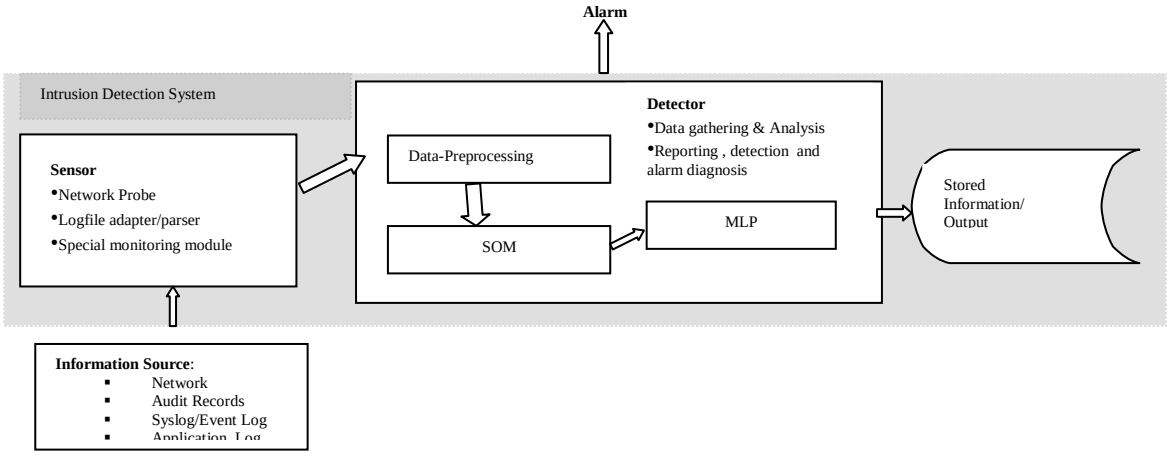

Figure 1: Artificial Neural Network Based IDS Model

- **Sensors:** In this model, sensors are systems that transform the information provided by an information source into a form suitable for further analysis by the detector. Sensors used here are very simple and just provide some basic parsing of the data supplied by the information source and by investigating the diagnostic output the detector generates along with the alarms.

- **Detectors:** The model employs a multiple unsupervised Neural Network – Self Organizing Maps (SOM) – to analyze and reporting the characteristics of a common connection i.e. data analysis and data gathering, which is of particular interest here on account of their efficient update scheme and ability to express topological relationships. This property of an SOM makes it very convenient for expressing relationships between different

groups of connections. While supervised artificial neural network is used for system detection that recognized anomalies, raised alarm and reporting.

- Processing: Sensor, Detectors and Knowledge based of Known Intrusion formed the processing block, which is the heart of the intrusion detection system. It is here that one or many algorithms are executed to find evidence (with some degree of certainty) in the audit trail of suspicious behaviour.
- Alarm: This part of the system handles all output from the system, whether it be an automated response to suspicious activity, or more commonly the notification of a Site Security Officer.
- A three-layer perceptron was designed with k input nodes, 2k hidden nodes and 2 outputs (intrusion and non-intrusion). Input layer with four neurons (input states) were used i.e. detection k = 4 as shown in figure 2.

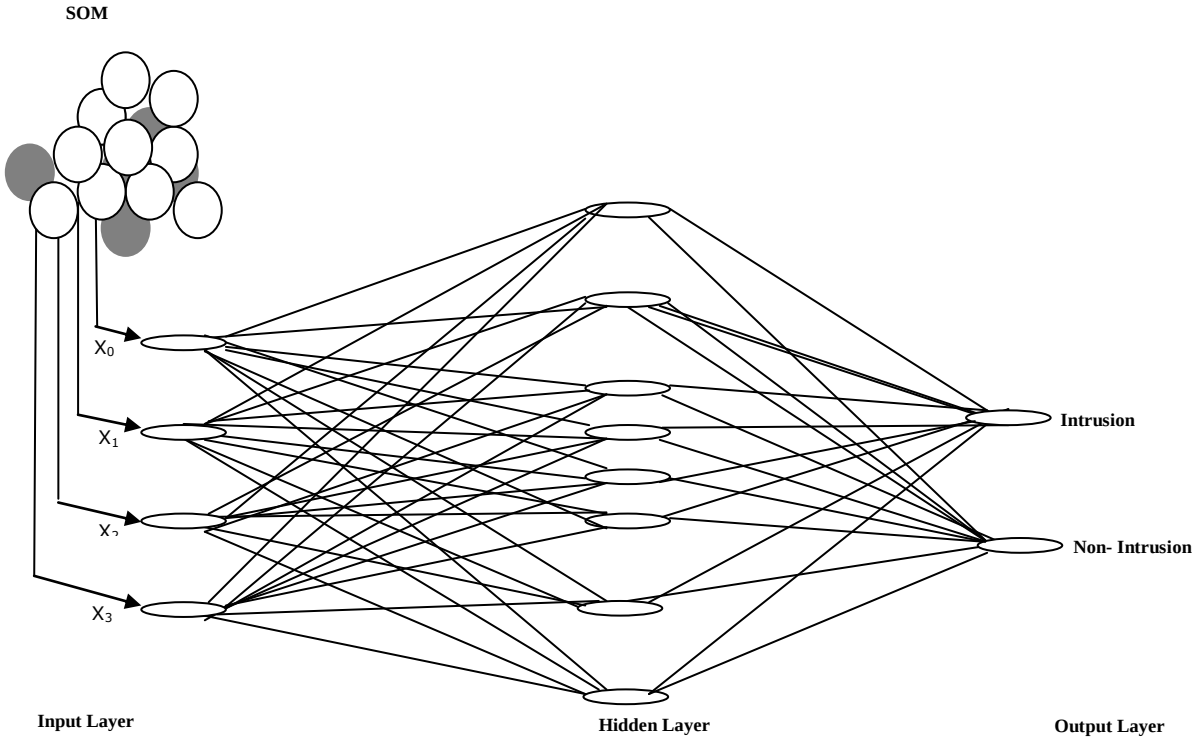

Figure 2: The Neural Network Strategy

3.2 Mathematical Model

In this design, we focus on detection of network attacks, we present methodology for both visualizing intrusion by using the Multiple Self-Organizing Map and classifying intrusions using Back-Propagation Neural Network. We gather major beneficial characteristics of both neural Network models into our hybrids IDS, consisting of both unsupervised and supervised learning algorithm. The training phase of SOM, are described as follows:

(1) Select a k-dimensional input x from the training data set and feed it parallel to all the neurons in the lattice. Each neuron determines its distance from the input data point in the k-dimensional input space. The criterion used for determining the winner neuron is the Euclidean distance. For K-dimensional space, the Euclidean distance between two points $X(x_1, x_2, \ldots, x_k)$ and $Y(y_1,y_2, \ldots, y_k)$ is given as follows:

$$\sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \ldots + (x_k - y_k)^2} \quad (1)$$

The neuron that has the smallest Euclidean distance from the input data point is declare as "winner ". Dot-product can also be used. For k-dimensional space, the dot product for two vectors $X(x_1, x_2, \ldots, x_k)$ and $Y(y_1,y_2, \ldots, y_k)$ is given as follows:

$$x_1 \cdot y_1 + x_2 \cdot y_2 + \ldots + x_k \cdot y_k \quad (2)$$

However, in this case the neuron with the maximum dot product is considered as winner.

(2) After the winner has been determined, the weight vectors of the winner and neighboring neuron are adjusted according to following learning function:

$$m_i(t+1) = \begin{cases} (m_i(t) + h_d(t)\,[x(i) - m_i(t)]) & \text{for each } i \in N_c(t) \\ m_i(t) \end{cases} \quad (3)$$

where,

t is an integer that represents discrete time co-ordinate . t is incremented by 1 for during every iteration of the training process.

$N_c(t)$ represents the neighbourhood radius during iteration t of the training process.

X(t) represent the input vector chosen during iteration t of the process.

$m_i\ (t)$ *and* $m_i\ (t+1)$ represent the vector measures of the neurons at distance i from the winner, during iterations t and t+1 respectively.

$h_{ci}(t)$ represents the neighborhood function $h_{ci}(t) = h\ (||r_c\ ,r_i\ ||\ ,t)$. Here $\boldsymbol{r_c}$ and $\boldsymbol{r_i}$ are the locations of the winner and the neuron *i* in the lattice.

There are two commonly used neighborhood function: bubble and Gaussian. We used Gaussian, which allow the adjusted factor vary as a bell-shaped Gaussian function. The winner neuron gets adjusted by the maximum amount, with the adjustment factor for the neighboring neurons decreasing with increase in distance from the winner neuron. The Gaussian function is specified as follow:

$$H_d(t) = \alpha(t)\ \exp\left(\frac{||(r_c, r1||)^2}{2\sigma^2(t)}\right) \qquad (4)$$

where $\boldsymbol{\sigma(t)}$ specifies the neighborhood radius.

(3) Repeat steps 1 and 2 until the training is complete. The number of the steps needs to be determined prior to the beginning of the training phase as the rate of convergence of the neighborhood function and the learning rate are calculated accordingly.

In this hybrid scheme, output weight information from SOM is fed into the Back Propagation network, as shown below.

The detection phases of Backpropagation are stated below:

The objective of Backpropagation in this work is to detect an intrusion. Mathematically, $\vec{Z} = f(\vec{x})$. each target vector is a function, f of the input vector. The task of the BP is to learn the function of f. This is achieved by finding regularities in the input patterns that correspond to regularities in the output patterns. The network has a weight parameter vector, whose values are changed to modify a function f computed by the network to be as close as possible to f. Given the input vector $X = x_1, x_2, \ldots, x_z$, the output from the hidden node will be as follows:

$$Y_j = g(u) = g\left(a_{oj} + \sum_{j=1}^{N} a_i x_i\right) \qquad (5)$$

where j = 1, 2,….$\mathbf{N_{input}}$ and $\mathbf{a_{ij}}$ is the weight of the $\mathbf{i^{th}}$ node for the $\mathbf{j^{th}}$ input . The output of the output node be calculated as follows.

$$Z_k = g\left(b_{ok} + \sum_{j=1}^{N} b_{jk} y_j\right) \qquad (6)$$

where $\mathbf{k = 1, 2, \ldots\ldots N_{output}}$ and $b_{jk}$is the weight of the $\mathbf{j^{th}}$ node for the $\mathbf{k^{th}}$ output . The transfer function mostly used a sigmoid or a logistic function gives the value in the range of [0,1]and can be described as

$$g(u) = \frac{1}{1+e^{-u}} \qquad (7)$$

The mean square error is the way of measuring the fit of the data and is calculated as :

$$E = \frac{\sum_{n-1}^{N}\sum_{k+1}^{K}(Z_{kn} - t_{kn})^2}{2NK} \qquad (8)$$

Where N is the no of examples in the data set K is the no of output of the network. Z_{kn} is the k^{th} actual output for the n^{th} example and t^{kn} is the k target output for the n^{th} example.

3.3 Measuring the Efficiency of the IDS

This study presents new insight into the Artificial Neural Network to detect Intrusion Detection. The Project provides the ability for the supposed administrator to train the network and trigger the execution of the IDS monitoring module. When intrusion is detected by the IDS, the appropriate alarm is raised and the administrator alerted of the event. When an intrusion is detected by the IDS, the IDS alert the administrator of the intrusion and ask the administrator if it should allow the supposed intruder to continue with his operations. If the administrator allows it due to the fact that it was a false alarm, then the IDS would lean from the event, but if otherwise, the user system is shut down and the user preempted from operation

- **Determination of detection rate:**

an instance of anomaly identified as normal, is a case of missed detection.

N_{attack} : the total number of attacks in the test set

N_{missed}: the number of missed instances

$\%Detected = (N_{attack} - N_{missed}) / N_{attack} * 100$

- **Determination of false positive rate:**

An instance of normal record falsely identified, as anomaly is a false positive.

N_{normal} : number of normal records in the test set

N_{false}: total number of false positives

$\%FalsePositive = (N_{false} / N_{normal}) * 100$

The efficiency of this model was measured by the numbers of false alarm it produces. A false positive is produce if the IDS claim there has been an intrusion, when there was not. As explained earlier, false positives are normal traffic that are classified as attacks.

3.4 Interface Design

The front-end design presents a pop up menu that has different options that assist for the purpose for the experiment. Users can then navigate through the menu. On loading the program, figures 9, 10, 11, 12 below presents the Training and Detecting screen of the IDS.

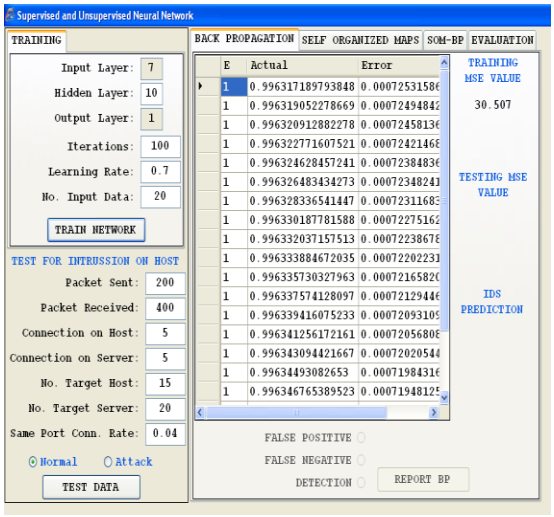

Figure 9: Back Propagation Result

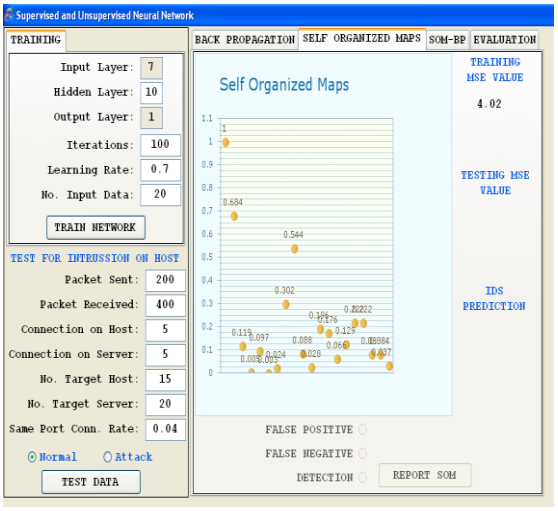

Figure 10: Self Organized Map Result

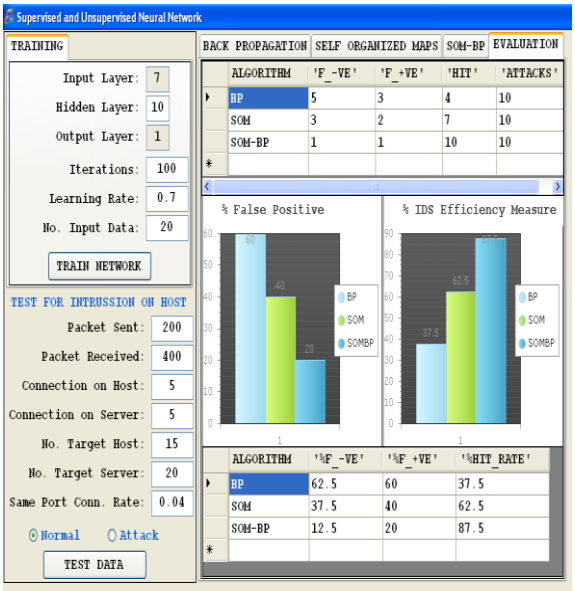

Figure 11: Hybrid Algorithm (Multiple SOM and Back Propagation Result) Three Algorithm

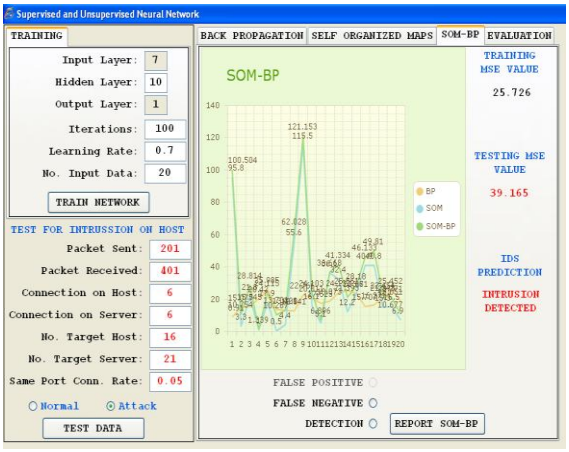

Figure 12: Visualizing Alert and Efficiency of Three Algorithm

4. CONCLUSION

In this paper, we have proposed a new way to handle Computer Security using combined self-organizing map and multilayer perceptron for Intrusion Detection System. The feature map was trained by Kohonen's self organization algorithm which simplified the feature vectors by converting them into fixed dimension of binary matrix. The SOM was able to perform good mapping for the MLP in classification task. We compared out system with a recent research and the experimental results showed that our proposed algorithm improve the detection accuracy of about 4%. The simulation results, as shown in figures below achieve more than 96 % detection rate and less than 3 % false alarm rate. For a previous work the detection rate is was 0.95, while this project work is 0.965. The difference seems small, but in the field of Intrusion Detection even one single successful attack can threaten the security of a whole network.

5. REFERENCE

[1] Alsharafat W. (2013), "Applying Artificial Neural Network and eXtended Classifier System for Network Intrusion Detection", The International Arab Journal of Information Technology, Vol. 10, No. 3, pp. 230-238.

[2] Bhavin S. and Bhushan H. T. (2012), "Artificial Neural Network based Intrusion Detection System: A Survey", *International Journal of Computer Applications* 39(6):13-18.

[3] Chaivat Jirapummin, Naruemon, Wattanapongsakorn and Prasert Kanthamanon (2000), "Hybrid Neural Networks for Intrusion Detection System", Department of Computer Engineering, Faculty of Engineering, King Mongkut's University of Technology Thonburi, Bangkok , Thailand.

[4] Devikrishna K. S. and Ramakrishna B. B. (2013), An Artificial Neural Network based Intrusion Detection System and Classification of Attacks, International Journal of Engineering Research and Applications (IJERA) ,Vol. 3, Issue 4, pp. 1959-1964 1959, ISSN: 2248-9622.

[5] Girardin L, "An eye for Network Intruder-Administator Shootouts," *Proc. of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring*, 1999 Comparison of Supervised Neural Network in Intrusion Detection.
http://ailab.das.ucdavis.edu/papers/vu02nn.pdf

[6] Goh Kia Eng, and Abdul Manan Ahmad (2005) " Malay Speech Recognition using Self-Organizing Map and Multilayer Perceptron", *Proceedings of the Postgraduate Annual Research Seminar, pp. 233-237.*

[7] John Zhong, Lei and Ali Ghorbani (2004) "Network Intrusion Detection Using an Improved Competitive Learning Neural Network" in Proceedings of the 2nd Annual Conference on Communication Networks and Services Research (CNSR 2004), Canada. IEEE Computer Society, ISBN 0-7695-2096-0 pp. 190-197.

[8] Jun Li, Gerhard Eschelbeck , "Multi-Tiered Intrusion Detection System" *http://fmg-www.cs.ucla.edu/ficus-members/lijun/pubs/TR010027.pdf*

[9] Kaleton Internet (2002)"Combination of Misuse and Anomaly. Network Intrusion Detection Systems", March 2002. Kaleton Internet. Dept. 5364 Suite 145. 269/2 Soi Potisarn Moo 6. Naklua Banglamung. Chonburi 20150. Thailand. http://www.kaleton.com/research/kaletonidspaper.pdf

[10] Kohonen. T (2001.) "Self-Organizing Maps", 3rd extended ed, ser. Information Sciences, Berlin, Germany: Springer, vol. 30

[11] Lee W , Stolfo S, and Mok K (1999) "A data mining framework for building intrusion detection models", In *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, California.

[12] Lee W , Stolfo S, and Mok K (2002) The Third International Discovery and Data Mining Tools Competition.[online], *http://kdd.ics.uci.edu/database/kddCup99/kddCup99.html*

[13] Mohammad S. A. and Abu N. B. (2012)," An Implementation of Intrusion Detection System using Genetic Algorithm ", International Journal of Network Security & Its Applications (IJNSA), Vol. 4, No. 2, March 2012.

[14] Mostaque M. H. (2013), Current Studies on Intrusion Detection System, Genetic Algorithm and Fuzzy Logic, International Journal of Distributed and Parallel Systems (IJDPS) Vol.4, No.2, pp.35-47.

[15] Nadiammai G.V. ,Hemalatha M. (2013) , " Handling Intrusion Detection System using Snort Based Statistical Algorithm and Semi-supervised Approach "Research Journal of Applied Sciences, Engineering and Technology 6(16): 2914-2922, ISSN: 2040-7459

[16] Northcut S and Novak J, "Network Intrusion Detection", 3rd ed. Indianapolis, IN: New Riders Publishing, 2002.

[17] Parveen K. and Nitin G. (2014), A Hybrid Intrusion Detection System Using Genetic-Neural Network, *International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 , pp. 59-63.*

[18] Peter Lichodzijewski, A.Nur Zincir, Heywood (2003) "Dynamic Intrusion Detection using Self-Organizing Maps", Faculty of Comp. Science Dalhousie University Halifax, *NS http://cs.stmarys.ca/~jmac/482-2005/CITSS-2k2.pdf*

[19] Pingchuan Ma (2003), "Log Analysis-Based Intrusion Detection via Unsupervised Learning", Master of Science, School of Informatics, University of Edinburgh Steve Lawrence

[20] Prasanta Gogoi1, D.K. Bhattacharyya1, B. Borah1 and Jugal K. Kalita. (2013), "MLH-IDS: A Multi-Level Hybrid Intrusion Detection Method", The Computer Journal, 57(4), pp. 602-623

[21] Reddy E.K. (2013), Neural Networks for Intrusion Detection and Its Applications, Proceedings of the World Congress on Engineering 2013 Vol II, WCE 2013, July 3 - 5, London, U.K.

[22] Robert Birkely. (June 2003) " A Neural Network Based Intelligent Intrusion System "*http://www.rbirkely.com/cv/intelligent_intrusion_detection_system.pdf*

[23] Sarasamma S, Zhu Q, Huff J, "Hierarchical Kohonen Net for Anomaly Detection in Network Security", IEEE Transactions on Systems, Man and Cybernetics - part B, vol. 35, No. 2, 2005.

[24] Shah A. T., Jagtap S. S., Kakade P. P., Tekawade N. B., and Daflapurkar P. M. (2014), "A Real-Time Intrusion Detection System using Artificial Neural Networks (ANN)", International Journal of Emerging Technology and Advanced Engineering, Vol. 4, Issue 3, pp. 756-759. (ISSN 2250-2459)

[25] Sherif M.B. (2013), "Implementation of Intelligent Multi-Layer Intrusion Detection Systems (IMLIDS)", International Journal of Computer Applications, 61(4):41-49.

[26] Sodiya A.S, Longe H.O.D and Akinwale A.T. (2004). "A new two tiered strategy to intrusion Detection", *Emerald Information Management and Computer Security*. vol. 13, No 5 http://www.emeraldinsight.com/09685227.htm

[27] Timo H. (2003) "Intrusion Detection with Neural Networks { Combination of Self-Organizing Maps and Radial Basis Function Networks for Human Expert Integration}" . *http://www.ieee-nns.org/files/EAC_Research_2003_Report_Horeis.pdf*

[28] Va N.P.Dao, Rao Vemuri (2002)" A Performance Comparison of Different Back Propagation Neural Networks Methods in Computer Network" http://www.cs.ucdavis.edu/~vemuri/papers/bp-intrusion%20detection.pdf

[29] Vu Dao (2002) "Computer Network Intrusion Detection Via Neural Networks Method"