An Empirical Study on Intrusion Detection System Using Classifier and Evolutionary Algorithms

Mr. Deepak Kumar Rathore
Assistant Professor
Dept. of CSE, LNCT, Bhopal (M.P.)
rathore.rath@gmail.com

ABSTRACT
The rapid increase in the internet speed and data transfer rates urged companies through all over the world to fully shift to dependent network data systems, especially after noticeable increase in the capacity of data storage devices. In this paper we discuss about the comparative study of malware detection techniques for the hybrid model with performance evaluation of on the basis of feature reduction techniques.

Keywords:- Intrusion Detection System (IDS), KDDCUP, RBF, Support Vector Machines (SVM), Genetic Algorithm (GA).

INTRODUCTION

Intrusion Detection Systems is a mechanism, which protects resources and data from unauthorized access, misuse, and malicious intrusions in a distributed computing environment [4]. The goal of the IDS is to detect violations in an information system. Traditionally, IDS divided into two kinds such as misuse detection and anomaly detection [3]. The goal of Intrusion Detection is to identify all the proper attacks and negatively identify all the non-attacks. Most of the contemporary IDSs employ a misuse based detection approach, wherein the network attacks are identified by using predefined attack signatures. Although misuse based detection approach provides an effective defence against known attacks, it fails to detect novel and unknown attacks [1].

Here figure 1, 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.

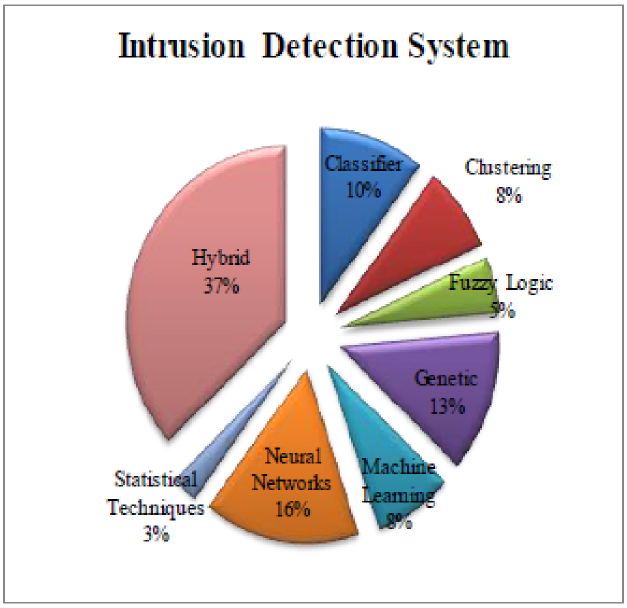

Fig 1: the percentage distribution of the number of papers under various IDS approaches.

The above diagram shows the Hybrid approaches improves the accuracy of the IDS when compared to single approaches. Results from the different individual systems are combined to provide more accuracy and reliability. Researchers are focusing on hybrid methodology for developing the IDS as it can combine the advantages of two algorithms. Here figure 2. shows the classification family of intrusion detection system in detail.

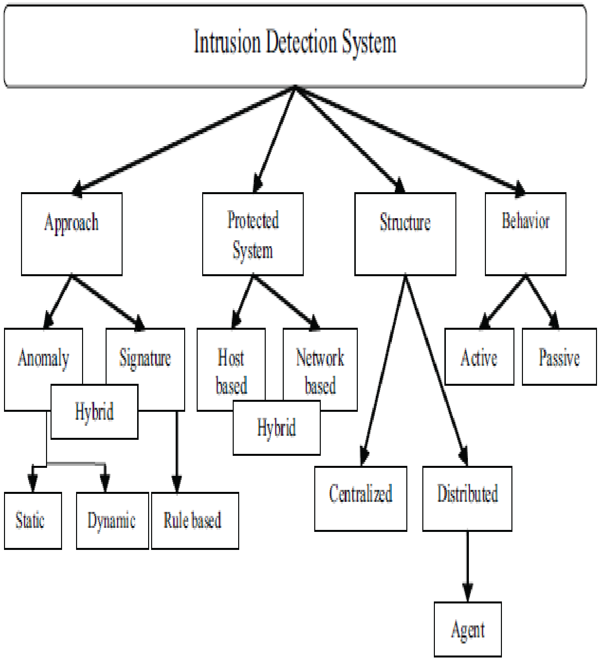

Fig 2. Classification of Intrusion Detection System.

II COMPARATIVE STUDY OF VARIOUS INTRUSION DETECTION TECHNIQUES

In this section we describe the various intrusion detection techniques with compare their performance evaluation on some performance parameter factors such as accuracy, precision and recall, here we using the KDDCUP 99 dataset for the experimental process, the IDS techniques we applied for this are Neural Network, Support vector machines and Genetic Algorithm.

No. of attributes	Techniques	Precision	Accuracy	Recall
42	RBF	90.24	85.22	85.26
	SVM	91.23	86.89	86.65
	GA	92.35	87.58	87.11
35	RBF	91.65	87.26	85.49
	SVM	92.36	88.57	86.57
	GA	93.48	89.58	87.68

Table 1: Shows that the comparative study for intrusion detection techniques.

No. of attributes	Techniques	Precision	Accuracy	Recall
30	RBF	91.78	86.47	87.89
	SVM	92.69	87.32	88.24
	GA	93.59	88.89	89.77
25	RBF	94.47	89.67	90.24
	SVM	95.25	90.45	91.66
	GA	96.11	91.18	92.48

Table 2: Shows that the comparative study for intrusion detection techniques.

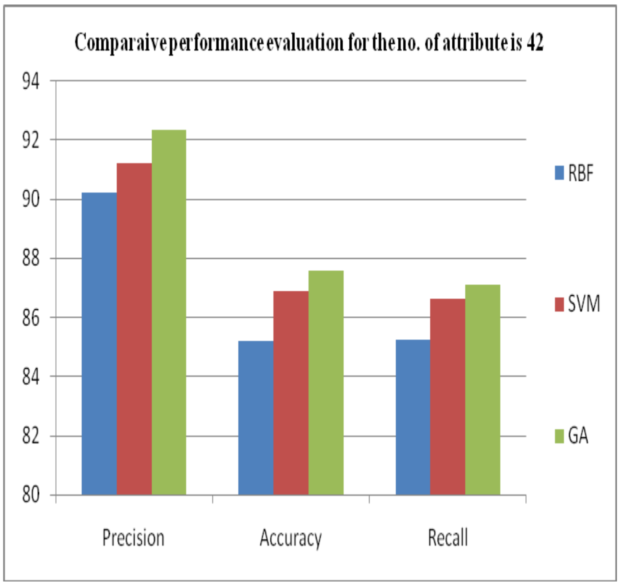

fig 3: The above figure shows that the comparative result analysis for the intrusion detection system using neural network, support vector machines and genetic algorithm, here our results shows that the comparison among the all methods for performance parameter such as precision, recall and accuracy, the number of used attribute are here 42.

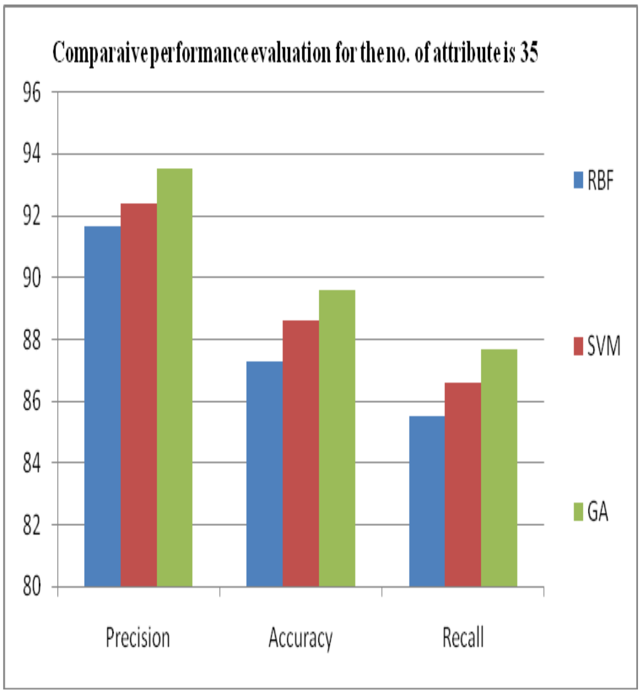

fig 4: The above figure shows that the comparative result analysis for the intrusion detection system using neural network, support vector machines and genetic algorithm, here our results shows that the comparison among the all methods for performance parameter such as precision, recall and accuracy, the number of used attribute are here 35.

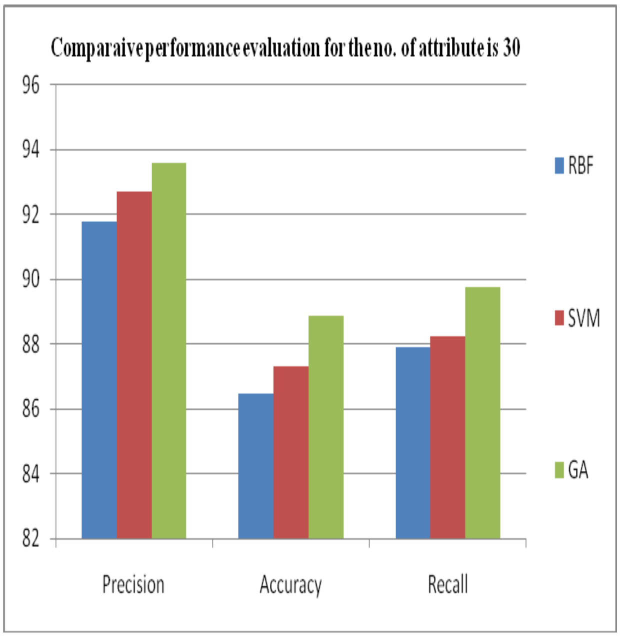

fig 5: The above figure shows that the comparative result analysis for the intrusion detection system using neural network, support vector machines and genetic algorithm, here our results shows that the comparison among the all methods for performance parameter such as precision, recall and accuracy, the number of used attribute are here 30.

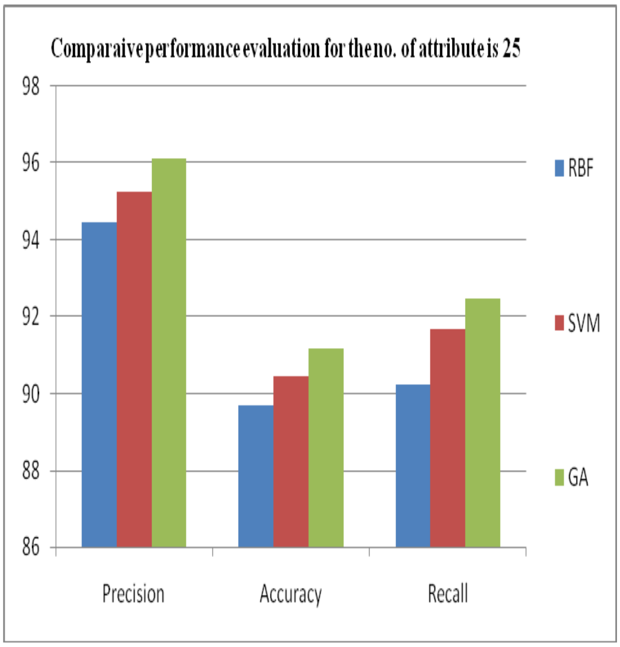

fig 6: The above figure shows that the comparative result analysis for the intrusion detection system using neural network, support vector machines and genetic algorithm, here our results shows that the comparison among the all methods for performance parameter such as precision, recall and accuracy, the number of used attribute are here 25.

III CONCLUSIONS

The IDS is tasked with monitoring and analyzing network activity to differentiate between normal and anomalous activities, for the experimental process we use the common dataset used for IDS developments and testing is the KDD99 dataset which divided in the category normal and abnormal datasets. In fact computers are in tremendous need for an efficient and powerful security policy to secure the information system and to prevent attackers from destroying it. Currently, we are facing an enormous growth of malicious code signature, cybercrimes and threats which can put the security administrator in very critical situations. The objective of this paper to study and compare various intrusion detection algorithms and techniques for the false detection and improve the performance of such system.

REFERENCES:-

[1] Basant Subba , Santosh Biswas, Sushanta Karmakar, “A Neural Network Based System for Intrusion Detection and Attack Classification,” 978-1-5090-2361-5/16, IEEE 2016. pp. 1-6.

[2] Gaby Abou Haidar and Charbel Boustany, "High Perception Intrusion Detection Systems Using Neural Networks," IEEE, 2015, pp. 497-501.

[3] SHEN Li, FENG Lin, "An Efficient Architecture for Network Intrusion Detection Based on Ensemble Rough Classifiers," The 8th International Conference on Computer Science & Education (ICCSE 2013) April 26-28, 2013. Colombo, Sri Lanka. pp. 1411-1415.

[4] James Brown, Mohd Anwar, Gerry Dozier, "An Evolutionary General Regression Neural Network Classifier for Intrusion Detection," 978-1-5090-2279-3/16, IEEE 2016. pp. 1-5.

[5] Shi-Jinn Horng, Ming-Yang Su, Yuan-Hsin Chen, Tzong-Wann Kao, Rong-Jian Chen, Jui-Lin Lai and Citra Dwi Perkasa, "A novel intrusion detection system based on hierarchical clustering and support vector machines," Elsevier, 2011, pp. 306-313.

[6] Asaf Shabtai, Uri Kanonov and Yuval Elovici, "Intrusion detection for mobile devices using the knowledge-based, temporal abstraction method," The Journal of Systems and Software, 2010, pp. 1524–1537.

[7] Gaby Abou Haidar and Charbel Boustany, "High Perception Intrusion Detection Systems Using Neural Networks," IEEE, 2015, pp. 497-501.

[8] Hachmi Fatma, Limam Mohamed, "A two-stage technique to improve intrusion detection systems based on data mining algorithms," 978-1-4673-5814-9/13, IEEE 2013. pp. 1-6.

[9] Adil Fahad, Zahir Tari, Ibrahim Khalil, Ibrahim Habib, Hussein Alnuweiri, "Toward an efficient and scalable feature selection approach for internet traffic classification," Computer Network, Elsevier ltd. 2013. pp. 1-18.

[10] D.P.Gaikwad and Ravindra C. Thool, "Intrusion Detection System Using Bagging Ensemble Method of Machine Learning," IEEE, 2015, pp. 291-295.

[11] D.P.Gaikwad and Ravindra C. Thool, "Intrusion Detection System Using Bagging Ensemble Method of Machine Learning," IEEE, 2015, pp. 291-295.

[12] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," Proceedings of the 2009 IEEE Symposium on computational intelligence in security and defense applications. pp. 1-6.

[13] Feng Du, "An Effective Pattern Matching Algorithm for Intrusion Detection," 2012 International Conference on Computer Science and Electronics Engineering, IEEE. pp. 34-38.

[14] Álvaro Herrero, Marti Navarro, Emilio Corchado and Vicente Julian, "RT-MOVICAB-IDS: Addressing Real-Time Intrusion Detection," Elsevier ltd. 2013, pp. 1-24.

[15] Bharanidharan Shanmugam and Norbik Bashah Idris, "Hybrid Intrusion Detection Systems (HIDS) using Fuzzy Logic," Intrusion Detection Systems, 2011, pp. 1-21.

[16]S. Saravanakumar, Umamaheshwari, D.Jayalakshmi, R.Sugumar, "Development and Implementation of Artificial Neural Networks for Intrusion Detection in Computer Network," IJCSNS, 2010, pp. 271-275.

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

[18] 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.

[19] Karim Ali,David Hasler,Franc¸ois Fleuret "FlowBoost Appearance Learning from Sparsely Annotated Video" 2011 IEEE.

[20] Shi-Jinn Horng, Ming-Yang Su, Yuan-Hsin Chen, Tzong-Wann Kao, Rong-Jian Chen, Jui-Lin Lai and Citra Dwi Perkasa, "A novel intrusion detection system based on hierarchical clustering and support vector machines," Elsevier ltd. 2011, pp. 306-313.