A Review on Performance Comparison of Artificial Intelligence Techniques Used for Intrusion Detection

Navaneet Kumar Sinha[1], Gulshan Kumar[2] and Krishan Kumar[3]
[1]*Department of Computer Science & Engineering,*
Punjab Institute of Technology, Kapurthala, Punjab, India
[2]*Department of Computer Applications, SBS State Technical Campus, Ferozepur, Punjab, India*
[3]*Department of Computer Science & Engineering, SBS State Technical Campus, Ferozepur, Punjab, India*
E-mail:[1]navaneetsinha@gmail.com, [2]gulshanahuja@gmail.com, [3]k.salujasbs@gmail.com

***Abstract*—In the current era of Internet, network security technology has become crucial in protecting the computing infrastructure on the network. The number of network attacks has risen, leading to the essentials of network intrusion detection systems (IDS) to secure the network. Optimizing the performance of IDS becomes an important open problem which receives more and more attention from the research community. In this work, implementation of Artificial intelligence based techniques in IDS is popular in the research community. The network traffic can be classified into normal and anomalous in order to detect intrusions. There are several classification techniques available to detect the attacks. Researchers compare these techniques and try to identify the best techniques for the different attack category. This paper presents a review on comparison of these techniques.**

Keywords: Intrusion Detection, Artificial Intelligence, KDDCup, Data Mining Techniques, Classification

I. INTRODUCTION

This is the era of the Internet and information system in which computing infrastructure and communication resources are shared over the open world of the Internet. However, this inter connectivity between computers also enables malicious users to misuse resources and mount an Internet attack. The continuously growing Internet attacks pose service challenges to develop a flexible, adaptive security oriented methods. Intrusion Detection System (IDS) is one of the most important components being used to detect Internet attacks [1]. Intrusion Detection System (IDS) is placed inside the protected network, looking for potential threats in network traffic and or audit data recorded by a host.

IDS are split into two categories: misuse detection systems and anomaly detection systems. Misuse detection is used to identify intrusions that match known attack scenarios. However, anomaly detection is an attempt to search for malicious behaviour that deviates from established normal patterns [2].

In order to detect the intrusion, various approaches have been developed and proposed [1]. The major techniques are Statistics based IDS, the behaviour of the system is represented by a random view point. On the other hand, knowledge based IDS techniques try to capture the claimed behaviour from available system data (protocol specification, network traffic instances, etc.). AI based IDS techniques involves establishment of an explicit or implicit model that allows the patterns to be categorized. In this paper our interest is in AI based IDS techniques.

Many authors have divided AI based techniques into different classes [1] [3]: Decision tree based techniques, Rule based techniques, Data Mining techniques, machine learning techniques and clustering techniques. These techniques are further classifies in different categories. Major Data mining techniques are fuzzy logic and Genetic algorithm based techniques. Major Machine learning techniques are Neural network (NN), Bayesian network, Markov model, Support Vector machine (SVM) and Clustering techniques etc.

In many papers the above techniques are tested on a dataset. They analysed the performance of the technique and also compared some techniques in term of different attacks [4]. In most of the papers KDDCup99 [4] [5] datasets are used to perform the test of AI technique. Because the KDD data set is widely used by researchers.

The KDD cup 1999 dataset set is based on the DARPA98 dataset which was built by the Defense Advanced Research Projects Agency (DARPA) in 1998 during the DARPA98 IDS evaluation program. KDD99 dataset is openly available on [5]. Two types of files KDD Training set and KDD Test set are available for training and testing purpose. The dataset has 41 attributes and one class attribute. Various researchers have used different feature reduction techniques to select most relevant and ir-redundant features of a dataset of intrusion detection system [6]. Because, presence of irrelevant and redundant features degrades the accuracy of results and increases the computational overhead.

The dataset is categories in five classes, four attack classes and a normal. Attacks fall into four main categories [5]:

1. DOS: denial-of-service, e.g., syn flood.
2. R2L: unauthorized access from a remote machine, e.g., guessing password.
3. U2R: unauthorized access to local superuser (root) privileges, e.g., various “buffer overflow” attacks.

4. Probing: surveillance and other probing, e.g., port scanning.

In this paper, we present the performance comparison of different AI techniques (ANN, Classification, clustering, SVM etc.) performed by many researchers. We also compare their work on the basis of different criteria such techniques used for comparison, dataset used, metrics evaluated, best performance technique, advantage, disadvantage etc.

The rest of this paper is organized as follows: In section II Literature Survey is discussed. In section III we present a table of their work on the basis of different criteria. Finally, section IV shows the summary.

II. LITERATURE SURVEY

Mukkamala and Sung (2003) investigated and compared the performance of IDS based on support vector machines (SVM), artificial neural network (ANN), multivariate adaptive regression splines (MARS) and linear genetic programs (LGPs) [7]. For experiment they used DARPA dataset on 5-class classification. They perform experiments on two randomly generated separate datasets of size 5092 and 6890 for training and testing. Through the variety of experiments they found that, with appropriately chosen population size, program size, crossover rate and mutation rate, LGPs outperform other techniques in term of detection accuracy at the expense of time. They also conclude comparative performance between others. MARS is superior to SVMs in respect to classifying U2R and R2L attacks. SVMs outperform ANNs in respect of scalability, training and running time, and prediction accuracy. Resilient back propagation achieved the best performance among the neural networks in terms of accuracy and training. But performance comparisons are based on very least performance metrics (detection accuracy, training time and testing time).

Nguyen and choi (2008) evaluated the performance of a set of classifiers on KDD dataset and based on the result they choose best algorithm for each attack category [8]. They also proposed two classifier algorithm selection models. They performed experiments on weka machine learning tool and KDD99 dataset. Ten widely used classifier algorithms BayesNet, NaiveBayes, J48 (C4.5 Decision Tree), NBTree, Decision Table, JRip (RIPPER), OneR, MLP (Multilayer Perceptron), SMO and LBk are evaluated on the basis of four attacks categories (DoS, Probe, U2R and R2L). To compare these classifiers, they used TP (True Positive) and FP (False Positive) of each algorithm. They also measured AA (average accuracy) and TT (training time) performance metric.

The advantage of their work is the comparative analyses are based on attack categories. Because no single algorithm could detect all attack categories with high detection rate and low false alarm, the result shows that for a given attack category, certain algorithms demonstrate superior performance compared to others. The best algorithms for each attack categories are identified as: JRip for DoS and Probe, Decision table for U2R and OneR for R2L. On the basis of this result a parallel model for classifier selection (JRip, Decision Table and OneR) is proposed in this paper. They also proposed a model for real time application classifier selection (J48, BayesNet and OneR).

Sadoddin and Ghorbani (2007) conducted blind experiments of unsupervised techniques on KDD99 dataset to analyze the performance of unsupervised techniques considering their main design choice [9]. In this paper algorithms of the three categories are studied Clustering techniques, Unsupervised SVM and K-Nearest-Neighbor. Clustering techniques include K-means, C-means, EM, Self-organizing Map (SOM), Y-means and Improved Competitive Learning Network (ICLN). The evaluation of the algorithm in this paper is done with various distributions of training and testing datasets. To carry out experiment different tools for different algorithm are used, Fuzzy Clustering and Data Analysis Toolbox for C-means, SOM Toolbox for SOM, LIBSVM library for One-Class SVM and Weka tool for EM. For Clustering techniques two sets of experiment are performed. In the first set performance of each clustering technique evaluated with two labeling heuristics, count-based and distance-based. At second set of experiment, the performance of each clustering technique is evaluated in direct versus indirect mode. In the result they concluded that direct-based is on the average dominant over count-based heuristic in almost all of the clustering techniques. The clustering techniques (Except Y-means) in indirect mode, perform better when trained with Train_8020 (percentage of normal and attack records is 80% and 20%, respectively), while USVM and Y-means perform better when trained with Train_9604. In direct mode, the performance of KNN-based outlier detection schemes decreases as the population of attack data increases in the target dataset. They also highlighted two observations. First, all techniques perform poorly in detecting R2L attack. Secondly, USVM and Y-means are clearly superior over other techniques in detecting U2R attacks. Fuzzy clustering is not suitable for distinguishing normal and abnormal data in intrusion detection because C-means delivers the worst results in almost all experiments. In this paper only unsupervised techniques are discussed and on the basis of very few performance metrics detection rate, false alarm rate and ROC curve.

Kumar and Kumar (2011) performed a set of experiment of supervised classifiers on benchmarked KDD cup 1999 dataset [10]. They analyzed common supervised classifiers used in literature for intrusion detection. Performance of various AI techniques is

compared from different categories viz: Rule based, Tree based, Functions, Lazy, Bayes and Meta. Kumar [4] identified. Some standard performance metrics are F-measure (FM), classification rate (CR), false positive rate (FPR), cost per example (CPE), precision (PR), root mean square error (RMSE), area under ROC curve (ROC), and detection rate (DR). The advantage of this research is that they first identified best classifiers for each attack class in the respective classifier category. Secondly, they compared best classifiers in the respective category to identify overall best classifier for different class attack. Because classifiers are designed by keeping in mind to optimize different criteria so it is very significant to compare classifiers in each classifier category. In this paper, it is concluded that bagged tree-J48 classifier is the best and the stable classifier with the overall correct classification of malicious traffic with minimum CPE, FPR and maximum ROC. It is also found that rule based JRip and Bagged tree-J48 for probe, Bagged tree-J48 for DoS, JRip for U2R and Naïve Bayes, bagged tree-J48 and neural network based MLP for R2L attack class can be better performed classifiers. They also reported that a single classifier cannot detect all the attack classes efficiently and suggested that a set of classifiers might be used to detect different attack classes. It is also observed from these experiments that all supervised classifiers are poor perform in detecting U2R and R2L attack classes.

Sabhnani and Serpen (2003) evaluated the performance of a comprehensive set of machine learning algorithms on four attack categories in the KDD 1999 cup dataset [11]. They selected nine algorithms from the variety of fields: neural networks, probabilistic models, statistical models, fuzzy-neuro system and decision tree. The algorithms identified are: Multilayer perceptron (MLP), Gaussia classifier (GAU), K-means clustering (K-M), Nearest cluster algorithm (NEA), Incremental radial basis function (IRBF), Leader algorithm (LEA), Hypersphere algorithm (HYP), Fuzzy ARTMAP (ART) and decision tree (C4.5). The classifiers are compared with the performance metric probability of detection (PD) and false alarm rate (FAR). The all classifiers tested on KDD data sets offered an acceptable level of misuse detection performance for only two attack classes Probe and DoS (poor for U2R and R2L). The results of the experiment show that for a given attack category, certain algorithms demonstrate superior detection performance compared to others. Finally, they concluded that MLP performs the best for probing, K-M for DoS as well as U2R, and GAU for R2L attack categories. On the basis of this conclusion sabhnani and Serpen [11] proposed a multi-classifier model which is able to perform best for all four attack classes Probe, DoS, U2R and R2L.

The multi-classifier model consists of different algorithms best for each attack category, as sub-classifiers: MLP for detection of probe attack, K-means for DoS as well as U2R attacks, and GAU for R2L attack.The Performance of this model is compared with KDD cup Winner, KDD Cup RunnerUp and Aggarwal and Joshi algorithms. The Multi-classifier model showed significant improvement in detection rate. The problem with this comparison is that the performance measured with very few performance metrics (PD, FAR and cost per example. And the other is the selection of classifiers to be compared was not follow standard.

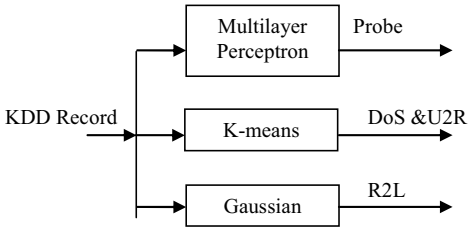

Fig. 1 Multi-Classifier Model

Wang *et al*. (2010) proposed a new neural network based detection approach called FC-ANN (fuzzy clustering based artificial neural network) [2]. The new FC-ANN approach is compared with selected well known classification approaches such as Decision tree, Naïve Bayes and BPNN. Performance metrics selected for this comparison are average accuracy, training time, precision, recall and F-value. The resulting analysis is critically done on several aspects. In terms of detection precision and detection stability FC-ANN outperforms BPNN and the other methods such as decision tree and NaïveBayes. In terms of average accuracy decision tree performs best and, also for probe and DoS attack class. Especially in case of low frequent attack classes U2R and R2L the new proposed approach FC-ANN gives significant improvement in detection precision and detection stability. The comparison is done for each attack class, but very less performance metrics are used.

Panda and Patra (2008) presented the comparison of three well known techniques such as ID3, J48 and Naïve Bayes [12]. The performance of classifiers is evaluated based on 10-fold cross validation test using KDD99 data set. The comparison is done with respect to performance metrics average accuracy, error rate, precision-recall, F-value, FPR, Area under the ROC curve, Kappa statistics and time taken to build the model. It is observed from all analysis that Naïve Bayes perform better than other two decision tree algorithms. However, decision trees are robust in detecting new intrusions, in comparison to the Naïve Bayes.

Kalyani and Lakshami (2012) presented the comparison of classification techniques such as Naive Bayes, J48, OneR, PART and RBF Network using NSL-KDD dataset [13]. The advantages of NSL-KDD dataset over KDDCUP'99 are also discussed. Several performance metrics are discussed such as TPR, FPR, RMSE, accuracy and time. J48 has higher accuracy, but

they found PART as best algorithm because it takes lesser time, has lowest average error and accuracy is followed by J48.

Chauhan *et al*. (2013) presented the comparison of top ten classification algorithms: BayesNet, Logistic, SGD, IBK, JRip, PART, J48, Random Forest,Random Tree and REPT Tree [14]. To evaluate the algorithms 10-fold cross validation test is used. In experiment 20% of NSL-KDD data set is used and classifiers are tested on WEKA, a well known machine learning tool. The performance of all the classifiers is compared based upon accuracy, specificity and time. This study shows that decision tree classifiers are best at classifying the intrusions. Out of which Random Forest has outperformed with respect to the accuracy, specificity and sensitivity, whereas IBK consumes less time compared with others.

Gharibian and Ghorbani (2007) presented a comparison of supervised probabilistic and predictive machine learning techniques for intrusion detection [15]. Two probabilistic techniques NaiveBayes and Gaussian and two predictive techniques, Decision Tree and Random Forests are employed. In implementation, training data sets with different attack population and percentage are used to evaluate classifiers. Three different population categories used are 8020 (80% normal and 20% attack), 8416 and 8812. In the maximum detection rate analysis, Decision Trees and Random Forests show good results in detecting DoS, while Gaussian and NaiveBayes show better results in other attack categories. Other metrics analysis as sensitivity standard deviation and mean are also presented in this paper. Based on the results obtained in the paper [15], probabilistic techniques show more robustness than predictive techniques when trained using different training data sets. It has also been observed that probabilistic techniques show better detection rate in the data that has less samples such as R2L, U2R and Probe. While for DoS that has more samples, the predictive techniques outperform the probabilistic techniques.

Jalil *et al*. (2010) evaluated the performance of Decision tree (J48) classification algorithm and compared it with Support Vector machine (SVM) and Neural Network (NN) algorithms in term of accuracy, detection rate, false alarm rate and accuracy for four categories of attack under different percentage of normal data [16]. As summarized, from these four categories of attack (Probe, DoS, U2R, and R2L), Decision Tree (J48) has shown excellent results that outperform Neural Network and Support Vector Machines.

D'silva and Vora (2013) discussed three different clustering algorithms, namely K-Means Clustering, Y-Means Clustering and Fuzzy C-Means Clustering [17]. The comparison is made by taking into account various criteria like the performance, efficiency, detection rate, false positive rate, purity of cluster, etc. Among these Fuzzy C-Means clustering can be considered as an efficient algorithm for intrusion detection since it allows an item to belong to more than one cluster and also measures the quality of partitioning. Advantage and disadvantage of all three algorithms are discussed, but separate test for comparison purpose is not done.

Srinivasulu *et al*. (2009) also presented a comparison of widely used classification algorithms CART (Induction Decision Tree), Naïve Bayes and Artificial Neural network [18]. The test is performed on KDDCup99 data set in WEKA tool. All the three classifications, Dataset and WEKA tool are also discussed in brief. Performance is compared with TPR, FPR, Area under curve ROC, precision and recall, and all metrics are also discussed. The performance of the Induction tree (CART) method and ANN methods are better than the NB classifier. But the time taken is more for ANN than other classifiers.

Osareh and Shadgar (2008) compared the efficiency of machine learning methods in intrusion detection system, including artificial neural network and support vector machine [19]. They compare the accuracy, detection rate, false alarm rate for 4 attack types. In comparison, the research applies different normal data proportion for training and test, finally get one average value, and expect to obtain more objective results. In this paper, it is found that SVM is superior to NN in detection; in false alarm rate and in accuracy for Probe, Dos and U2R and R2L attacks, while NN could outperform the SVM only in accuracy.

Reddy *et al*. (2011) also presented a survey of various data mining techniques that have been proposed towards the enhancement of IDSs [20]. They also discussed the various AI techniques used in brief and also mentioned the drawbacks of IDS.

MeeraGandhi *et al*. (2010) also evaluated the performance of a set of classifier algorithms of rules (JRIP, Decision Tabel, PART, and OneR) and trees (J48, RandomForest, REPTree, NBTree) [21]. The algorithms are evaluated on KDD dataset. To compare the classifiers, TP (True positive) and FP (False Positive), Prediction Accuracy and learning time to build the model in seconds for each algorithm are considered. The results indicate that the C4.5 decision tree Classifier J48 outperforms in prediction than Rules. PART classifier, the Computational Performance differs significantly.

Neelima *et al*. (2014) presented a survey of the various data mining techniques that have been proposed towards the enhancement of IDSs [22]. Different data mining techniques used in intrusion detection are discussed in this paper.

Singh and Bansal (2013) presented the comparison of Multilayer Perception, Radial Base Function, Logistic Regression and Voted Perception [23]. They concluded that Multilayer Perceptron feed forward neural network has highest classification accuracy and lowest error rate as compared to other neural classifier algorithm network.

TABLE I SURVEY OF COMPARISON OF AI TECHNIQUES

S. No.	Paper	AI Techniques	Performance Metrics	Dataset	Advantage/Disadvantage	Best Techniques
1	Mukkamala and Sung [7]	MARS, SVM, LGP, ANN (RP, SCG, OSS)	DR, Training and Testing Time	DARPA	Anomaly Detection. Very least performance metrics	LGPs outperforms in term of accuracy at the expense of time.
2	Nguyen and Choi [8]	BayesNet, Naïve Bayes, J48, NBTree, Decesion Table, Jrip, OneR, MLP, SMO, LBK	TP, FP, Average Accuracy, Training Time	KDD99	Proposed a New Model for Real Time	JRip for DoS and Probe, Decision table for U2R, OneR for R2L in term of DR
3	Sadoddin and Ghorbani [9]	Clustering-K means, C-means, EM, SOM, Y-mean & ICLN, USVM, KNN	DR, FPR, ROC Curve	KDD99	Different tools for different algorithms used	
4	Kumar and Kumar [10]	RForest, RTree, NBTree, J48, Simple CART, Jrip, Decision Tree, NaïveBayes, BayesNet, SMO, MLP, RBFNetwork, LibSVM, IB1, LBK, K-star, Bagging, Boosting & Random SubspaceTree.	CR, CPE (Cost Per Example), RMSE, Precision (PR), ROC, AvG FM, Avg. DR, FPR	KDD99	Comparative Analysis of Techniques in each category as well as comparison b/w best classifiers of each category.	Bagged tree-J48 for overall correct classification, JRip and Bagged tree-J48 for probe, Bagged tree-J48 for DoS, JRip for U2R, Naïvebayes, bagged tree-J48 and MLP for R2L.
5	Sabhnani and Gerphen [11]	MLP, GAU, K-Mean, NEA, RBF, LEA, HYP, Fuzzy ARTMAP, C4.5	Detection Rate, FAR, CPE	KDD99	Multiple simulation tools are used. Less metrics selected. Proposed a MultiClassifier Model.	MLP for probing, K-M for DoS as well as U2R, and GAU for R2L.
6	Wang *et al*. [2]	Decision Tree, Naïve Bayes, BPNN, FC-ANN (proposed Method)	Precision, Recall, F-value, Avg. Accuracy, Training time,	KDD99	Evaluation for each type of Attacks and proposed an ANN based Approach.	Decision tree, FC-ANN in term of precision and recall, FC-ANN perform better for U2R and R2L
7	Panda and Patra [12]	Decision Tee(ID3 and J48) and Naïve Bayes	Avg. Accuracy, error rate, PR, ROC Area, Kappa statistics and time, F-Value, FPR	KDD99	Only three Classifiers are compared. 10-cross validation test performed	Naïve Bayes. Decision trees are robust in detecting new intrusions
8	Chauhan *et al*. [14]	BayesNet, Logistic, SGD, IBK, JRip, PART,J48, Random Forest, Random Tree and REPT Tree	Accuracy, sensitivity, specificity and time	NSL-KDD	The different training set is not used 10-fold cross validation is performed	Random Forest
9	Gharibian and Ghorbani [15]	NaiveBayes, Gaussian, Decision Tree and Random Forests	Detection rate, RMSE, standard deviation	KDD99	very few metrics are selected only four techniques are compared	Naïve Bayes and GAU are for DoS. Decision Tree and Random Forests for other attacks
10	Jalil *et al*. [16]	Detection Tree(J48), Support vector machine (SVM) and Neural Network (NN)	Avg. Accuracy, DR, FAR and accuracy for four attack classes.	KDD99	Different percentages of normal data are used. Performance in term attack classes. But only three techniques are compared.	Decision Tree (J48)
11	D'silva and Vora [17]	K-Means, Y-Means and Fuzzy C-Means Clustering	Efficiency, DR, FPR, purity of cluster	NA	Only clustering techniques are compared. No test result presented	Fuzzy C-Means
12	Srinivasulu *et al*. [18]	CART (Induction Decision Tree), Naïve Bayes and Artificial Neural network	TPR, FPR, F-measure, ROC Area, precision and recall	KDD99	Only three of classifiers are compared. Performance is not measured in terms of 4 attack categories	CART and Naïve Bayes
13	Osareh and Shadgar [19]	ANN and SVM	accuracy, DR, FAR	KDD99	Only ANN Technique and SVM is compared	SVM best in detection
14	MeeraGandhi *et al*. [21]	JRIP, Decision Tabel, PART, OneR, J48, RandomForest, REPTree, NBTree	TP, FP, Prediction Accuracy and Time to build the model	KDD99	rules and tree based approach are compared	C4.5 (J48)
15	Singh and Bansal [23]	RBF Network, Voted perceptron, Logistic Regression, Multilayer perceptron	CCI, ICI, KAPPA STATISTiCS, MAE, RMSE, RAE, RRSE, Time	NSL-KDD	Only ANN Techniques	Multilayer Perceptron

III. SUMMARY

The security is the primary concern in every field such as to prevent data from attacks and detect intruder. This paper has presented a survey of comparison of the various AI techniques that have been proposed towards the enhancement of IDSs. We presented literatures from the various papers and from the literature survey, it is analyzed that no single classification technique is sufficient to detect all four attack categories. Some researchers purposed to use the Multi classifier model to better perform for all attack classes. In most of the paper very few selected type of techniques are compared, there should follow a standard selection of techniques for comparing the performance. The NSL-KDD dataset has advantage over KDD99 but more researches are used KDD99 dataset.

REFERENCES

[1] Kumar *et al*.. "The use of artificial intelligence based techniques for intrusion detection: a review." *Artificial Intelligence Review*, vol. 34, no. 4, pp. 369-387, Dec. 2010.

[2] Wang *et al*. "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering." *Expert Systems with Applications,*vol. 37, no. 9, pp. 6225-6232, Sept. 2010.

[3] Chauhan *et al*. "Survey on data mining techniques in intrusion detection." *International Journal of Scientific & Engineering Research.vol.2 no. 7* ,July 2011.

[4] Tavallaee *et al*. "A detailed analysis of the KDD CUP 99 data set," *In Proceedings of the second IEEE Symposium on Computational Intelligence for Security and Defense Applications,* CISDA . pp. 1-6, 2009.

[5] "KDDCup 1999 Dataset". [Available online]: http://kdd.ics.uci.edu/databases/kddcup1999.html/

[6] Ahuja *et al*. "An empirical comparative analysis of feature reduction methods for intrusion detection." *International Journal of Information and Telecommunication Technology (ISSN: 0976-5972)* 1, no. 1, 2010.

[7] Mukkamala and Sung. "A comparative study of techniques for intrusion detection." In *Tools with Artificial Intelligence, Proceedings in 15th IEEE International Conference on*, pp. 570-577. IEEE, 2003.

[8] Nguyen and Choi. "Application of data mining to network intrusion detection: classifier selection model." In *Challenges for Next Generation Network Operations and Service Management*, pp. 399-408. Springer Berlin Heidelberg, 2008.

[9] Sadoddin and Ghorbani. "A comparative study of unsupervised machine learning and data mining techniques for intrusion detection." In *Machine Learning and Data Mining in Pattern Recognition*, pp. 404-418. Springer Berlin Heidelberg, 2007.

[10] Kumar and Kumar. "AI based supervised classifiers: an analysis for intrusion detection." In *Proceedings of the International Conference on Advances in Computing and Artificial Intelligence*, pp. 170-174. ACM, 2011.

[11] Sabhnani and Serpen. "Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context." In *MLMTA*, pp. 209-215. 2003.

[12] Panda and Patra. "A comparative study of data mining algorithms for network intrusion detection." In *Emerging Trends in Engineering and Technology, ICETET'08. First International Conference on*, pp. 504-507. IEEE, July 2008.

[13] Kalyani and Lakshmi. "Performance assessment of different classification techniques for intrusion detection." *IOSR Journal of Computer Engineering, vol. 7* 2, no. 5, Nov. 2012

[14] Chauhan *et al*. "A Comparative Study of Classification Techniques for Intrusion Detection." In *Computational and Business Intelligence (ISCBI), 2013 International Symposium on*, pp. 40-43. IEEE, 2013.

[15] Gharibian and Ghorbani. "Comparative study of supervised machine learning techniques for intrusion detection." In *Communication Networks and Services Research, 2007. CNSR'07. Fifth Annual Conference on*, pp. 350-358. IEEE, 2007.

[16] Jalil *et al*. "Comparison of machine learning algorithms performance in detecting network intrusion." In *Networking and Information Technology (ICNIT), 2010 International Conference on*, pp. 221-226. IEEE, 2010.

[17] D'silva and Vora. "Comparative Study of Data Mining Techniques to Enhance Intrusion Detection." *International Journal of Engineering Research and Applications (IJERA) ISSN* pp. 2248-9622, 2013.

[18] Srinivasulu *et al*. "Classifying the network intrusion attacks using data mining classification methods and their performance comparison." *International Journal of Computer Science and Network Security* vol. 9, no. 6 pp. 11-18, 2009.

[19] Osareh and Shadgar. "Intrusion detection in computer networks based on machine learning algorithms." *International Journal of Computer Science and Network Security (IJCSNS)* vol. 8, no. 11, pp. 15-23, 2008.

[20] Reddy *et al*. "A study of intrusion detection in data mining." In *World Congress on Engineering (WCE)*,vol. 3, pp. 6-8. 2011.

[21] MeeraGandhi *et al*. "Effective network intrusion detection using classifiers decision trees and decision rules." *Int. J. Advanced network and application, Vol. 2,* 2010.

[22] Neelima *et al*. "Leverage Data Mining Techniques in Intrusion detection.", *International Journal of Emerging Technology and Advanced Engineering, vol.4, pp.2 2014.*

[23] Singh and Bansal. "A Survey on Intrusion Detection System in Data Mining." *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET,). Vol. 2, no. 6, June 2013*