Performance Analysis of Some Neural Network Algorithms using NSL-KDD Dataset

Jamal Hussain[1] Aishwarya Mishra[2]

Professor, Dept. of Mathematics and Computer Science, Mizoram University, Aizawl, India

Research Scholar, Dept. of Mathematics and Computer Science, Mizoram University, Aizawl, India

Abstract *- Consequent upon the growth of Internet and multifarious technologies including smart devices and their massive use and operations on Internet platform not only caused serious threats on security but also abnormal traffic detection. A number of assorted attacks on Internet seriously affect the systems. This not only leads to deteriorate the performance in the computer but also malfunctioning of the system. Vast growth of data in various areas due to adoption of computer technologies precipitated to anomalies. Thus, in such an alarming situation, anomalous traffic detection became a major concern of the security. Intrusion detection system is one of the redressed techniques that can be employed to determine the system security which detects the intrusion. In this paper performance of NSL-KDD dataset has been evaluated using LVQ, RBFN, DECR_RBFN, EVRBFN, MLP_BP, SONN networks of ANN showing the results that constitute binary class. Based on various performance measures analytical results were derived.*

Keywords: Neural Network, NSL-KDD, Intrusion Detection, Accuracy, LVQ, RBFN, DECR_RBFN, EVRBFN, MLP_BP, SONN

1. INTRODUCTION

Application of computer technology and its application in various sectors through networking sparked the society with the increased volume of intrusion. Intrusion reveals the sense of unwanted penetration to other systems in an inappropriate manner through a virtual mode for villainous activities. Hence, security of the system has become indispensable to protect from unwanted and wildcat entry from the intruders. Thus, intrusion detection remains as a judicious option to safeguard the system connected to public domain. Intrusion Detection System (IDS) functions as a system to detect intrusion not only in business sectors but also in educational sector. Hence, it is considered to be emerging area of research. It is a globally accepted technique that is employed to detect intrusion in data mining as in the present context; data mining methods have gained momentum in addressing network security issues [1]. Application of systems for various productive works on internet domain needs proper security to avoid unlawful activities by the hackers who, all the time use the brain for destructive purpose in a network environment. The system carries an in-built mechanism known as firewall to prevent such attacks in network security. In other words, firewall in the system acts as a filtering technique of the traffic. The hackers control over the system available in a network domain through malicious traffic in ports by using SMTP and HTTP which results to loss of data of the victims' system. Therefore, in such a grim situation, Intrusion Detection System becomes inevitable by installing IDS Sensors between firewall and LAN [2,3]. The primary function of IDS is not only to detect the unauthorised attacks but also alerts the system administrator [4]. Further, it is also associated with detection of intimidating actions especially in network environment.

IDS in a network environment are stimulated for detecting aggressive actions from external source. This, being concerned with the network security, is used for (i) anomaly detection and (ii) signature detection. It can be discussed that while, anomaly detection relates to abnormal function of the system, signature detection pertains to perceive the difference between anomaly or attack patterns identified as signatures [5].

To be more specific, Misuse or Signature based system primarily belongs to rule based detection where data from the audit logs are analysed for creating a rule or signature for the attack which is generally alerts through alarms. Further, the anomaly based system relates to determination of the abnormal behaviour which is ascertained through analysing the audit logs [6]. The operation of the IDS Sensor is explained in Fig. 1 below.

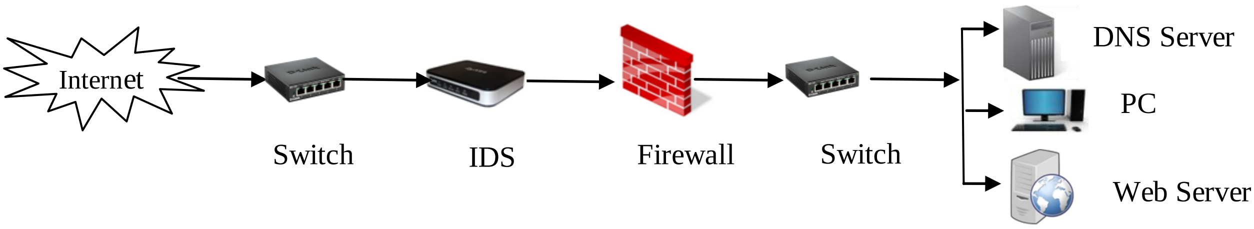


Fig:1 Operation of Intrusion Detection System
Source: Myers, M (2009). Managing and Trobleshooting Networks, 2nd Ed., New Delhi, McGraw Hil [30]

Sporadic attempts have been made by substantial researchers who have viewed the Intrusion Detection System in various angles. Some viewed that the anomaly detection is an important problem in the dynamic network domain, its learning including understanding and number of attacks are caused on computer due to increase in the speed of information data flow. The network threats and security raised a major issue with regards to the data integrity and loss of data. Their studies also focussed on Intrusion Detection System using different neural networks and machine learning techniques. Increase problems on web security and monitoring activities of the network and threats are the essential features of IDS that can be classified as Data and Model of intrusion and the researchers suggested for use of Support Vector Machine to specify the classifier construction problem [7, 8, 9, 10, 12, 13, 14, 15, 16, 24, 25].

In particular, Wang *et.al* (2013) in a study presented an intrusion detection system of hybrid neural network model based on Radial Basis Function (RBF) network and Elman network where, RBF network is a real-time pattern classifier, and Elman network achieves the memory ability for former event. [11]. Based on the hybrid model, intrusion detection system uses DARPA data set to do test evaluation. It uses ROC curve to display the test result intuitively. Further, Wang *et.al* (2010) argue for implementation of Artificial Neural Networks (ANNs) so as to improve the IDS performance of Intrusion Detection systems (IDS) compared to other traditional methods. The authors advised to follow general procedure of FC-ANN where fuzzy clustering technique is the first step that is used to generate different training subsets followed by the second step based on different training subsets, different ANN models to be trained to formulate different base models and the third and final step involves a meta-learner, fuzzy aggregation module which is employed to aggregate these results. Experimental results on the KDD CUP 99 dataset showed that the proposed new approach, FC-ANN, outperforms BPNN and other well-known methods such as decision tree, the naïve Bayes in terms of detection precision and detection stability[17]. Further, in particular Aneetha and Bose (2012) deduced that, Self-Organizing Map algorithm, which is a technique of ANN, is also used to surmount fixed architecture and random weight vector assignment of simple SOM. Distance threshold parameter is used to create new nodes. It also applies K-means clustering algorithm to group similar nodes [29].

II. DATASET DESCRIPTION

The Lincoln Laboratory of Massachusetts of Technology which incidentally happens to be a private research university in Cambridge happens to the pioneer institute to develop DARPA (Defence Advanced Research Projects Agency) Datasets in 1998, 1999 and 2000 where, data sets of 1998 & 1999 are the result of the DARPA Intrusion Detection Evaluation while, datasets of 2000 focus on Intrusion Detection Scenario-Specific [19]. Tavallaee *et. al* [20] observed that, the data captured in DARPA'98 Intrusion Detection System evaluation comprises 7 weeks of network traffic data (5 weeks for training purpose and 2 weeks for testing purpose) which can be processed into 5 million connection records each with 100 bytes. Mention may be made that, two weeks of test data constitute 2 million connection records approximately. KDD'99 dataset which originally hails from DARPA'98 dataset comprises around 4,900,000 single connection vectors where each 41 features constitute and labelled as normal or an attack with one specific attack type. The authors further proposed that, NSL-KDD, a refined and condensed dataset of original KDD'99 dataset constitutes same 41 features and one class attribute which is composed of 21 classes which are covered under four classes of attacks [6] such as, Probe, User to Root (U2R), Remote to Local (R2L) and Denial of Service (DoS). In this paper, the multi class NSL-KDD dataset is converted to binary class dataset by combining different types of anomalies. So, now there are two class *i.e.*, normal and anomaly. The four types of attacks as classified in NSL-KDD dataset are[31],

A) Denial of Service (DoS)

This is concerned with Denial of Service. It is also a type of attack where the hacker builds memory resources too busy to serve the legitimate networking requests and hence, denying users access to a machine. DoS attack initiate in three ways such as by,

(i) Abusing the computer's legitimate features

(ii) Targeting the implementation bugs

(iii) Exploiting the mis configuration of the systems

Further, the attacker provides different modes of services which are inaccessible by the authentic uses and based on the same, DoS attacks are classified. Examples of such attacks include, apache, smurf, Neptune, ping of death, back, mail bomb, UDP storm etc.

B) Remote to Local Attack (R2L)

It pertains to unauthorized access from a remote machine. Here, a user attacks a remotely located machine by sending the packets over the internet and the user does not have access to expose the machine vulnerabilities, and exploit privileges which a local user would have on the computer. Examples of such class fall as xlock, xnsloop, phf, sendmail, dictionary etc.

C) User to Root Attack (U2R)

It is associated with unauthorized access to local super user (root) privileges. Invariably, these types of attacks are the exploitations where the hacker commences on the system with a normal user account and efforts to abuse vulnerabilities in the system for gaining super user privileges. Examples, perl, Xtream etc.

D) Probe

It relates to surveillance and other probing in the class. Here, the hacker while scanning a machine or a networking device for determining weakness or vulnerabilities what may later to be exploited so as to compromise the system. This technique primarily is associated with data mining viz, satan, saint, portsweep, mscan, nmap etc.

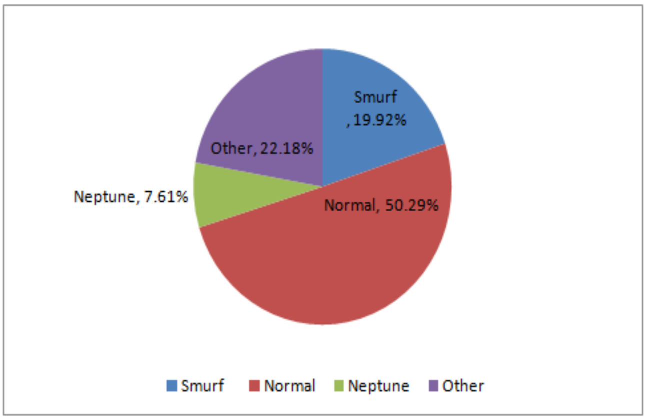
The four attack types with corresponding attack of each category in NSL-KDD dataset is discussed in Table-1.

Table-1: Attack types with corresponding attack name in NSL-KDD dataset

Attack Type	Attack Name
Denial of Sevice (DoS)	Back, land, Neptune, pod, smurf, teardrop
Remote to Local (R2L)	guess_passwd, ftp_write, imap, phf, multihop, warezmaster, spy
User to Root(U2R)	buffer_overflow, loadmodule, perl, rootkit
Probing	Satan, ipsweep, nmap,portsweep

III. DATA DISTRIBUTION IN KDD'99 DATASET

The KDD data set is a well known benchmark in the research of Intrusion Detection techniques. The KDD'99 dataset includes a huge number of repeated records of 78% and 75% redundant data on training and test dataset. The redundant dataset can harm the result of the evaluation to a much higher degree of detection accuracy. The data distribution of KDD'99 dataset is shown in Figure-2 below. Travallaee *et.al* (2009) viewed that, the necessary adjustment made on KDD'99 dataset results in a dataset known as NSL-KDD. Further, Mchugh (2000) observed that NSL-KDD is also not ideal as it restrains the evaluation result which is due to the use of synthetic simulation of normal with scripted anomaly.



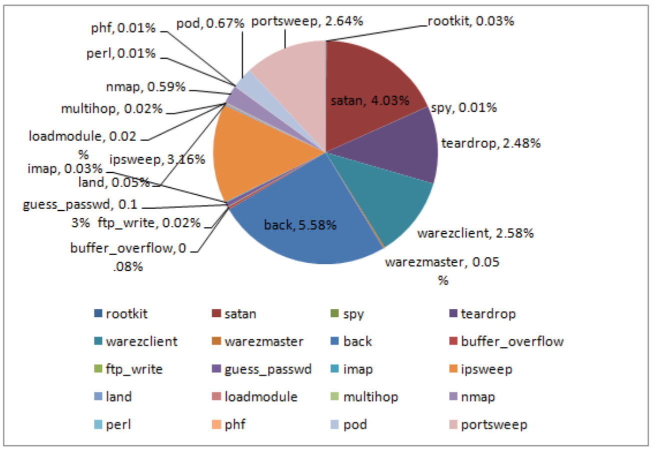


Fig:2 Data Distribution in KDD'99 dataset

IV. EXPERIMENTAL FRAMEWORK

In this experiment, NSL-KDD dataset is taken as input for the different classifiers *i.e.,* LVQ,RBFN,DECR-RBFN,EV-RBFN,MLP_BPandSONN[18,21,22,23]. Then different performance matrices are used to analyze the performance of the classifiers. The architecture of the proposed model is placed below in Fig.3.

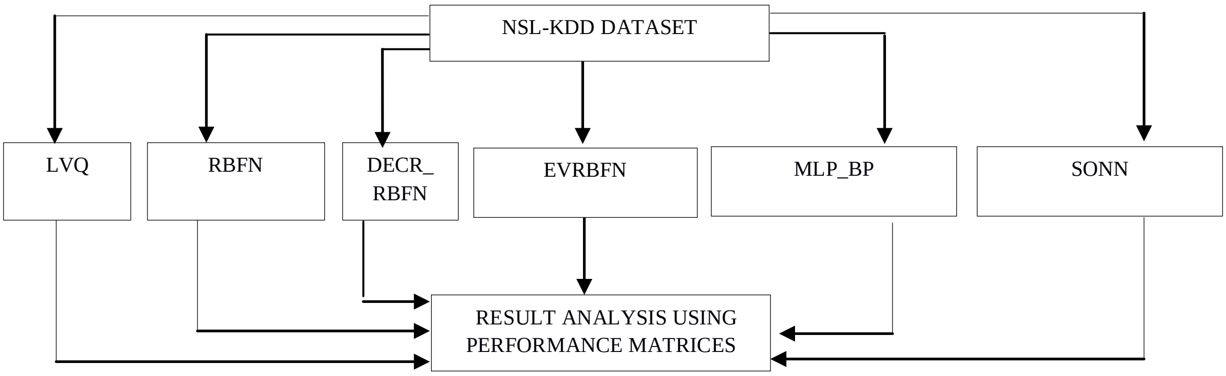


Fig. 3: Architecture of proposed model

V. EXPERIMENTAL RESULTS

The whole experiment is done by using KEEL software which is freely available at [http://sci2s.ugr.es /keel/ datasets.php]. The 10 fold cross validation method is used in this paper where one fold is kept for testing and others are for training. For the performance analysis, the performance metric (accuracy) is used by the help of the confusion matrix. There are different types of performance metrics [28] are used in this paper i.e.(1) Overall Accuracy, (2) Specificity (3) Sensitivity (4) G-Mean .The specificity is the proportion of the TN and (TN+FP) and with the higher specificity fewer positive cases are labelled as negatives, so this ratio can be regarded as the percentage of negative cases correctly classified as belonging to the negative class. The proportion of cases that are TP for all the cases that are positive in diagnostic test (TP+FN) is called sensitivity. The Geometric Mean (G-Mean) is another metric used to evaluate the performance results by using both specificity and sensitivity. It ranges from 0 to 1 and an attribute that is perfectly correlated to the class provides a value of 1.

$$OverallAccuracy(OA) = \frac{TP+}{TP+FP+} \quad (1)$$

$$Specificity = \frac{TN}{TN+FP} \quad (2)$$

$$Specificity = \frac{TN}{TN+FP} \quad (3)$$

$$G - Mean = \sqrt{Specificity * Sensitivity} \quad (4)$$

Where, TP = Total number of correctly classify positive examples

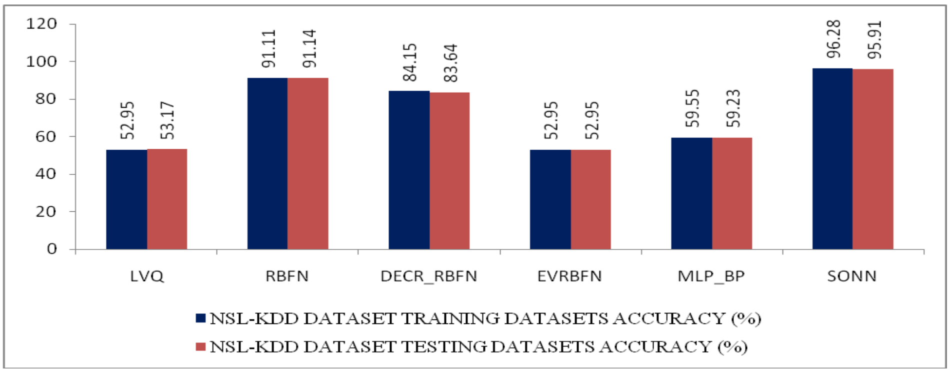
FP = Total number of miss-classified negative examples

TN = Total number of correctly classify negative examples

FN = Total number of miss-classified positive examples

Table 2: Results of different classification methods (Accuracy)

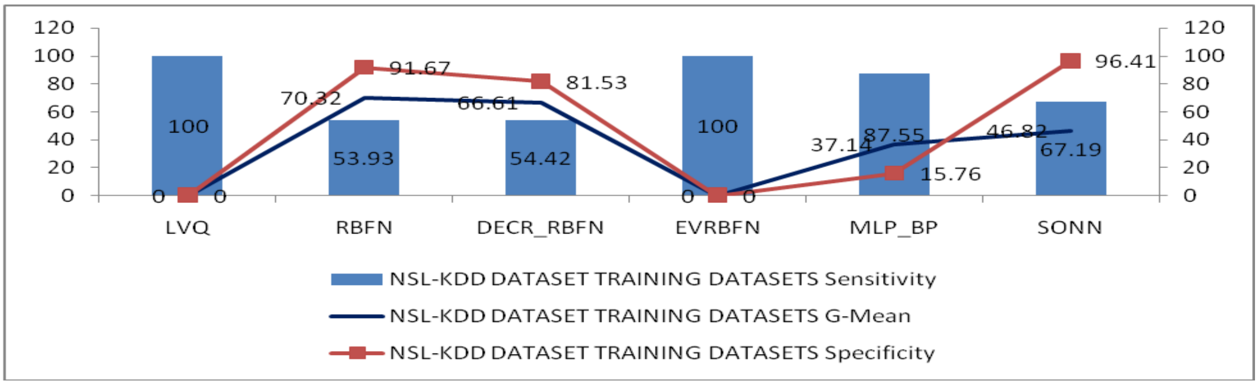
Classification Methods	NSL-KDD Training Dataset Accuracy (%)	NSL-KDD Test Dataset Accuracy (%)
LVQ	52.95	53.17
RBFN	91.11	91.14
DECR_RBFN	84.15	83.64
EVRBFN	52.95	52.95
MLP_BP	59.55	59.23
SONN	96.28	95.91



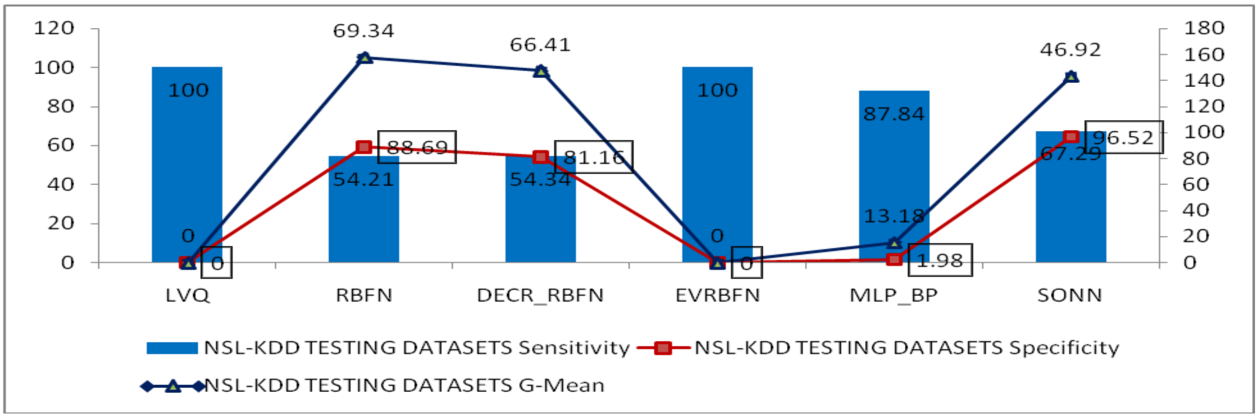
Graph-1: Results of different classification methods (Accuracy)

Table 3: Results of different classification methods (Sensitivity, Specificity, G-Mean)

Classification Methods	NSL-KDD Training datasets			NSL-KDD Test datasets		
	Sensitivity	Specificity	G-Mean	Sensitivity	Specificity	G-Mean
LVQ	100.00	00.00	00.00	100.00	00.00	00.00
RBFN	53.93	91.67	70.32	54.21	88.69	69.34
DECR_RBFN	54.42	81.53	66.61	54.34	81.16	66.41
EVRBFN	100.00	00.00	00.00	100.00	00.00	00.00
MLP_BP	87.55	15.76	37.14	87.84	01.98	13.18
SONN	67.19	96.41	46.82	67.29	96.52	46.92



Graph-2: Results of different classifiers for training dataset (Sensitivity, Specificity, G-Mean)



Graph-3: Results of different classifiers for test dataset (Sensitivity, Specificity, G-Mean)

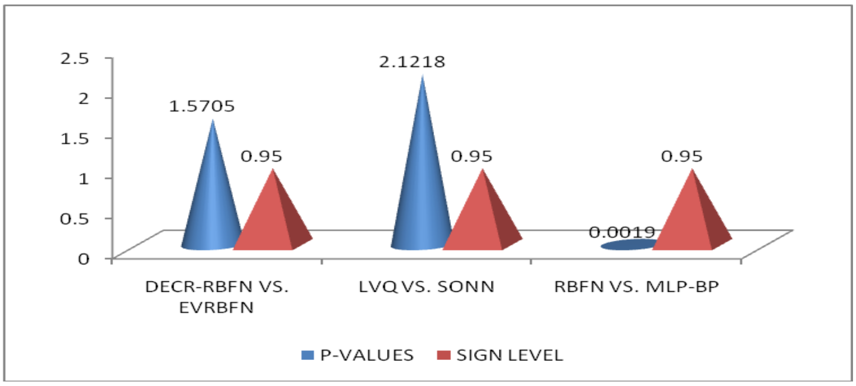
After doing the experiment, the SONN method has shown the best results than other algorithms *i.e.*, 96.28% for the training datasets and 95.91% for the testing datasets using the performance metrics accuracy.

VI. STATISTICAL TEST

For the statistical analysis the Mann Whitny U test (non-parametric test) is used in this paper [26]. The standard sign level value is 0.95. Here, the two samples are independent and very useful.Table-4 placed below visualises the statistical test followed by Graph-4 for clear understanding.

Table 4: Statistical test using Mann Whitny U test

METHODS	P-VALUES	SIGN LEVEL	HYPOTHESIS	SELECTION
DECR_RBFN VS. EVRBFN	1.5705	0.95	REJECTED	EVRBFN
LVQ VS. SONN	2.1218	0.95	REJECTED	SONN
RBFN VS. MLP-BP	0.0019	0.95	REJECTED	RBFN



Graph-4: P-value and sign level for Mann Whitny U test

V. DISCUSSION AND CONCLUSION

In this paper, 10 fold cross-validation technique was employed for six types of classifiers using NSL-KDD dataset. Here, out of 10 fold, 9 fold data is used for training while, the other one is for testing. The entire experiment has been performed by using KEEL software. To measure the experimental result, different performance matrices are used such as, (i) accuracy, (ii) specificity, (iii) sensitivity and (iv) G-mean. A full 41 features of NSL-KDD dataset was used throughout the experiment.

Table-2 supplemented with Graph-1shows the comparison of accuracy for both training and test dataset using NSL-KDD applying different neural network algorithms. Among them, SONN shows the best result i.e., 96.28% for the training dataset and 95.91% for the test dataset.

Table-3 and its corresponding Graph-2 (training) and Graph-3 (test) shows the result for other performance matrices such as specificity, sensitivity and G-mean among which for both training and test dataset LVQ and EVRBFN shows the best result i.e, 100% each in sensitivity. On the other hand, SONN shows the best result for specificity i.e, 96.41%and 96.52% for both training and test dataset respectively. Again the table visualised that, RBFN shows 70.32% and 69.34% for G-mean in both training and test dataset.

Further, the result of the statistical test using 'MannWhitnyU' in Table-4 and its accompanying Graph- 4 depicts the P-value of DECR_RBFN vs EVRBFN which comes to 1.5705 and LVQ vs SONN results 2.1218 which is greater than the standard sign level value i.e, 0.95. So, we selected the second classifier i.e, EVRBFN and SONN. On the other hand, for RBFN vs MLP-BP classifiers, p value is 0.0019 which is less than the standard sign level value. So, we selected RBFN classifier.

REFERENCES

[1] R. R. Reddy, B. Kavya and Y. Ramadevi,Y..A survey on SVM for Intrusion Detection. *International Journal of Computer Application*. 98(19): 38-43, 2014.

[2] B. Ingre and A. Yadav. Performance Analysis of NSL-KDD dataset using ANN. *Signal Processing and Communication Engineering Systems (SPACES)*.92-96, 2015.

[3] G. Schaffer. Building a cheap and powerful intrusion detection system. *Computer world*. 2007 Available http://www.computerworld.com/article/2541227

[4] Kemmerer and G. Vigna. Intrusion detection: A brief history and overview. *Security & Privacy*.27-30, 2002.

[5] ›derick. Network Intrusion Detection Signature. 2001. Available http://online. Securityfocus. com/infocus/1524.

[6] S. Kumar and A. Yadav. Increasing performance of intrusion detection system. *IEEE Int. conf. on Advanced communication control and computing technology*.546-550,2014

[7] S. Ranshous, S. Shen, D. Koutra, C. Faloutsos and N.F. Samatova. Anomaly Detection in Dynamic Networks: A Survey. *WIREs Computational Statistics*.7.223-247, 2014.

[8] J. Rejchrt. Network Anomaly Detection–Survey Evaluation. 2014. Available https://labs. ripe.net/ Members/jan_rejchrt/network-anomaly-detection-2013-survey evaluation.

[9] A.A. Sayer, S. N. Pawar and V. Mane. A Review of Intrusion Detection System in Computer Network, *International Journal of Computer Science and Mobile Computing*, 3(2): 700-703, 2014.

[10] A. Shrivastava, M. Baghel and H. Gupta, H. A Review of Intrusion Detection by Soft Computing and Data Mining Approach, *International Journal of Advanced Computer Research*, 3(12): 224-228, 2013.

[11] J. Wang and Y. Yu.. Research on Hybrid Neural Network in Intrusion Detection System, *World Academy of Science, Engineering and Technology*, 7(4): 481-485,2013.

[12] R. R. Panko. . Corporate Computer and Network Security, 2nd ed., New Delhi, 2012.

[13] P. K. Singh, A. K. Vatsa, R. Sharma and P. Tyagi. Taxonomy Based Intrusion Attacks and Detection Management Scheme in Peer to Peer Network, *International Journal of Network Security & Its Applications* (IJNSA), 4 (5): 167-179, 2012.

[14] T. Vamsidhar, A. Reddyboina and V. Rayala. Intrusion Detection System for Web Application with attack classification, *Journal of Global Research in Computer Science*, 3(12): 44 -50, 2012.

[15] D. P. Vinchurkar and A. Reshamwala. A Review of Intrusion Detection System Using Neural Network and Machine Learning Technique, *International Journal of Engineering Science and Innovative Technology*, 1(2): 54-63, 2012.

[16] R. Somer. Viable Network Intrusion Detection: Trade-offs in High Performance Environments, VDM Verlag Dr. Muller, Germany: 9-11, 2010.

[17] G. Wang, J. Hao, J. Ma and L. Huang. A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering, 37(9): 6225-6232, 2010.

[18] L. Cherkasova, K. Ozonat, N. Mi, J. Symons and E. Smirni. Automated Anomaly Detection and Performance Modelling of Enterprise Applications. *Journal of ACM*

Transactions on Computer Systems, 27(3): 6.1-6.32, 2009.

[19] DARPA Intrusion Detection Data sets. Cyber Systems and Technology. MIT Lincoln Laboratory, http://www.ll.mit.edu.

[20] M. Tavallaee, E. Baghari, W. Lu and A. A. Ghorbani. A detailed analysis of the KDD CUP 99 datasets, *In. Proc. 2nd IEEE Symposium on Computational Intelligence in Security and Defence Applications.*53-58, 2009.

[21] J. C. Bezdek and L. I. Kuncheva. Nearest prototype classifier designs: An experimental study. *International Journal of Intelligent Systems*, 16(12): 1445-1473, 2001.

[22] D. S. Broomhead and D. Lowe. *Radial basis functions, multi-variable functional interpolation and adaptive networks* (Royal Signals and Radar Establishment Memorandum 4148). Royal Signals and Radar Establishment Malvern (United Kingdom).1-40, 1988.

[23] V. M. Rivas, J. J. Merelo, P. A. Castillo, M. G. Arenas and J. G. Castellano. Evolving RBF neural networks for time-series forecasting with EvRBF. *Information Sciences*, 165(3): 207-220, 2004.

[24] R. Rojas and J. Feldman. Neural Networks: A Systematic Introduction . Springer-Verlag, Berlin, New-York, 1996.

[25] I. G. Smotroff, D. H. Friedmanand D. Connolly. Self organizing modular neural networks, 1991. Available http://ieeexplore.ieee.org/document/ 155336/.

[26] H. B. Mann and D. R. Whitney On a test of whether one of two random variables is stochastically larger than the other. *The Annals of Mathematical Statistics*, 50-60, 1947.

[27] J. McHugh. Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory. ACM Transactions on Information and System Security. 3(4):2000. Available http://www.cs.cmu.edu/~maxion/courses/ mchugh00.pdf.

[28] R. Caruana and A. Niculescu-Mizil. Data mining in metric space: an empirical analysis of supervised learning performance criteria. *Proc.of the10th ACM SIGKDD int. conf. on Knowledge discovery and data mining*, 2004.

[29] A. S. Aneetha and S. Bose. The combined approach for anomaly detection using neural networks and clustering techniques, *Computer Science & Engineering*. 2(4): 37-46, 2012.

[30] M. Myers. Managing and Trobleshooting Networks, 2nd Ed., New Delhi, McGraw Hill, 2009.

[31] Neeraj Kumar, Upendra Kumar and G. Sahoo. Intrusion Detection Algorithm for data security. *International Journal of Computer Trends and Technology (IJCTT)* , 29 (3):158, 2015.