NEURAL NETWORK BASED INTRUSION DETECTION SYSTEM AND ATTACK CLASSIFICATION USING BACK PROPAGATION ALGORITHM

[1]Mandala Anusha, [2]Aparajita, [3] Devendra Ku. Singh, [4]Dr. Manish Shrivastava
[1] B.tech Student, [2] B.tech Student, [3]Assistant Professor, [4]Assistant Professor.
[1,2,3,4]Dept. of C.S.E,
[1]Guru Ghasidas Vishwavidyalaya,
Bilaspur (C.G.), Chhattisgarh, India.

Abstract: There is rapid increase in the way we are using the internet from the last few years in many areas like business, research and education., it is essential to keep data secure and safe. Intrusion detection systems(IDS) are used for securing the data. Most of the research is going on machine learning now a days. Back propagation neural network (BPN) approach is used by several researchers for their experiments and most of them used KDDCup'99 dataset and categorized the attacks into normal, R2L, Dos, probe, U2L.This paper primarily focused on research which is based on KDDCup'99 dataset of 311029 instances and are categorized into 5 classes of attacks and obtained detection rate of 90.0%.

***Keywords* - classification of attacks, Back Propagation Neural Network(BPNN) algorithm, Intrusion Detection System (IDS), detection rate.**

I. INTRODUCTION

Intrusion is a set of actions which compromise the security goals like.. confidentiality , integrity of files or accessibility of a computer resource. The method of identifying, detecting and responding to malicious activities in the system which are targeted at the resources is known as intrusion detection. The system which is designed to analyse network system against a given set of parameters and observe and find the data for which these threshholds are met is called intrusion detection system. Mainly they are two types of intrusion detection system(IDS)…,Former is host based IDS which monitors important operating system files and the latter is network IDS which analyses the traffic of the incoming network.

IDS is classified into two types based on detection approach.,ANAMOLY and SIGNATURE based..,, signature based is used for the detecting attacks based on specific patterns like byte sequence patterns, we can detect the attacks. Anomaly based is used first for identifying unknown attacks, later due to huge development of threats, machine learning is the basic model which is used for comparing new behaviour with the trustworthy model.

Neural network method has the ability to detect unknown and known attacks. It is of two types unsupervised(training without teacher) and supervised(training with teacher) algorithm. Neural network approach is used in many research papers. Back propagation neural network(BPN) has given good detection rate when compared with other neural networks. Therefore it is used for classification of attacks, depending on that deterrent action can be taken. Learning with teacher approach is used for training the data set in Back Propagation Neural network algorithm. The main intention of this paper is to classify attacks into 5 major types using BPN algorithm. KDD'Cup99 dataset of 311029 instances is used for training BPN network.

Most of the researchers used back propagation for classification of events into major attack classes and achieved better results [2],[3],[4]. In this research paper by using back propagation algorithm, the main thing is to detect, categorize(classify) events into specific attack type and system is evaluated by monitoring detection rate.

II. METHODOLOGY

Initially using KDD 99 dataset network is trained . Then a small part of the data is initially used for the training purpose. In this we used 17 hidden layers with 41 input features and 5 output features.

Working :

Back propagation algorithm is used for the training purpose. The working of back propagation agorithm is discussed below:

(i) first design the network and then initialize the parameters.

(ii) pick out the succeeding training pair from the data set which is being trained and supply the input vector to the network input.
(iii)Specify the hidden layers that are needed for the network.
(iv)calculate the output given by the network.
(v)after training the network, calculate the error.
(v)and then calculate the weights variations, using the formula

$$u_{jk} \leftarrow u_{jk} - \eta \frac{\partial E}{\partial u_{jk}}$$

and then again feed the network with the updated weights for better accurate results.
(vi)The training is continued until desired result is obtained with the minimum possible deviations.

In Intrusion Detection System(IDS), attacks can be predicted in four different types:True positivity(TP), False negativity(FN), True negativity(TN), False positivity(FP).

True Positivity(TP):It is the value of the class which we want to calculate.

False Negativity(FN):It is computed by adding the values in the corresponding row excluding TP.

True Negativity(TN):It is computed by adding the values of the columns and rows excluding that column and row.

False Positivity(FP):It is computed by adding the values in the corresponding column excluding TP.

Overall Accuracy: It is the ratio of the number of items which are correctly predicted to the entire no of classes.,It is given by the formula

AC = (TP+TN)/(TP+TN+FP+FN)

Now, calculating the overall accuracy for class1 (normal) from the given table3.1:

AC[1]=(72603+128478) / (72603+128478+34+16483)
= 0.924
= 92.4%

Sensitivity(recall value): sensitivity is defined as the true positive rate of the given particular class.It is given by the formula

Sensitivity = (TP)/(TP+FN)

Now, calculating the sensitivity for class1 (normal) from the given table3.1:

Sensitivity[1] = (72603) / (72603+34)
= 0.999
= 99.9%

Specificity: specificity of a particular class gives us the true negative rate of that particular class.It is given by the formula:

Specificity = (TN)/(TN+FP)
Now we are calculating the specificity for class1 (normal) from the given table3.1:

Specificity[1] = (128478) / (128478+16483)
= 0.886
= 88.6%

Precision: It is the state of being precise or exact or accurate value.

Precision=(TP)/(TP+FP).

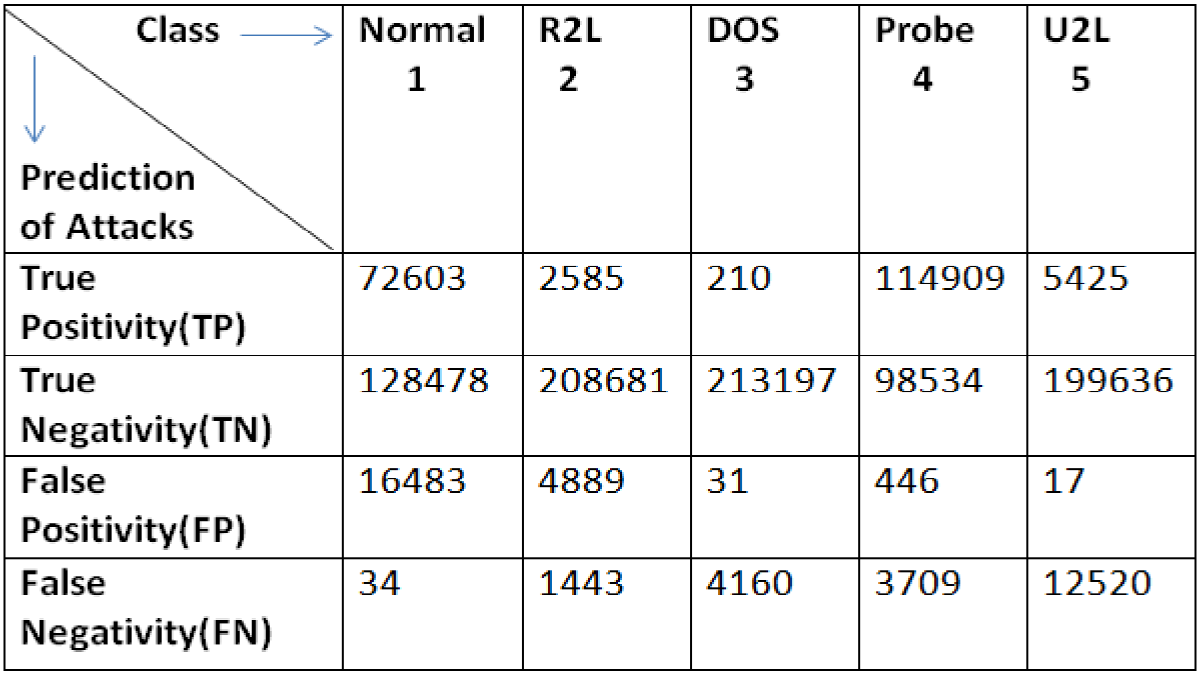
Now we are calculating the Precision for class1 (normal) from the given table3.1:

Precision^1 = (72603) / (72603+16483)
= 0.8149
= 81.49%

From below calculated values(i.e table: 3.2)..,,We can conclude that last row in training confusion matrix indicates PRECISION and last column in confusion matrix indicates SENSITIVITY.

III. EXPERIMENTAL RESULTS

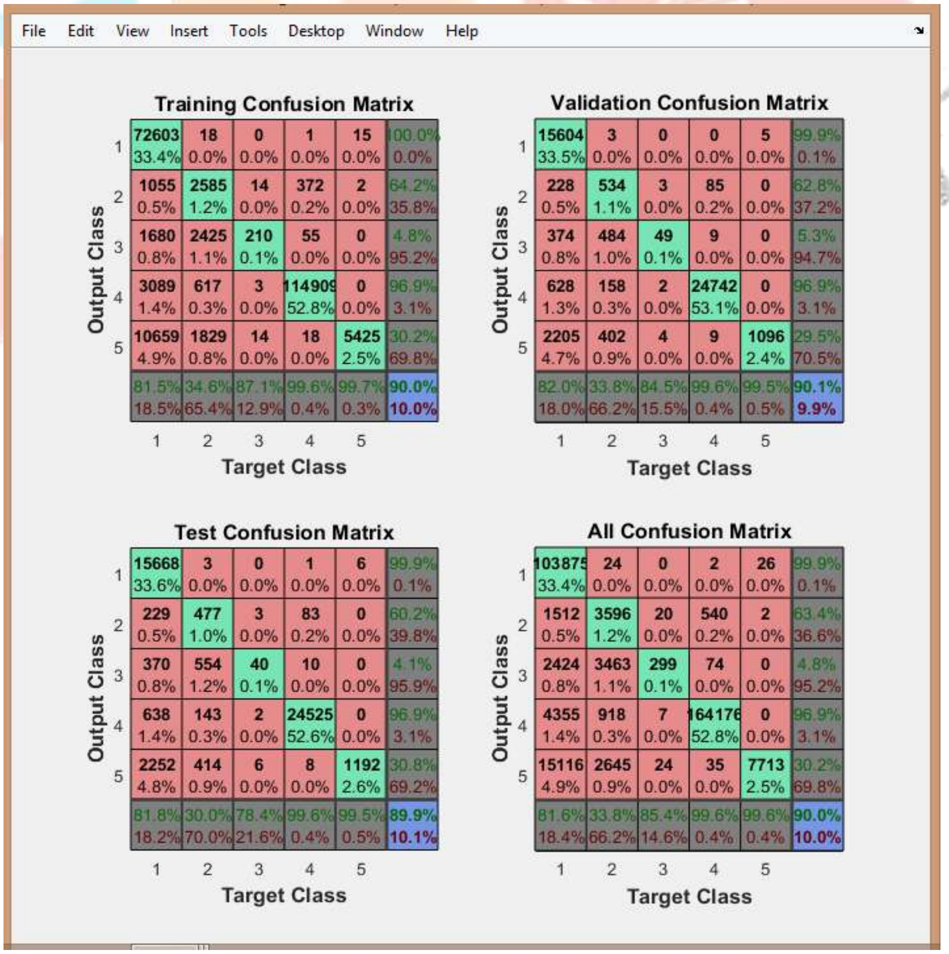
table 3.1:observation table1



Class → ↓ Prediction of Attacks	Normal 1	R2L 2	DOS 3	Probe 4	U2L 5
True Positivity(TP)	72603	2585	210	114909	5425
True Negativity(TN)	128478	208681	213197	98534	199636
False Positivity(FP)	16483	4889	31	446	17
False Negativity(FN)	34	1443	4160	3709	12520

Table3.2: observation table2

	1	2	3	4	5
ACCURACY	92.4%	97.6%	98%	98.09%	49.1%
SENSITIVITY	99.9%	64.17%	4.8%	96.87%	30.2%
SPECIFICITY	88.6%	97.7%	99.9%	99.54%	99.99%
PRECISION	81.49%	34.58%	87.1%	99.6%	99.68%



Training Confusion Matrix

Output Class

1	72603 33.4%	18 0.0%	0 0.0%	1 0.0%	15 0.0%	100.0% 0.0%
2	1055 0.5%	2585 1.2%	14 0.0%	372 0.2%	2 0.0%	64.2% 35.8%
3	1680 0.8%	2425 1.1%	210 0.1%	55 0.0%	0 0.0%	4.8% 95.2%
4	3089 1.4%	617 0.3%	3 0.0%	114909 52.8%	0 0.0%	96.9% 3.1%
5	10659 4.9%	1829 0.8%	14 0.0%	18 0.0%	5425 2.5%	30.2% 69.8%
	81.5% 18.5%	34.6% 65.4%	87.1% 12.9%	99.6% 0.4%	99.7% 0.3%	90.0% 10.0%
	1	2	3	4	5	

Target Class

Validation Confusion Matrix

Output Class

1	15604 33.5%	3 0.0%	0 0.0%	0 0.0%	5 0.0%	99.9% 0.1%
2	228 0.5%	534 1.1%	3 0.0%	85 0.2%	0 0.0%	62.8% 37.2%
3	374 0.8%	484 1.0%	49 0.1%	9 0.0%	0 0.0%	5.3% 94.7%
4	628 1.3%	158 0.3%	2 0.0%	24742 53.1%	0 0.0%	96.9% 3.1%
5	2205 4.7%	402 0.9%	4 0.0%	9 0.0%	1096 2.4%	29.5% 70.5%
	82.0% 18.0%	33.8% 66.2%	84.5% 15.5%	99.6% 0.4%	99.5% 0.5%	90.1% 9.9%
	1	2	3	4	5	

Target Class

Test Confusion Matrix

Output Class

1	15668 33.6%	3 0.0%	0 0.0%	1 0.0%	6 0.0%	99.9% 0.1%
2	229 0.5%	477 1.0%	3 0.0%	83 0.2%	0 0.0%	60.2% 39.8%
3	370 0.8%	554 1.2%	40 0.1%	10 0.0%	0 0.0%	4.1% 95.9%
4	638 1.4%	143 0.3%	2 0.0%	24525 52.6%	0 0.0%	96.9% 3.1%
5	2252 4.8%	414 0.9%	6 0.0%	8 0.0%	1192 2.6%	30.8% 69.2%
	81.8% 18.2%	30.0% 70.0%	78.4% 21.6%	99.6% 0.4%	99.5% 0.5%	89.9% 10.1%
	1	2	3	4	5	

Target Class

All Confusion Matrix

Output Class

1	103875 33.4%	24 0.0%	0 0.0%	2 0.0%	26 0.0%	99.9% 0.1%
2	1512 0.5%	3596 1.2%	20 0.0%	540 0.2%	2 0.0%	63.4% 36.6%
3	2424 0.8%	3463 1.1%	299 0.1%	74 0.0%	0 0.0%	4.8% 95.2%
4	4355 1.4%	918 0.3%	7 0.0%	164176 52.8%	0 0.0%	96.9% 3.1%
5	15116 4.9%	2645 0.9%	24 0.0%	35 0.0%	7713 2.5%	30.2% 69.8%
	81.6% 18.4%	33.8% 66.2%	85.4% 14.6%	99.6% 0.4%	99.6% 0.4%	90.0% 10.0%
	1	2	3	4	5	

Target Class

Fig3.1.1: confusion matrix

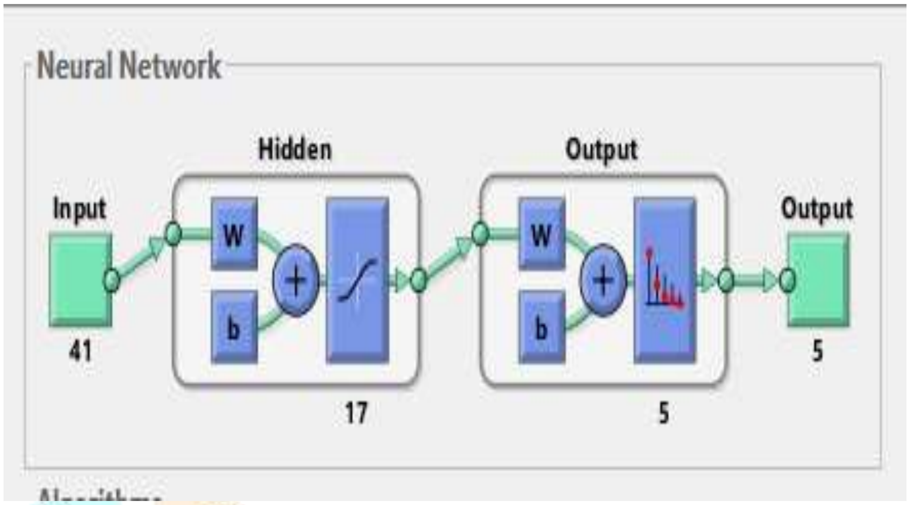


Fig3.1.2: neural network

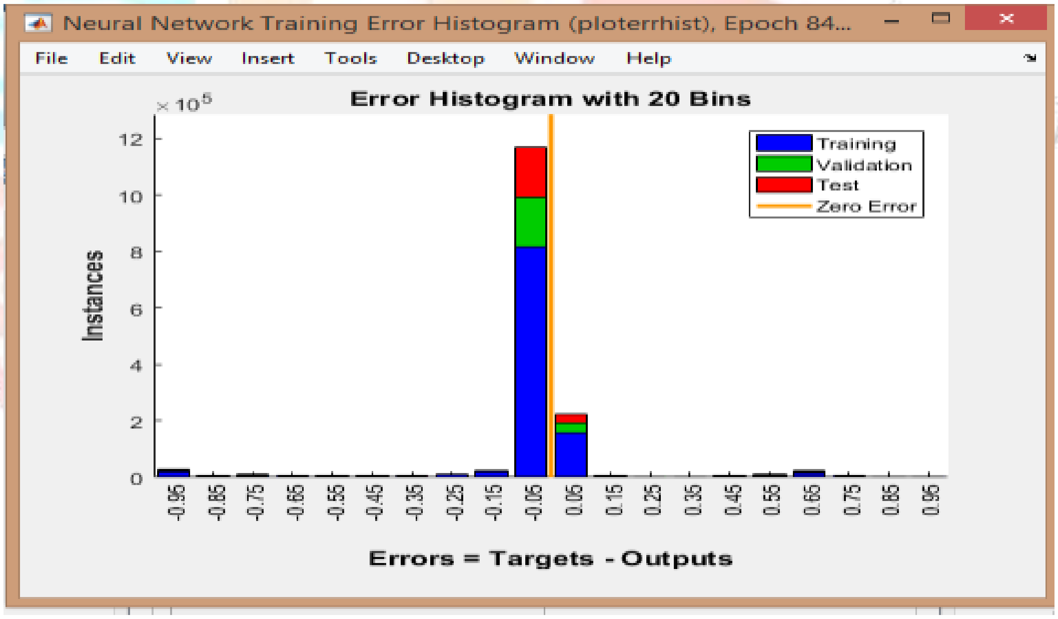


Fig3.1.3: error histogram of neural nework

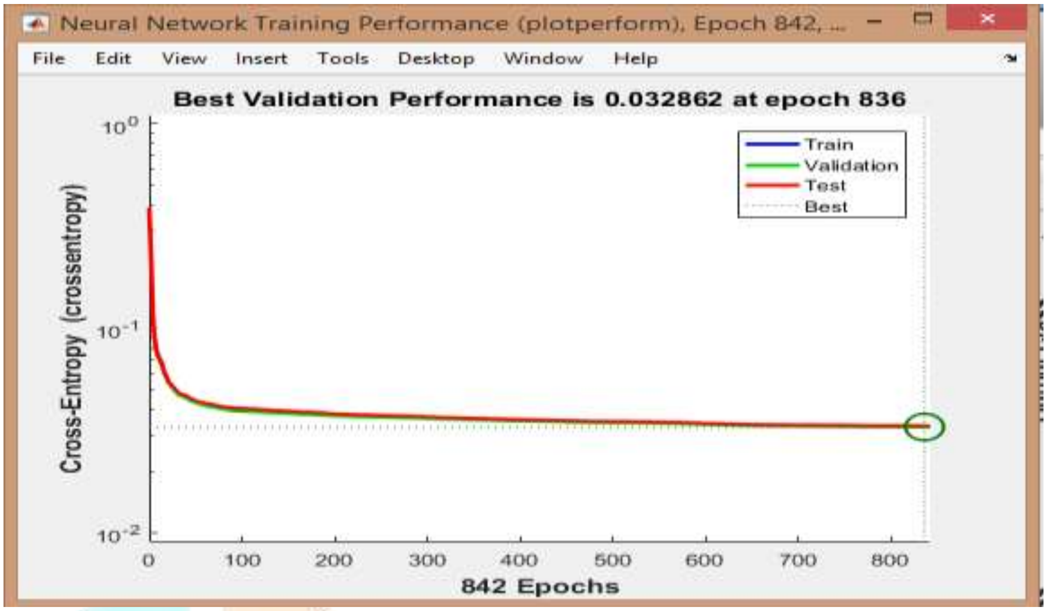


fig3.1.4: performance

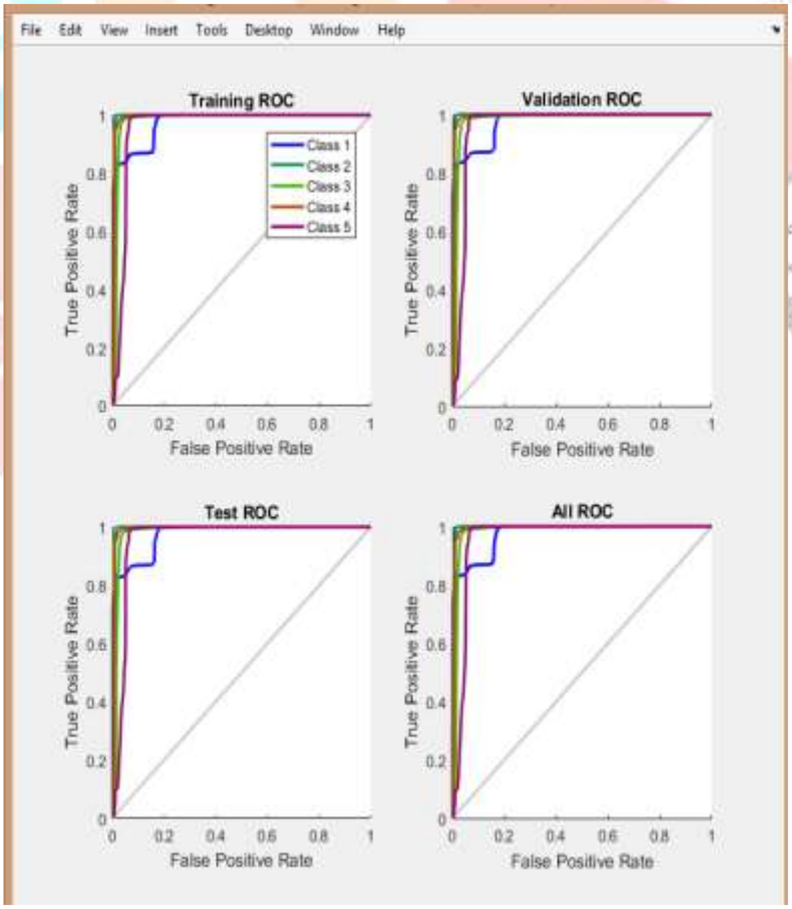


Fig3.1.5:receiver operating characteristic

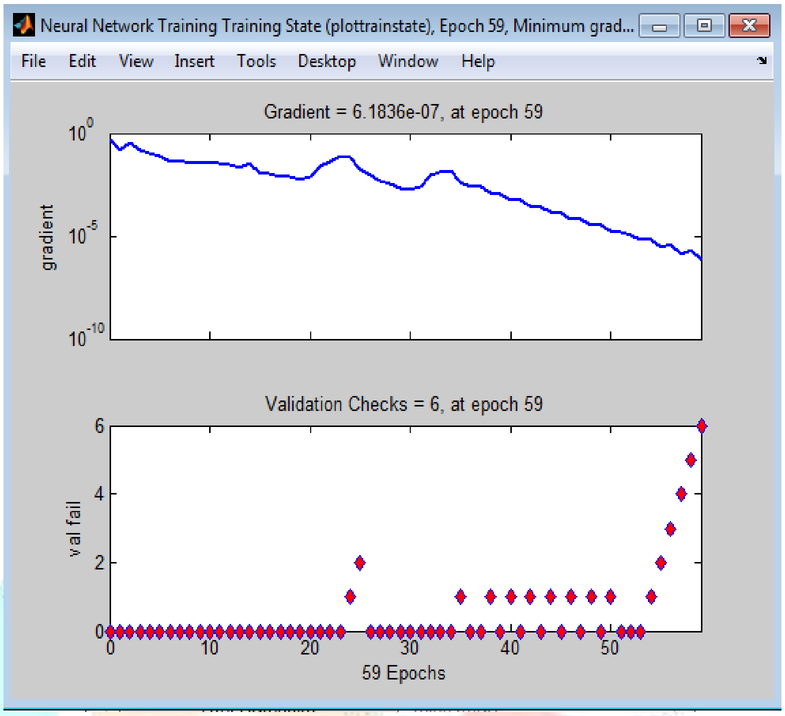
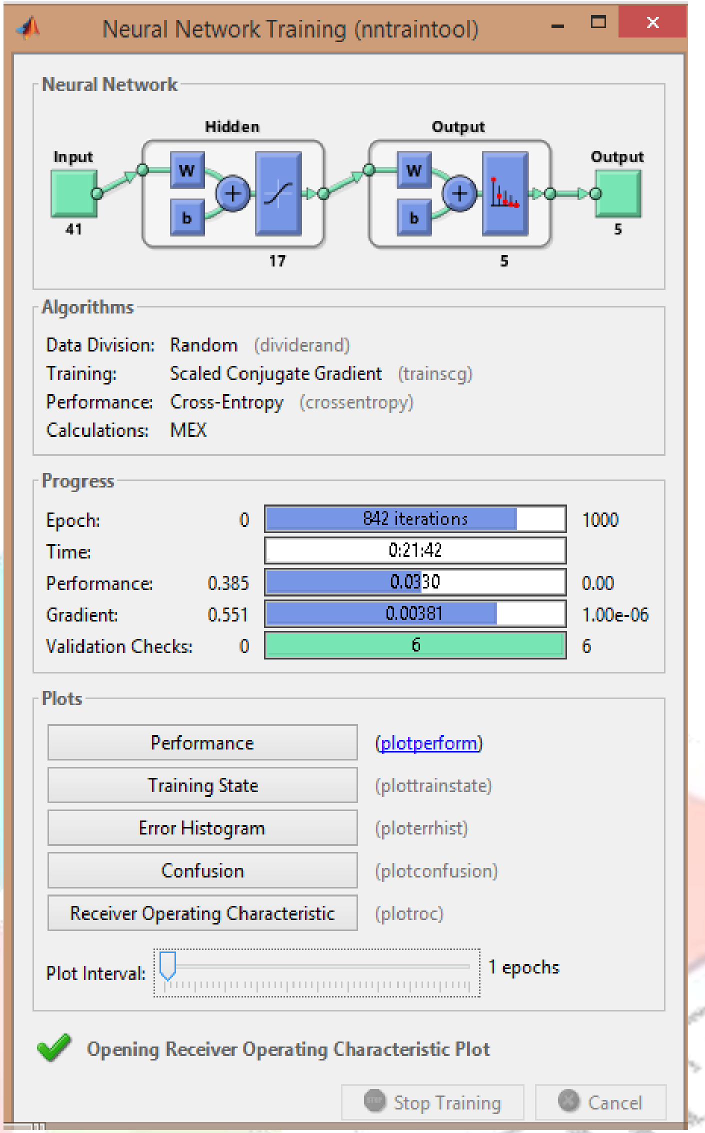

Neural Network Training Training State (plottrainstate), Epoch 59, Minimum grad...
File Edit View Insert Tools Desktop Window Help
Gradient = 6.1836e-07, at epoch 59
gradient
10^{0}
10^{-5}
10^{-10}
Validation Checks = 6, at epoch 59
val fail
6
4
2
0
0
10
20
30
40
50
59 Epochs

Fig3.1.6: training state



Algorithms

Data Division: Random (dividerand)
Training: Scaled Conjugate Gradient (trainscg)
Performance: Cross-Entropy (crossentropy)
Calculations: MEX

Progress

Epoch:	0	842 iterations	1000
Time:		0:21:42	
Performance:	0.385	0.0330	0.00
Gradient:	0.551	0.00381	1.00e-06
Validation Checks:	0	6	6

Plot Interval: 1 epochs

✓ Opening Receiver Operating Characteristic Plot

ssFig3.1.7: neural network training

IV. CONCLUSION AND FUTURE WORK

In future, our work will depend on Particle Swarm Optimization(PSO) with the help of Back Propagation Neural Network(BPNN) which is hybrid model..

REFERENCES

[1] https://en.wikipedia.org/wiki/Intrusion_detection_system
[2] Jaiganesh V.et alssss.,"An Analysis of Intrusion Detection System using Back Propagation NeuralNetwork", IEEE 2013 Publication.
[3] Han C., Yi Lv, Yang D., Hao Y., "An Intrusion Detection System Based on Neural Network",2011 International Conference on Mechatronic Science, Electric Engineering and Computer, August 19-22, 2011, Jilin, China,IEE Publication.
[4] Faraj S, Al-Janabi and Saeed H, "A Neural Network Based Anomaly Intrusion Detection System",2011 Developments in E-systems Engineering,DOI 10.1109/DeSE.2011.19,IEEE publication.
[5] Roshani Gaidhane, C. Vaidya et al." Intrusion Detection and Attack Classification using Back-propagation Neural Network", International Journal of Engineering Research & Technology (IJERT) IJERTIJERT ISSN: 2278-0181 in march 2014.
[6] Ning P., Jajodia S.,"Intrusion Detection Techniques", http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.89.2492&rep=rep1&type=pdf.

[7] Kim J., Bentley P.,Aickelin U., Greensmith J., Tedesco G., Twycross J.,"Immune System Approaches to Intrusion Detection- A Review",Natural Computing, Springer, in print, doi: 10.1007/s11047-006-9026-4, pp TBA

[8] Xiaonan Wu S. and Banzhaf W.," The Use of Computational Intelligence in Intrusion Detection Systems: A Review", A technical report #2008-05,Memorial University of Newfoundland, St John’s, NL A1B 3X5, CA.

[9] M. E. Elhamahmy, Hesham N. et.al “A New Approach for Evaluating Intrusion DetectionSystem” , CiiT International Journal of Artificial Intelligent Systems and Machine Learning, November 2010.