ISSN: 2581-3404 (Online)
International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-3, Issue-4, 2019

Experimental Evaluation of Neural Network and Optimization Techniques for Intrusion Detection System

Amita Tiwari[1], Prof. Atul Shrivastava[2]

[1]M. Tech Scholar, Department of CSE, SIRTE, Bhopal (India)

[2]Professor, Department of CSE, SIRTE, Bhopal (India)

[1]amitatiwari777@gmail.com, [2]akshri5@gmail.com

ABSTRACT

In today’s high technology environment, internet can be a hazardous place, since enterprises are becoming more and more competent and dependent on their information systems. The threats to information systems create security concern of both industry and public about the proper use of sensitive data. Nowadays security issues are growing in a tremendous rate. So it is expedient to have a mechanism to keep track of its security issues in the network or host. In this paper presents the comparative performance evaluation for the network based intrusion detection system and show the experimental results with the existing techniques, our simulated results shows proposed method gives better results than the existing techniques in terms of accuracy and other performance parameters.

Keywords:- Intrusion detection system, Neural network, Optimization techniques, Accuracy, Precision, Recall.

INTRODUCTION

In recent years the security becomes the most serious problem in issues of securing data or information year over year. Because the intruders introduce a new variety of intrusions in the market, so that user can’t manage their computer system or network. There are two types of classification used in an Intrusion detection system the attacks can be classified into two different categories one is misuse or signature based detection and the second one is anomaly based detection.

The misuse or signature based intrusion detection system detects the intrusion by comparing with its existing signatures in the database. The signature based intrusions are called known attacks, when log file contains the list of known attacks detecting from the computer system or networks. The anomaly based intrusion detection is called as unknown attacks and this type of attack is occurred from the network. The intrusion detection systems are classified as Network based intrusion detection system and Host based intrusion detection system [3]. IDS are one of the key technologies to guarantee the systems security. IDS make a real time response to intrusion actions and intrusion processes. The goal of Intrusion Detection is to identify all the proper attacks and negatively identify all the non-attacks. And the various techniques for detection of vulnerabilities that improve the performance of the detection of known and unknown vulnerabilities, and use a dataset which is efficient means without redundancy. Here Below diagram shows the percentage wise distribution of the research paper under various methodologies that are applied in the creations of IDS. The most commonly and widely applied approach is the hybrid approach.

Intrusion Detection Systems (IDS) turned into a standard component in security foundations as they allow network administrators to find approach infringement. Current IDS have assortment of genuine downsides: Current IDS are infrequently tuned to distinguish striking administration level system assaults. This abandons them inclined to unique and novel malicious assaults. Information overload: Another perspective that doesn't relate on to misuse detection however is exceptionally fundamental and what extent of information an expert will with proficient analysis. The amount of learning must review and looks forward rapidly. Contingent upon the intrusion identification instruments used by an association and its size there's the likelihood for logs to prevail in a great many records for every day.

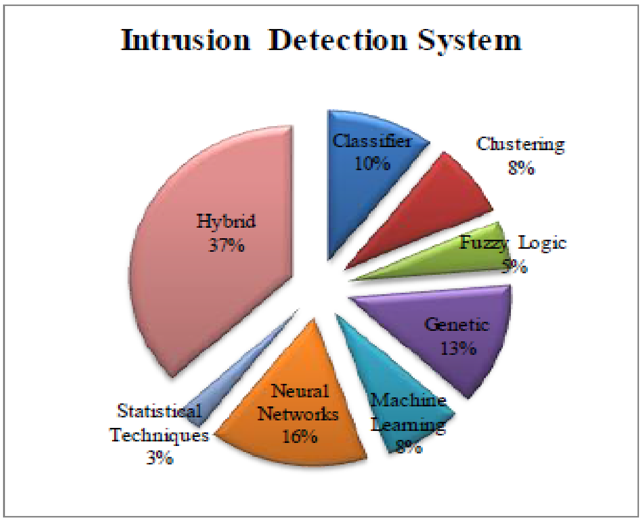


Fig 1: The percentage distribution of the number of papers under various IDS approaches.

The rest of this paper is organized as follows in the first section we describe an introduction of about intrusion detection system. In section II we discuss about the proposed work and architecture for intrusion detection system, In section III we discuss about experimental work for the intrusion detection system, finally in section IV we conclude the about our paper.

II PROPOSED WORK

In this section we discuss about the proposed methods and their architecture for the network based intrusion detection system, here we also compare our proposed methods with the existing techniques. Artificial neural network is an information processing model that is inspired by the biological nervous systems, such as brain, process information. It tries to represent the physical brain and thinking process through electronic circuit or software. Artificial neural network is the network of individual neurons. Each neuron is a neural network acts as an independent processing element. Each processing element (neuron) is fundamentally a summing element followed by an activation function. The output of each neuron (after applying the weight parameter associated with the connection) is fed as the input to all of the neurons in the next layer.

In this paper for the improvement in the intrusion detection system for the efficient classification of dataset of system we used the swarm intelligence family methods i.e. particle swarm optimization for the feature selection and classification for the various types of attacker and unknown user.

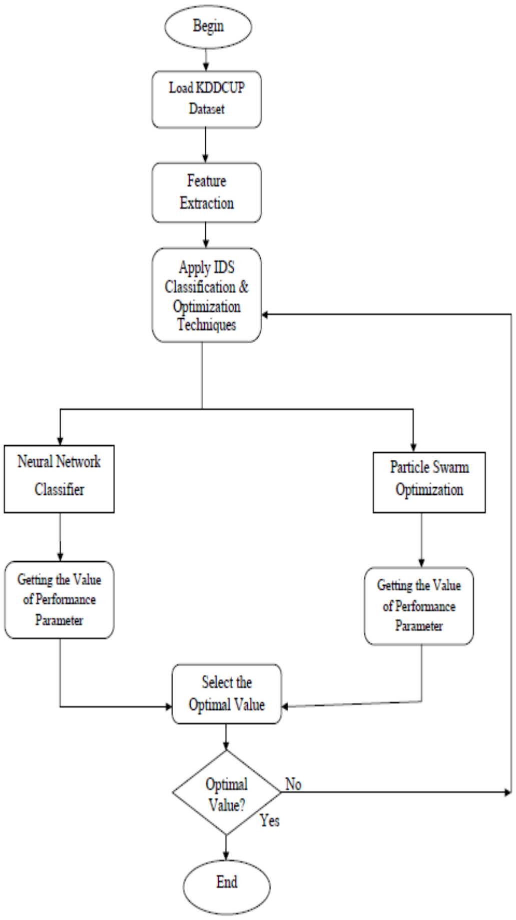
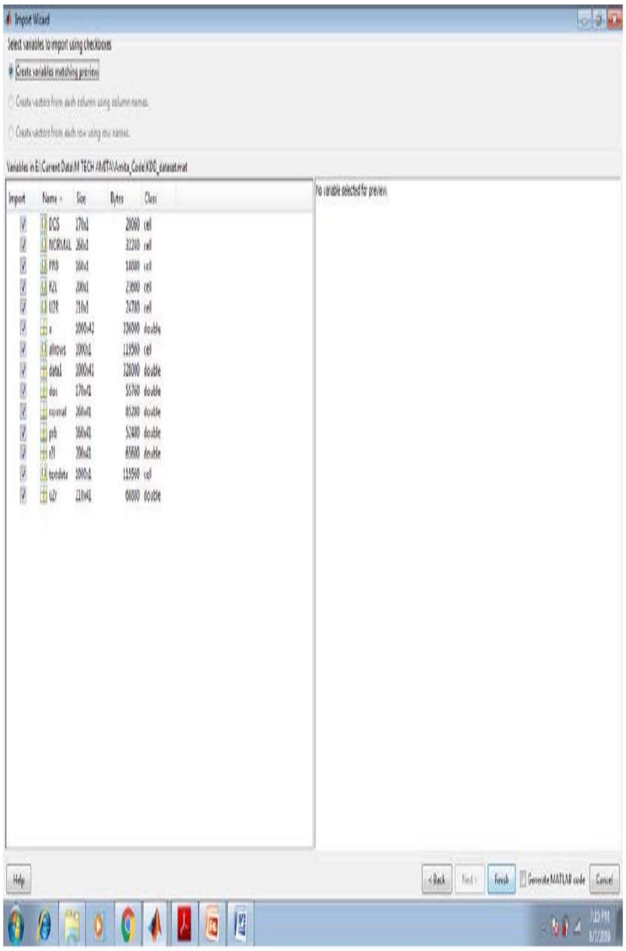

Begin
Load KDDCUP Dataset
Feature Extraction
Apply IDS Classification & Optimization Techniques
Neural Network Classifier
Particle Swarm Optimization
Getting the Value of Performance Parameter
Getting the Value of Performance Parameter
Select the Optimal Value
Optimal Value?
No
Yes
End

Fig 2: proposed model for intrusion detection.

III EXPERIMENTAL WORK

Network Intrusion Detection System (NIDS) constitutes an essential security tool for organizations to monitor network traffic and identify network attacks. In this paper presents the comparative performance evaluation for the various parameters such as the precision, recall and accuracy, using the neural network techniques and the optimization techniques, here we also discuss the our simulated result and the comparative graph based on the value as we found after the experimental result process. All the results are tested with the kddcup dataset and simulated with the matlab software.



Import Wizard

Select variables to import using checkboxes

● Create variables matching preview.

○ Create vectors from each column using column names.

○ Create vectors from each row using row names.

Variables in E:\Current Data\M TECH AMITA\Amita_Code\KDD_dataset.mat

Import	Name	Size	Bytes	Class
☑	DOS	170x1	20060	cell
☑	NORMAL	360x1	32220	cell
☑	PRB	160x1	18880	cell
☑	R2L	200x1	23800	cell
☑	U2R	210x1	24780	cell
☑	a	1000x42	336000	double
☑	allrows	1000x1	119560	cell
☑	data1	1000x41	328000	double
☑	dos	170x41	55760	double
☑	normal	260x41	85280	double
☑	prb	160x41	52480	double
☑	r2l	200x41	65600	double
☑	testdata	1000x1	119560	cell
☑	u2r	210x41	68880	double

No variable selected for preview.

Fig 3: The above figure shows that the main dataset upload windows for the experimental process.

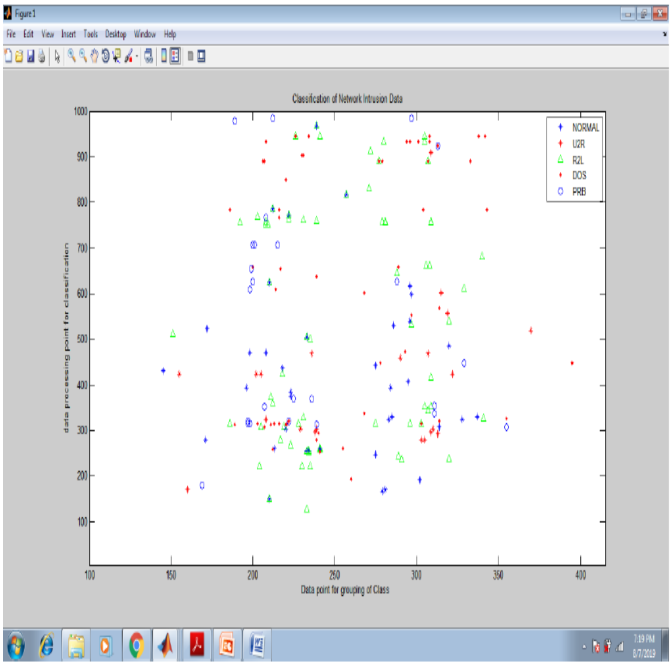


Fig 4: Shows that the intrusion data classification, when the number of generating value is 0.15 and the method is optimization.

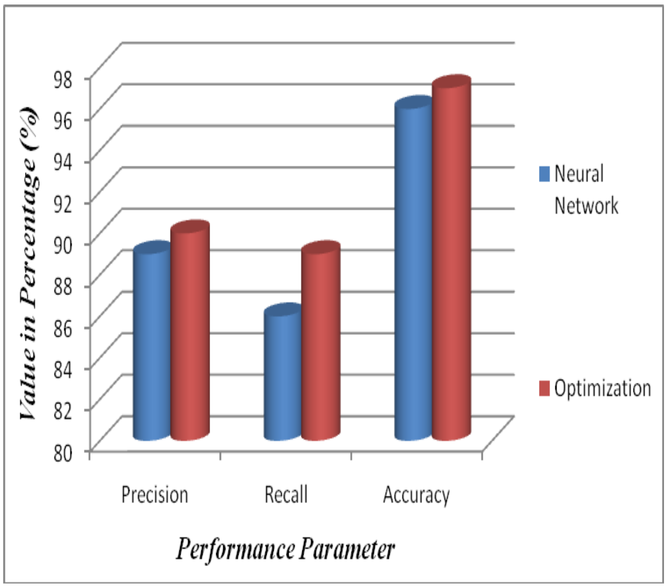


Fig 5: This grpah show the comparative experimental study for the neural network and the optimizatiomn metods for the input value is 0.15.

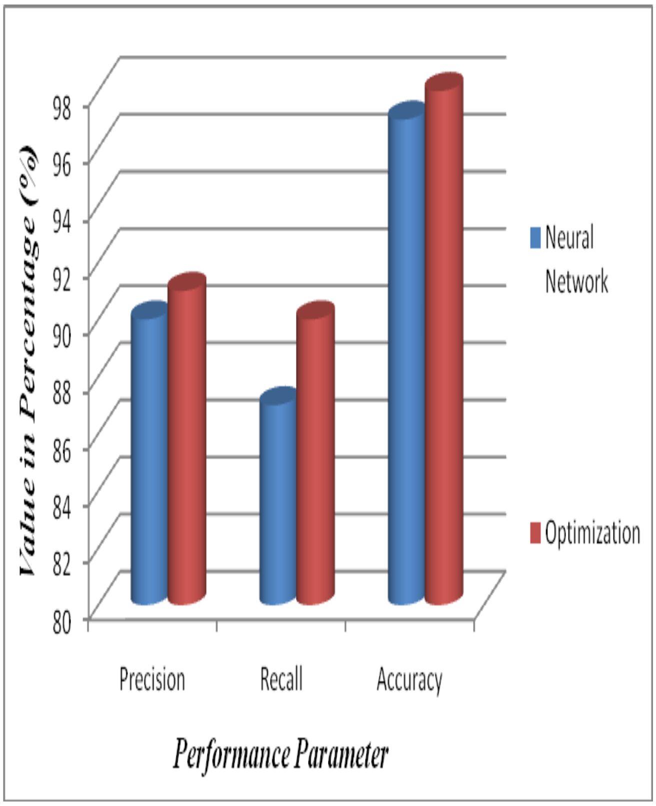


Fig 6: This grpah show the comparative experimental study for the neural network and the optimizatiomn metods for the input value is 0.45.

IV CONCLUSIONS

Intrusion detection based upon computational intelligence is currently attracting considerable interest from the research community. In this paper proposed an efficient intrusion detection model using the classification and optimization techniques, the classification techniques such as feed forward neural network is used and compare with the optimization techniques which is another with classify the kddcup dataset using their attributes or features, thee kddcup contain both the data set i.e. normal and abnormal class of data. Our proposed method gives better results than the existing techniques, In future we also work with feature reduction techniques for the improvement in results and focus on some specific features form the kddcup dataset for the better accuracy and improve the performance of the overall system.

REFERENCES:-

[1] Malek Al-Zewairi, Sufyan Almajali, and Arafat Awajan, “Experimental Evaluation of a Multi-Layer Feed-Forward Artificial Neural Network Classifier for Network Intrusion Detection System”, International Conference on New Trends in Computing Sciences, IEEE 2017, pp 167-172.

[2] D.P.Gaikwad, Ravindra C. Thool, “Intrusion Detection System Using Bagging Ensemble Method of Machine Learning”, International Conference on Computing Communication Control and Automation, IEEE 2015. Pp 291-295.

[3] Preeti Singh, Amrish Tiwari, “An Efficient Approach for Intrusion Detection in Reduced Features of KDD99 using ID3 and classification with KNNGA”, Second International Conference on Advances in Computing and Communication Engineering, IEEE 2015. Pp 445-452.

[4] James Brown, Mohd Anwar, Gerry Dozier, “An Evolutionary General Regression Neural Network Classifier for Intrusion Detection”, IEEE, 2016. Pp 1-5.

[5] Duygu Sinanc Terzi, Ramazan Terzi, Seref Sagiroglu, “Big Data Analytics for Network Anomaly Detection from Netflow Data”, IEEE, 2017. Pp 592-598.

[6] Elike Hodo, Xavier Bellekens, Ephraim Iorkyase, Andrew Hamilton, Christos Tachtatzis, Robert Atkinson, “Machine Learning Approach for Detection of nonTor Traffic”, ARES 2017. Pp 1-6.

[7] Syed Ali Raza Shah, Biju Issac, “ Performance Comparison of Intrusion Detection Systems and Application of Machine Learning to Snort System”, 2017. Pp 1-25.

[8] Enamul Kabir, Jiankun Hu, Hua Wang, Guangping Zhuo, “A Novel Statistical Technique for Intrusion Detection Systems”, Pp 1-39.

[9] Rashidah Funke Olanrewaju, Burhan Ul Islam Khan, Athaur Rahman Najeeb, Ku Nor Afiza KuZahir, Sabahat Hussain, "Snort-Based Smart and Swift Intrusion Detection System", Indian Journal of Science and Technology, 2018. Pp 1-9.

[10] Wrushal K. Kirnapure, Arvind R. Bhagat Patil, " Survey on Classification, Detection and Prevention of Network Attacks using Rule based Approach", International Journal of Computer Applications, 2017. Pp 11-17.

[11] L. Khalvati, M. Keshtgary, N. Rikhtegar, "Intrusion Detection based on a Novel Hybrid Learning Approach", Journal of AI and Data Mining, 2018, Pp 157-162.

[12] Pratham Harshit Rajmahanty, S. Ganapathy, " Role of Decision Trees in Intrusion Detection Systems: A Survey", International Journal of Advances in Computer and Electronics Engineering, 2017. Pp 9-13.

[13] Sheetal Panjeta, Er. Kanika Aggarwal, "Review paper on Different Techniques in Combination with IDS", International Journal of Engineering Science and Computing, May 2017. Pp 11623-11630.

[14] Prasanta Gogoi, B. Borah and D. K. Bhattacharyya, "Network Anomaly Identification using Supervised Classifier", in Informatica 37 (2013) 93-105.

[15] Carlos A. Catania, Facundo Bromberg and Carlos García Garino, "An autonomous labeling approach to support vector machines algorithms for network traffic anomaly detection", Elsevier, International Journal of Expert Systems with Applications 39(2012), pp.1822–1829.

[16] Weijun li1and Zhenyu Liu2, "A method of SVM with Normalization in Intrusion Detection", Elsevier, Procedia Environmental Sciences, 2011 pp. 256-262.

[17] Sebastian Zander, Thuy Nguyen and Grenville Armitage, "Automated Traffic Classification and Application Identification using Machine Learning", in Proceedings of the IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05) , 2005.

[18] Jiankun Hu and Xinghuo Yu, "A Simple and Efficient Hidden Markov Model Scheme for Host-Based Anomaly Intrusion Detection", in IEEE Network January/February 2009.

[19] P. Shrinivasu and P.S.Avadhani, "Genetic Algorithm based Weight Extraction Algorithm for Artificial Neural Network Classifier in intrusion Detection", in Procedia Engineering 38 (2012) 144-153.

[20] Jiankun Hu and Xinghuo Yu, "A Simple and Efficient Hidden Markov Model Scheme for Host-Based Anomaly Intrusion Detection", in IEEE Network January/February 2009.