Performance Analysis of Network Based Intrusion Detection System Ratio using Classification Methods

Kiran Vanpure[1], Avinash Pal[2]

[1]M. Tech Scholar, Department of IT, PCST, Indore (India)

[2]Professor, Department of CSE/IT, PCST, Indore (India)

Abstract

The performance of intrusion detection system depends on classification of unknown types of attacks. The detection of unknown types of attack is very difficult due to large number of attribute and huge amount of network data. For the improvement of unknown attack feature reduction is important area of research. In this paper we discuss about the intrusion detection system, here we proposed a new model for this system and compare with the other existing techniques and model then we found that our proposed model is best for the generation of performance parameter and improve the efficiency and accuracy rate. Here we used the classification techniques such as feed forward neural network and support vector machines for the classification of data and the selection of best optimal features.

Keywords: - Supervised techniques, Swarm Intelligence, Neural network, Classifier, Intrusion Detection system.

INTRODUCTION

An Intrusion Detection System (IDS) inspects the activities in a system for suspicious behavior or patterns that may indicate system attack or misuse. There are two main categories of intrusion detection techniques; Anomaly detection and Misuse detection. The former analyses the information gathered and compares it to a defined baseline of what is seen as "normal" service behavior, so it has the ability to learn how to detect network attacks that are currently unknown.

Misuse Detection is based on signatures for known attacks, so it is only as good as the database of attack signatures that it uses for comparison. Misuse detection has low false positive rate, but cannot detect novel attacks.

However, anomaly detection can detect unknown attacks, but has high false positive rate. An intrusion detection system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches. In other words, intrusion detection is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a system/network.

Traditionally, intrusion detection systems have been classified as a signature detection system, an anomaly detection system or a hybrid/compound detection system. A signature detection system identifies patterns of traffic or application data presumed to be malicious while anomaly detection systems compare activities against a "normal" baseline. On the other hand, a hybrid intrusion detection system combines the techniques of the two approaches. Both signature detection and anomaly detection systems have their share of advantages and drawbacks. The primary advantage of signature detection is that known attacks can be detected fairly reliably with a low false positive rate.

The major drawback of the signature detection approach is that such systems typically require a signature to be defined for all of the possible attacks that an attacker may launch against a network. Anomaly detection systems have two major advantages over signature based intrusion detection systems. The first advantage that differentiates anomaly detection systems from signature detection systems is their ability to detect unknown attacks as well as "zero days" attacks. This advantage is because of the ability of anomaly detection systems to model the normal operation of a system/network and detect deviations from them. A second advantage of anomaly detection systems is that the aforementioned profiles of normal activity are customized for every system, application and/or network, and therefore

making it very difficult for an attacker to know with certainty what activities it can carry out without getting detected. However, the anomaly detection approach has its share of drawbacks as well. For example, the intrinsic complexity of the system, the high percentage of false alarms and the associated difficulty of determining which specific event triggered those alarms are some of the many technical challenges that need to be addressed before anomaly detection systems can be widely adopted.

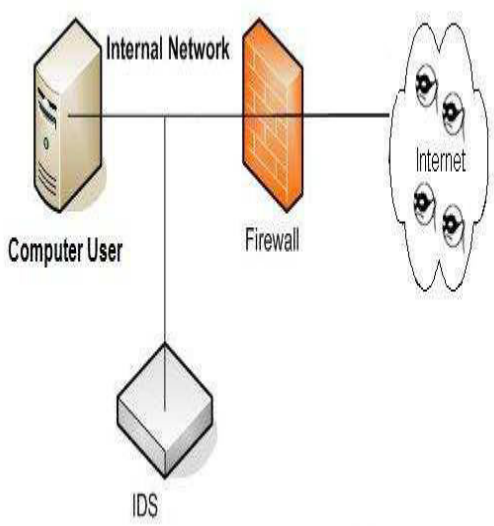

Figure 1: Intrusion detection systems in the network environment.

Types of intrusion detection systems there are two types of intrusion detection systems that employ one or both of the intrusion detection methods outlined above. Host-based systems base their decisions on information obtained from a single host (usually audit trails), while network-based intrusion detection systems obtain data by monitoring the traffic in the network to which the hosts are connected. An intrusion detection system dynamically monitors the events taking place in a monitored system, and decides whether these events are symptomatic of an attack or constitute a legitimate use of the system. Figure depicts the organization of IDS where solid arrows indicate data/control flow while dotted arrows indicate a response to intrusive activities.

The intrusion detection process functions in a way that each packet entering the system is investigated and a copy of the condition of the packet is saved as a reference for the new detection [1]. A Real-Time (RT) response in this field (computer security) is very important as less than fifteen minutes are required by some distributed and coordinated attacks to stop a large area of the Internet from normal functioning [13].

The rest of this paper is organized as follows in section II we discuss about the proposed methods and architecture. In section III we define the dataset. In section IV we discuss about the empirical results. And finally conclude the paper.

II NETWORK-BASED IDS

These days the network-based intrusion detection systems are the very vital role play in the field of commercial product marketing and selling. It is contain usually consist of a set of single-purpose hosts that "sniff" or capture network traffic in various parts of a network and report attacks to a single management console. Because no other applications run on the hosts that are used by a network based IDS, they can be secured against attack.

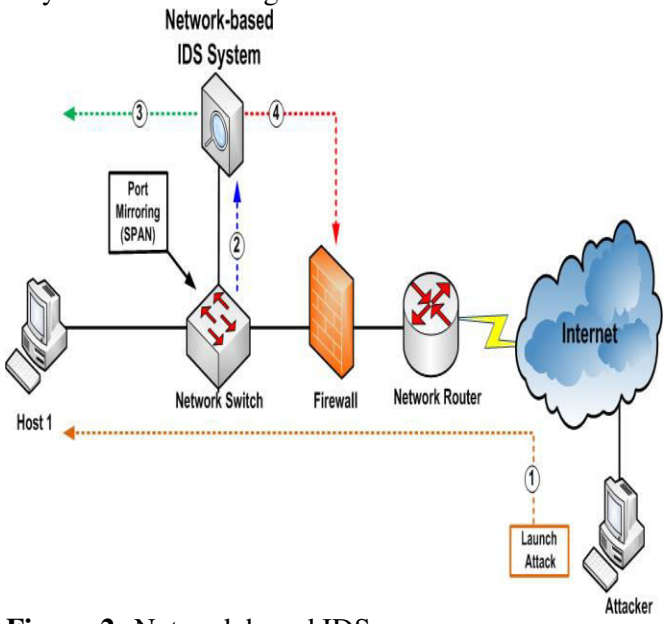

Figure 2: Network based IDS.

III PROPOSED METHOD

In this section discuss the Proposed methodology architecture for the Intrusion detection system using Existing methods Neural network, Evolutionary Algorithms such as Genetic Algorithm and some Swarm Intelligence such as Particle swarm optimization.

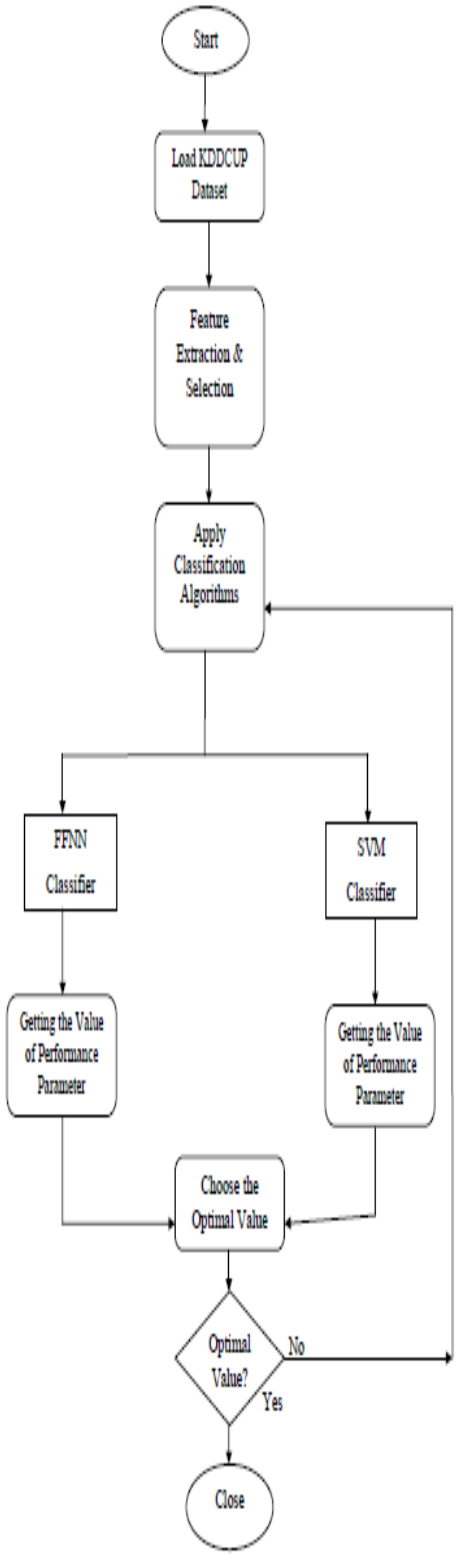

Figure 3: Proposed model for network based intrusion detection system.

In this paper our proposed model compares with the other existing techniques and gives us the better results for this system.

There are some steps we have to follow to implement this system are following: -
Step 1- begin the intrusion detection system.
Step 2- Upload the KDDCUP 99 dataset which is combination of normal and abnormal dataset.
Step 3- Select the feature for the experimental process.
Step 4- Apply the NIDS classification techniques with features.
Step 5- After the applied NIDS techniques we get the some performance evaluation parameter.
Step 6- we compare the all performance evaluation parameter values in the terms of their ratio.
Step 7- Finally we compare the all performance parameters value with all IDS techniques and choose the best optimal value.
Step 8- If performance parameter value is not optimal then go to step no. 4
Step 9- finally we end the proposed IDS system.

IV EXPERIMENTAL RESULT ANALYSIS

In this dissertation we perform experimental process of proposed classification algorithm for intrusion detection system. The proposed method implements in mat lab 7.14.0 and tested with very reputed data set KDDCUP 99 Dataset.

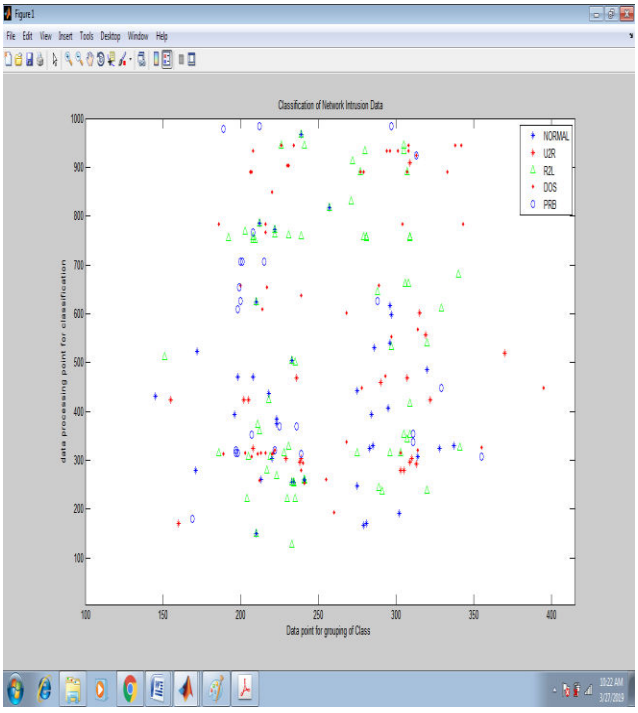

Figure 4: This picture shows that the experimental solution for the input value is 0.15 and the method is support vector machine.

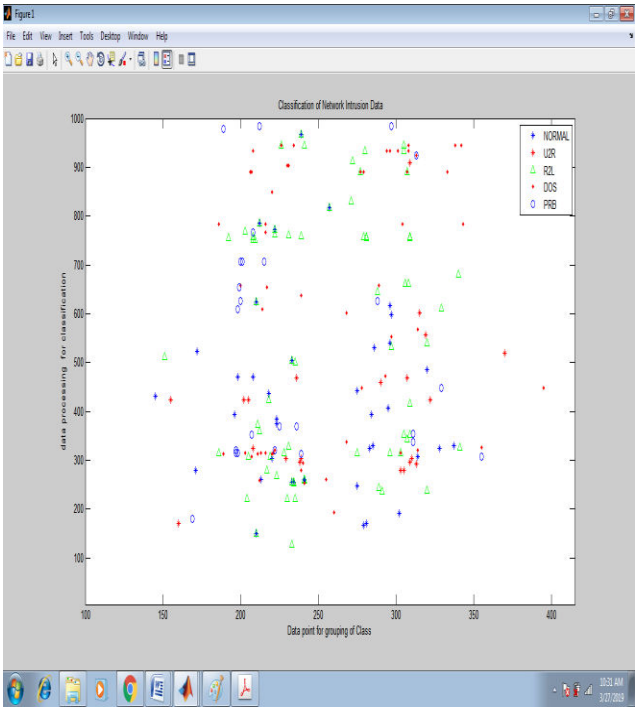

Figure 5: This picture shows that the experimental solution for the input value is 0.70 and the method is support vector machine.

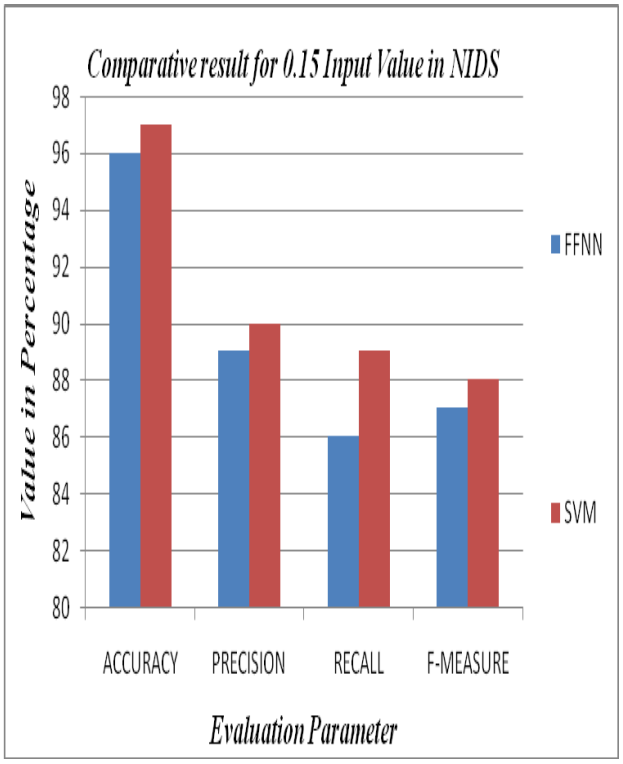

Figure 6: Shows that the comparative result graph for the input value i.e. 0.15.

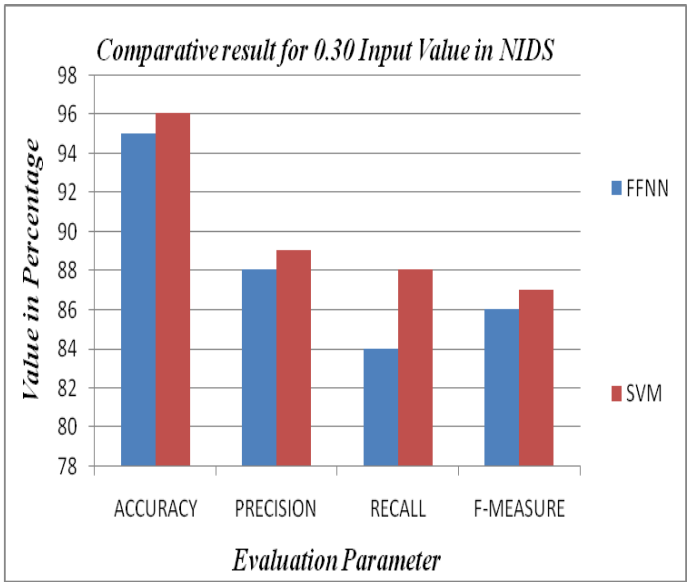

Figure 7: Shows that the comparative result graph for the input value i.e. 0.30.

V CONCLUSIONS AND FUTURE SCOPE

The current scenario of intrusion detection system suffered from detection rate and false alarm generation, the problem of detection and false alarm generation arise due to large features attribute of intruder file. A great advantage of hybrid method is without learning of parameter work a complete system and reduces feature of anomaly file. In this paper we proposed novel methods for the detection of intrusion using various techniques such as fed forward neural network and support vector machines. Our proposed methods also enhanced the detection ratio of intrusion detection and classified data. In future we also reduce the computational time of proposed algorithm and we also focus with some feature reduction techniques for the real time system or on demand system.

REFERENCES: -

[1] Zheni Stefanova, Kandethody Ramachandran, "Network Attribute Selection, Classification and Accuracy (NASCA) Procedure for Intrusion Detection Systems", IEEE 2017. pp 1-7.

[2] Malek Al-Zewairi, Sufyan Almajali, 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.

[3] Sivasangari Gopal, Sathya M, "A Feature Selection for Intrusion Detection System Using a Hybrid Efficient Model", International Journal of

Scientific Research in Computer Science, Engineering and Information Technology, 2018. pp 1917-1929.

[4] Mahmood Sharif, Jumpei Urakawa, Nicolas Christin, Ayumu Kubota, Akira Yamada, "Predicting Impending Exposure to Malicious Content from User Behavior", In Proceedings of 2018 ACM SIGSAC Conference on Computer & Communications Security, 2018. pp 1487-1501.

[5] Win, Thu Yein, Tianfield, Huaglory, Quentin Mair, "Big Data Based Security Analytics for Protecting Virtualized Infrastructures in Cloud Computing", IEEE Transactions on Big Data (99), 2017. pp. 1-15.

[6] Ziyun Zhu, Tudor Dumitras, "ChainSmith: Automatically Learning the Semantics of Malicious Campaigns by Mining Threat Intelligence Reports", IEEE 2016, pp 1-15.

[7] Kasun Amarasinghe, Milos Manic, "Improving User Trust on Deep Neural Networks based Intrusion Detection Systems", Accepted version of the paper appearing in the proceedings of the 44th Annual Conference of the IEEE Industrial Electronics Society, 2018. pp 1-8.

[8] Jen-Li Liao, Kuan-Cheng Lin, Jyh-Yih Hsu, "Botnet detection and feature analysis using Back propagation neural network with bio-inspired algorithms", Int. J. Cognitive Performance Support, Vol. 1, No. 2, 2018, pp 132-142.

[9] Rashidah Funke, Olanrewaju, Burhan Ul Islam Khan, Athaur Rahman Najeeb, Ku Nor Afiza Ku Zahir, Sabahat Hussain, "Snort-Based Smart and Swift Intrusion Detection System", Indian Journal of Science and Technology, Vol 11, 2018. pp 1-9.

[10] Xiao Wang, Quan Zhou, Jacob Harer, Gavin Brown, Shangran Qiu, Zhi Dou, John Wang, Alan Hinton, Carlos Aguayo Gonzalez, Peter Chin, "Deep learning-based classification and anomaly detection of side-channel signals", Proc. of SPIE, 2018. pp 1-9.

[11] Hossam Faris, Alao M. Al-Zoubi, Ali Asghar Heidari, Ibrahim Aljarah, Majdi Mafarja, Mohammad A. Hassonah, Hamido Fujita, "An Intelligent System for Spam Detection and Identification of the most Relevant Features based on Evolutionary Random Weight Networks", Information Fusion (2018), pp 1-28.

[12] Kasun Amarasinghe, Kevin Kenney, Milos Manic, "Toward Explainable Deep Neural Network based Anomaly Detection", IEEE 2018, pp 1-8.

[13] Gavin Watson, "A Comparison of Header and Deep Packet Features when Detecting Network Intrusions", 2018, pp 1-10.

[14] Ahmed Elsherif, "Automatic Intrusion Detection System Using Deep Recurrent Neural Network Paradigm", JISCR, 2018. pp 28-41.

[15] Ruby Sharma, Sandeep Chaurasia, "An Integrated Perceptron Kernel Classifier for Intrusion Detection System", I. J. Computer Network and Information Security, 2018, pp 11-20.

[16] Shelly Xiaonan Wu and Wolfgang Banzhaf, "The Use of Computational Intelligence in Intrusion Detection Systems: A Review," Applied Soft Computing, 2010, pp. 2-42.

[17] S. Revathi and Dr. A. Malathi, "A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion Detection," IJERT., 2013, pp. 1848-1853.

[18] Chien-Yuan Chiu, Brijesh Verma, "Multi-Objective Evolutionary Algorithm Based Optimization of Neural Network Ensemble Classifier," 978-1-4799-5255-7/14, 2014 IEEE. pp. 1-5.

[19] Changsheng Xiang, Yong Xiao, Peixin Qu, Xilong Qu, "Network Intrusion Detection Based on PSO-SVM," TELKOMNIKA Indonesian Journal of Electrical Engineering Vol.12, No.2, February 2014, pp. 1502-1508.

[20] Feras N. Al-Obeidat, El-Sayed M. El-Alfy "Network Intrusion Detection Using Multi-Criteria PROAFTN Classification" IEEE, 2014. Pp 1-5.

[21] V. Engen, J. Vincent, and K. Phalp "Enhancing network based intrusion detection for imbalanced data" Int. J. Knowl.-Based Intell. Eng. Syst., vol. 12, no. 5–6, pp. 357–367, 2008.

[22] S. T. Powers and J. He"A hybrid artificial immune system and self organizing map for network intrusion detection" Inf. Sci., vol. 178, no. 15, pp. 3024–3042, 2008.

[23] K. Shafi, T. Kovacs, H. A. Abbass, andW. Zhu "Intrusion detection with evolutionary learning classifier systems" Nat. Comput., vol. 8, no. 1, pp. 3–27, 2009.