IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

Performance Comparison of Multi class SVM, Support Vector Machine, k-NN and Binary Classification for Intrusion Detection

Kumar Parasuraman[1*], A. Anbarasa Kumar[2]

1Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, Tirunelveli, India
[2]Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, Tirunelveli, India

[*]*Corresponding Author: kumarcite@gmail.com,anbumtech08@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 14/Aug/2018, Published: 31/Aug/2018

Abstract — Intrusion detection is a fundamental part of security tools, for example, adaptive security appliances, intrusion detection systems, intrusion prevention systems and firewalls. Intrusion detection systems (IDS) plays a important role in detecting the attacks that occur in the PC or networks. Intrusion detection systems (IDS) are the network security mechanism that monitors network and system activities for malicious action.it become indispensable tool to keep information system safe and reliable. Different intrusion detection methods are used, but their performance is an problem. . Intrusion detection performance depends on accuracy, which needs to enhance to decrease false alarms and to increase the detection rate. Such procedures demonstrate limitations, are efficient for use in large datasets, for example, system, and network data. The intrusion detection system is used to analyzing huge traffic data, therefore efficient classification method is important to overcome the issue. Well-known machine learning techniques, namely, SVM, Multiclass SVM, k-NN, Binary Classification (BC) are applied. These techniques well known because of their capability in Classification. The NSL–knowledge discovery and data mining, dataset is used, which is considered a benchmark in the evaluation of intrusion detection mechanisms. The results indicate that Multiclass SVM outperforms other approaches.

Keywords— Support vector machine SVM, Multiclass SVM, k-NN, Binary Classification, NSL-KDD

I. INTRODUCTION

Intrusion is an extreme issue in security and a prime issue of security breach, because of single instance of intrusion can take or erase information from PC and network system in few seconds. Intrusion can likewise harm system hardware. Moreover, intrusion can cause tremendous misfortunes financially and trade off the IT critical infrastructure, in this way prompting data inadequacy in cyber war. In this way, intrusion detection is critical and its prevention is necessary [9]. Different intrusion detection procedures available, however the exactness remains an issue; accuracy depends on detection and false alarm rate. The issue on exactness should be reduce the false cautions rate and to expand the detection rate. This thought was the stimulus for this research work. In this manner, Support vector machine (SVM), Multi Class SVM, Binary Classification (BC), k-Nearest Neighbors (k-NN) connected in this work; these strategies have been demonstrated successful in their capacity to address the classification problem[13].Intrusion detection mechanism are approved on a standard dataset, KDD. This work utilized the NSL– knowledge discovery and data mining (KDD) dataset, which is an enhanced type of the KDD and viewed as a benchmark in the assessment of intrusion detection methods. The remainder of the paper is organized as detailed below. The related work presented in Section II. The proposed model of intrusion detection to which different machine learning techniques are applied in described in Section III. The implementation and results are discussed in Section IV. The paper is concluded in Section V, which provides a summary and directions for future work. All experiments were implemented in the MATLAB 2015a environment.

II. RELATED WORK

Securing PC and network information is essential for organizations and people in because the fact that compromised information can cause extensive damage. To stay away from such conditions, intrusion detection systems are essential. Recently, extraordinary machine
Learning approaches proposed to enhance the execution of intrusion detection systems [11]. It proposed an intrusion detection framework [14] based on SVM and approved their technique on the NSL– KDD dataset. They guaranteed that

their technique, which has 86.05 % effectiveness rate, was better than different methodologies; however, they did not say utilized dataset statistics, number of training, and testing samples. Moreover, the SVM performance decreases when huge information included, and it is anything but a perfect decision for breaking down tremendous huge network traffic for intrusion detection [18].

It connected a hybrid model of SVM and KPCA with GA to intrusion detection, and their system indicates 90.25% detection rate [15]. They used the KDD CUP99 dataset for the check of their system, but this dataset is characterized by limitations. One illustration is repetition, which makes the classifier biased to every now and again happening records. They applied KPCA for include reduction, and it is limited by the possibility of missing important features because of choosing top percentages of the principal component from the principal space[4],[6]. Moreover, the SVM is not fitting for large data, for example, observing the high bandwidth of the network.

Intrusion detection systems give assistance with detecting, preventing, and resisting unauthorized access [7]. This group classifier method, which is a combination of PSO and SVM [16]; this classifier outperformed different methodologies with 92.90% accuracy. They used the knowledge discovery and data mining 1999 (KDD99) dataset, which has the beforehand specified drawbacks. Moreover, the SVM is not a good choice for huge data analyses, since its execution degrades as data size increases.

It proposed an intrusion detection mechanism in view of hypergraph genetic algorithm (HG-GA) for parameter setting and feature selection in SVM [17]. They guaranteed that their technique outperformed the existing methodologies with a 95% detection rate on NSL– KDD dataset; it hasbeen used for experimentation and approval of intrusion detection systems [19].

The security of network systems is one of the most critical issues in our daily lives, and intrusion detection systems are significant as prime defence techniques [21]. They developed their model based on SVMs, and they tested their model on a KDD CUP 1999 dataset. The results showed an accuracy reaching 89.02%. However, SVMs are not preferred for heavy datasets because of the high computation cost and poor performance.

III. PROPOSED MODEL

The key phases of the proposed demonstrate include the dataset, Pre-processing, classification, and result evaluation. Each phase of the proposed system is important and includes significant impact its execution. The centre focal point of this work is to research the execution of various classifiers, namely, SVM, Multi-Class SVM, Binary Classification, k-NN in intrusion detection [1]. Figure 1 demonstrates the model of intrusion detection system proposed in this work [8], [12].

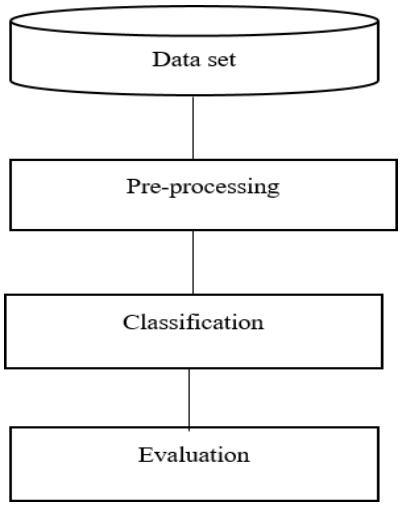

Figure 1. Proposed model for Intrusion Detection System

A. DATA SET

Dataset select for experimentation is a huge task, because of the fact that the execution of the system depends on the correctness of a dataset. The more precise the data, the more accurate the effectiveness of the system. The dataset can grouped by various means, for example, 1) sanitized dataset, 2) simulated dataset, 3) test bed dataset, and 4) standard dataset. However, difficulties happen in the utilization of the initial three systems. A real traffic method is costly, while the cleaned strategy is perilous. The improvement of a simulation system is additionally complex and challenging. In addition, different types of traffic are required to display different network attacks, which is complex and costly [2]. To overcome these challenges, the NSL– KDD dataset used to approve the proposed system for intrusion detection [22].

B. PRE-PROCESSING

The classifier cannot process the raw dataset because of some of its representative features. Hence, pre-processing is fundamental, in which non-numeric or symbolic features are eliminated or replaced, on the grounds that they do not vital participation in intrusion detection. However, this procedure generates overhead including additionally preparing time; the classifier's architecture becomes complex and waste memory and processing resources. In this manner, the non-numeric features are excluded from the raw dataset for enhanced performance of intrusion detection systems.

C. CLASSIFICATION

Placing an activity into normal and intrusive categories is the core function of an intrusion detection system, which is known as intrusive analysis engine. Along these lines, different classifiers connected as intrusive analysis engines in intrusion detection in the literature, for example, multilayer

perceptron, SVM, naive Bayes, self-organizing map, and BC. In any case, in this study, the three different classifiers of SVM, multi class SVM, KNN, BC, are connected in view of their demonstrated capacity in classification issues. Details of each classification approach are given.

IV. METHODOLOGY

1) SUPPORT VECTOR MACHINE

Support vector machines (SVM) is an effective method for solving classification and regression problems. SVM is initially a usage of Vapnik's Structural Risk Minimization (SRM) principle, which is also to have low generalization error or equivalently does not experience the ill effects of over fitting to the preparation training data set. A model is said to overfit or has a high generalization error in the event that it performs inadequately on cases not present in the training set. SVM is especially effective on data sets that are linearly separable [23], i.e. where hyperplane H can be discovered that partitions the instances into two classes with the instances in an oneclass altogether fall on one side of H. Since there is a limitless number of applicant, hyperplanes that can be select SVM chooses the hyperplane H with the goal that it maximizes its distance to the nearest data points in either class. This is referred to as margin maximization. So far, we have just considered the situation where the data set is linearly separable. In any case, for some real data sets, such a hyperplane may not exist. In these cases, SVM utilizes a function to map the data into an alternate component space where such separability is then possible [5], [24]. This change frequently comes through mapping to a high-dimensional space. A function used to perform such a transformation is known as a Kernel function. Consequently, kernel function plays a significant part in both the theory and application of SVM. The following kernel functions are commonly used along with SVM.

Linear Kernel : k (xi,xj)=xixj
Polynomial Kernel : k (xi,xj)=yxtixj+rd)2
BF Kernel : k (xi,xj)=eY||xi-xj||2
Sigmoid Kernel : k (xi,xj)=tanh(yxtixj+r)

To stretch out SVM to multi-class classification, a set of five binary classifiers are trained, one for each class. Let i = (1,...,5) be index into the quintuple T = (Normal, Probe, DoS, U2R, and R2L) and let Bi denote the corresponding binary classifier for the target class I in T. Every one of the five binary classifiers were trained utilizing the entire training set, but each for its corresponding target class. As it were, when training the classifier Bi, the label 1 is allotted to observation that have a place with class i, and 0 to those that have a place with some other class. This is known as the One-Versus-All approach for classifying the observations into one of the five classes.

SVM produces the best outcomes for classify when the RBF kernel function is utilized Experimental outcomes have demonstrated that execution of SVM classifiers with RBF kernel function will vary with the choice of RBF function. Therefore, in this paper, we train six diverse SVM experts with various RBF parameters, to ensure that SVM algorithm is maximally used. This approach will also ensure more prominent assorted variety of experts in ensemble classifier. Selected values for RBF parameter are defined by RBF vector with values:

RBF = [5 2 1 0.5 0.2 0.1]

Afterward, it will be shown that exactness of every binary classifier inside every expert system will vary, as indicated by the selected value in RBF vector. Because of RBF, vector six SVM experts are developed as takes after:

SVM 1: RBF= 5;
SVM 2: RBF= 2;
SVM 3: RBF= 1;
SVM 4: RBF= 0.5;
SVM 5: RBF= 0.2;
SVM 6: RBF= 0.1;

2) K-NN CLASSIFIERS

The k-nearest neighbor (k-NN) is a simple and effective strategy for objects classification as per the nearest training examples in the feature element space. Consider an set of observations and targets (x1, y1), . . ., (xn, yn), where observations xi∈ Rd and targets yi∈ {0, 1}; at that point for a given i, k-NN rates the neighbors of a test sequence among the training sample, and uses the class labels of the nearest neighbors to expect the test vector class. Thus, k-NN takes the new points and classifies them according most of the votes acquired for the K nearest points in the training data. In k-NN, the Euclidean distance is regularly used as the distance metric to measure the closeness between two vectors.

$$d^2(x_i,x_j)=||x_i-x_j||^2=\sum(x_{ik}-x_{jk})^2$$

Dissimilar to SVM, k-NN classifiers can be utilized to solve multiclass problems. Nevertheless, to make k-NN experts and SVM experts good, we expected to execute five binary classifiers for this technique also. In this manner, the structure of the k-NN experts system, depicted Fig. 2, is the same as that of the SVM experts. Similarity between this two methodologies enables us to join both SVM and k-NN experts into ensemble experts system. The k parameter of k-NN classifiers expresses the number of neighbors in a set of training observations that are nearest to the given observation in approval or testing data set. Variety of this parameter will affect the accuracy of each binary classifier To assurance more prominent variety of classifiers and to maximally use capability of k-NN classifier, we have made six k-NN experts with various estimations of k parameter, defined by k vector:

k = [1, 3, 5, 7, 9, 11]

By selecting different k parameter, we create six k-NN experts as follows:

K-NN 1: k=1

K-NN 2: k=3
K-NN 3: k=5
K-NN 4: k=7
K-NN 5: k=9
K-NN 6: k=11

3) BINARY CLASSIFICATION

Binary classification is the task of classifying the features of a given set into two categories the basis of a classification rule. The actual output of many binary classification algorithms is a prediction score [10].The score indicates the system's certainty that the given observation belongs to the positive class. To make the decision about whether the observation should be classified as positive or negative, as a consumer of this score, you will interpret the score by picking a classification threshold (cut-off) and compare the score against it. Any observations with scores higher than the threshold then predicted as the positive class and scores lower than the threshold then predicted as the negative class.

The predictions now fall into four groups based on the actual known answer and the predicted answer: correct positive predictions (true positives), correct negative predictions (true negatives), incorrect positive predictions (false positives) and incorrect negative predictions (false negatives). Binary classification accuracy metrics quantify the two types of correct predictions and two types of errors. Typical metrics are accuracy (ACC), precision, recall, false positive rate, F1-measure. Each metric measures a different aspect of the predictive model. Accuracy (ACC) measures the fraction of correct predictions. Precision measures the fraction of actual positives among those examples that are predicted as positive. Recall measures how many actual positives were predicted as positive. F1-measure is the harmonic mean of precision and recall

4) MULTI CLASS SUPPORT VECTOR MACHINE

As SVM solves only binary class classification problem, the multiclass problem needs to be decomposed into several binary class problems. Each of the binary classifiers is applied in new data point, the frequency of number of times the point is assigned the same label is counted, and the label with highest count is assigned to that point. There are several methods for the decomposition of multiclass problem.

ONE-VERSES-ALL

One-verses-all is also called as the winner takes all strategy. This is the simplest approach to reducing the problem of classification from k classes into k binary problems. Each problem is different from other k-1 problems. This method requires k binary classes in which we train kth classifier with positive example belonging to class k and negative examples belonging to other k-1 classes. An unknown example is tested, and the classifier for which maximum output is produced is measured to be the winner class. That class label is assigned to that example. Although this approach is simple, its performance can be compared with approaches that are more complicated

ONE-VERSUS-ONE

For every pair of different classes, one binary classifier is constructed. In this way, the multiclass problem is broken into a series of a set of binary class problems so that we can apply SVM model for each pair of classes. Total k (k-1) /2 classifiers are needed to classify the unknown data. The binary classifier is trained taking one class as positive and other class as negative. For a new data point x if that classifier classifies x in first class, then a vote is added to this class. If the classifier classifies x in the second class, the vote is added to the second class. This process is repeated for each of the k (k-1)/2 classifiers. Finally, the label of the class with maximum number of votes is assigned to the new data point x. In this way, the class to which the unknown data point belongs is predicted.

A. EVALUATION

The designed system is evaluated based of the standard dataset NSL– KDD, which is randomized and partitioned into three sections, in particular, the full dataset, the half dataset, and the 1/4 dataset. The full dataset comprises of 65,535 samples, the half dataset includes 32,767 samples, and the 1/fourth dataset comprises of 18,383 samples. Accuracy, precision, and recall are utilized as assessment metrics. These metrics are described here Accuracy: Accuracy is computed as "the total number of two correct predictions, True Positive (TP) + True Negative (TN) divided by the total number of a dataset Positive (P) + Negative (N)".

$$Accuracy = \frac{TP+TN}{P+N}$$

Precision: Precision is calculated as "the number of correct positive predictions (TP) divided by the total number of positive predictions (TP + FP)". Precision is also known as a positive predictive value.

$$Precision = \frac{T\ P}{TP+FP}$$

Recall: Recall is calculated as "the number of correct positive predictions (TP) divided by the total number of positives (P)". Recall is also known as the true positive rate or sensitivity.

$$Recall = \frac{TP}{P}$$

B. THE NSL-KDD CUP 99 DATA SET

The execution of the proposed algorithm is tested on NSL KDD Cup 99 benchmark dataset from UCI machine learning repository. NSL-KDD Cup 99 dataset is the new form of the KDD Cup 99 dataset. NSL-KDD Cup 99 dataset settles a portion of the restrictions of the KDD Cup 99 dataset [3]. The KDD 1999 Container Benchmark intrusion detection dataset connected in the 3rd International Knowledge Discovery and Data Mining Tools Competition. It is a model fit for

recognizing characteristic between intrusions and normal connections for making a network intrusion detector. In NSLKDD Cup 99 dataset, each case entitled with features of a class of system data. Each class is marked with either normal or attack. The classes in NSL-KDD Cup 99 dataset are assembled into five principle classes: (a) Normal, (b) Denial of Service (DoS), (c) Remote to User (R2L), (d) User to Root (U2R), and (e)Probe is shown below in Figure3.. Each instance in NSL-KDD Cup 99 dataset is a network connection, which have total 41 input features (either discrete or continuous values).

The features in NSLKDD Cup 99 dataset are separated into three categories.

(a) the basic input features of network connection including some flags in TCP connections, duration, prototype, number of bytes from source IP addresses or from destination IP addresses, and service,

(b) The contented input features of network connections, and

(c) The statistical input features that are computed by either a time window or a window of positive kind of connections

Table I, II, and III describes the datasets in details.

Table I- NSL KDD CUP 99 DATASET DESCRIPTIONS

Dataset	No. of attributes	Types of attributes	Total instances	Class values
Training 100%	41	Real & nominal	1,25,973	23
Training 20%	41	Real & nominal	25,192	23
Testing	41	Real & nominal	22,544	40

Table II- NSL KDD CUP 99 DATASET DESCRIPTIONS

Main Attacks	22 attack classes
DoS	Back, land, Neptune, pod, smurf, teardrop
R2L	ftp_write, guess_ passwd, imap ,multhop, phf, spy, warezclient, warezmaster
U2R	Buffer_overflow, perl, loadmodule, rootkit
Probing	Ipsweep, nmap, portsweep, satan

Table III- INSTANCES IN EACH CLASS IN TRAINING DATASETS

Class values	Training 100%	Training 20%
normal	67343	13449
back	956	196
land	18	1
neptune	41214	8282
pod	201	34
smurf	2646	529
teardrop	892	188
fp_write	8	1
guess_ passwd	53	10
imap	11	5
multhop	7	2
phf	4	2
spy	2	1
warezclient	890	181
warezmaster	20	7
buffer_overflow	30	6
loadmodule	9	1
perl	3	3
rootkit	10	4
ipsweep	3599	710
nmap	1493	301
portsweep	2931	587
satan	3633	691

The strong advantage of NSL-KDD Cup 99 dataset is that the training and testing instances are reasonable, so it becomes reasonable to implement the experiments on the total set of training and testing dataset without the need to randomly choose a small portion of dataset.is shown in Table III The NSL-KDD Cup 99 dataset has the following higher positions over the original KDD 99 dataset:

NSL-KDD Cup 99 dataset does exclude repetitive preparing instances that confound the learning classifiers.

•There is no duplicate instances in the testing data of NSLKDD Cup 99 dataset. So, the mining models created by learning classifiers are biased free.

•The training instances from each attacks group is opposite proportional to the percentage of instances in the original KDD dataset. Therefore, the classification accuracy of learning algorithm varies in a more extensive territory that makes it more effective to have an exact judgment of various learning methods.

•The number of training and testing instances are responsible to run the analyses without randomly chosen small portion of training instances.

KDD 99 dataset is perfect dataset to test intrusion detection since it has the large number of excess instances, which makes the learning classifiers be biased towards the frequent instances, and in this way keep them from learning unfrequented instances that are normally more destructive to computer networks.

As User to Root (U2R) and Remote to User (R2L) attacks are generate in these methodologies is mentioned in Table II. The presence of these repeated instances in the testing dataset will cause the evaluation results to be biased by the classifiers that have better order rates on the frequent instances.

V. RESULTS

RECEIVER OPERATING CHARACTERISTIC (ROC)

Receiver operating characteristic (ROC) curve is utilized to analyze the nature of the classifier or other automated system is shown below in Figure.2. The AUC Area under the ROC Curve is the measure of productivity for the classifier in the mining task. ROC curve illustrates the execution of the binary classifier system. Multiclass classification issue regards binary classifier as one versus all and calculate the operating point for each class, the take out come about by computing the average of all.

Classifier gives the outcome as true positive (TP) and the true negative (TN) if the result lies under the false positive (FP) means classifier indicates the attack in progress but actually no attack is occurring and false negative (FN) it implies that classifier shows that no malicious action is going on while there is really an attempt of intrusion is taking place. Therefore, the outcome is overlapping and not accurate whether positive or negative. To deal with this overlapping result ROC curves are utilized.

TP- Classifying an intrusion as an intrusion
FP- Incorrectly classifying normal data as an intrusion.
TN- Correctly classifying normal data as normal.
FN- Incorrectly classifying an intrusion as normal

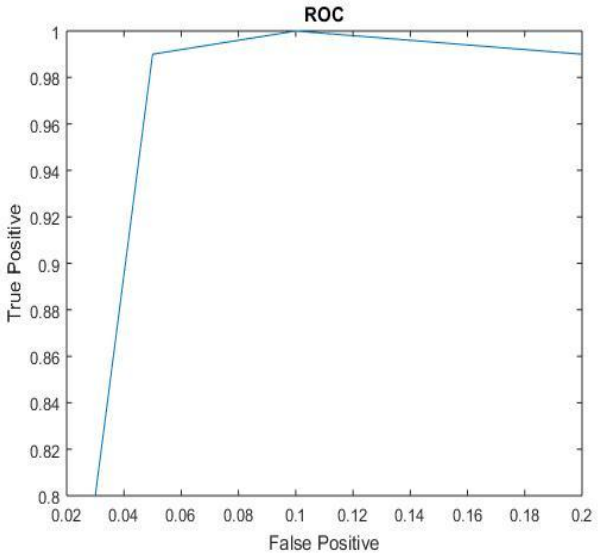

Figure 2. Receiver operating characteristic (ROC)

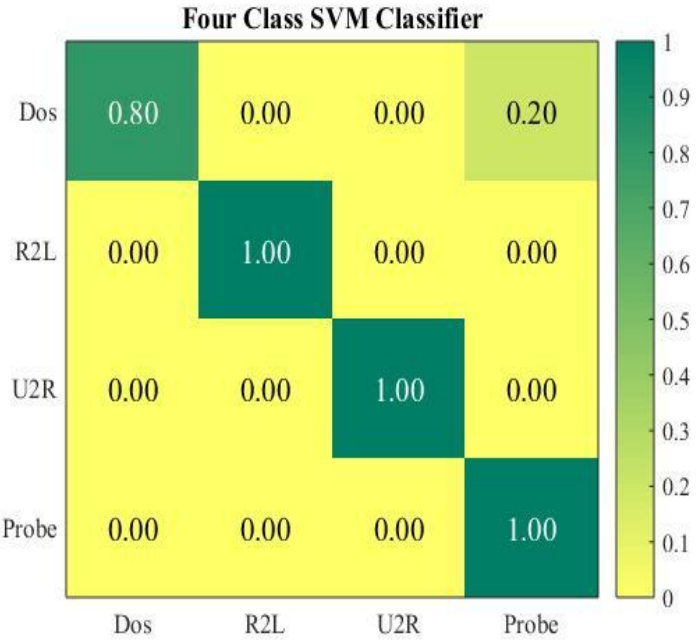

Figure 3. Types of Attacks

The accuracy of SVM, Multi class SVM, k-NN and Binary Classification (BC) on 20% testing and 80% training data samples is shown in Table I and Figure 3. Multi class SVM performs better compared with SVM, k-NN and Binary Classification (BC) on full data samples, whereas Multi class SVM indicates improved accuracy over SVM, k-NN and Binary Classification (BC) on half data samples. Multi class SVM outperforms other techniques on 1/4 data samples, as depicted in Figure 4.

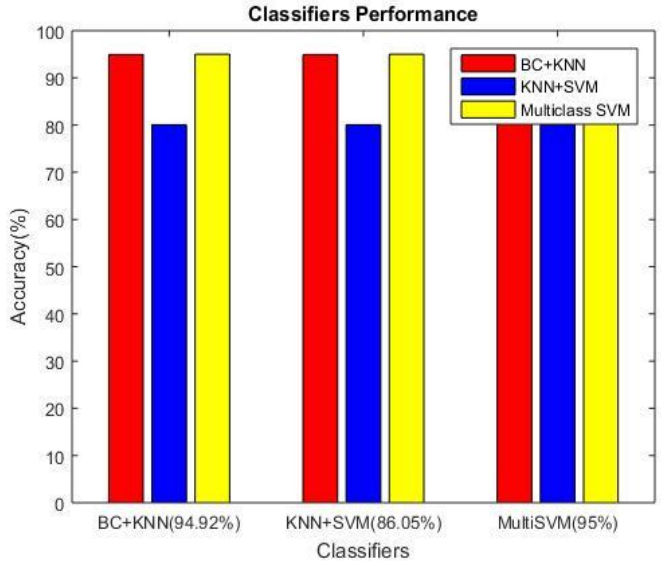

Figure 4 Accuracy of Multiclass SVM

The precision of SVM, Multi class SVM, k-NN and Binary Classification (BC) on 20% testing and 80% training data samples is shown in Figure 5. The precision of Multi class SVM is better than that of SVM, k-NN and Binary Classification (BC) on the full data samples, and it is outperforms that of SVM. On half data samples, the precision of Multi class SVM is higher than that of SVM, k-NN and Binary Classification (BC). On 1/4th data samples, the precision of Multi class SVM is equal to that of SVM. Furthermore, the Multi class SVM performs better than SVM, k-NN and Binary Classification (BC) in the 1/4 dataset.

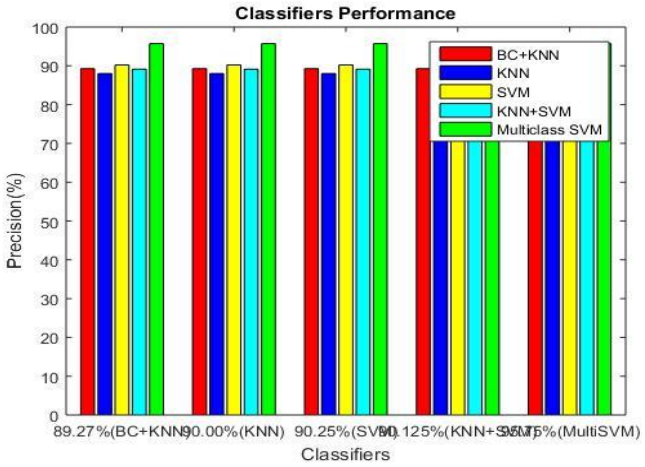

Figure 5 Precision of Multiclass SVM

VI. CONCLUSION

Intrusion detection and prevention are essential to current and future networks and information systems, because our daily activities are heavily dependent on them. Furthermore, future challenges will become more frightening because of the Internet of Things. In this respect, intrusion detection systems have been important in the last few decades. Several techniques have been used in intrusion detection systems, but machine learning techniques are common in recent literature. Additionally, different machine learning techniques have been used, but some techniques are more suitable for analysing huge data for intrusion detection of network and information systems. To address this problem, different machine learning techniques, namely, SVM, Multiclass SVM, k-NN, Binary Classification (BC) are investigated and compared in this work. Multiclass SVM outperforms other approaches in accuracy, precision, and recall on the full data samples that comprise 65,535 records of activities containing normal and intrusive activities. Furthermore, the Multiclass SVM indicated better results than other datasets in half of the data samples and in 1/4 of the data samples. Therefore, Multiclass SVM is a suitable technique for intrusion detection systems that are designed to analyze a huge amount of data. In future, Multiclass SVM will be explored further to investigate its performance in feature selection and feature transformation techniques.

REFERENCES

[1] Binhan Xu, Shuyu Chen, Hancui Zhang, Tianshu Wu," Incremental k-NN, SVM Method in Intrusion Detection"
[2] Manjiri V. Kotpalliwar, 2Rakhi Wajgi" Classification of Attacks Using Support Vector Machine (SVM) on KDDCUP'99 IDS Database"
[3] Muhammad Shakil Pervez, and Dewan Md. Farid "Feature Selection and Intrusion classification in NSL-KDD Cup 99 Dataset Employing SVMs"
[4] Sumaiya Thaseen, Ch.Aswani Kumar "Intrusion Detection Model Using fusion of PCA and
Optimized SVM"
[5]A.M.Chandrasekar, K.Raghuveer, Intrusion Detection Techniques by using K-Means, Fuzzy Neural Networks, SVM Classifier
[6] Noreen Kausar , Brahim Belhaouari Samir, Suziah Sulaiman, Iftikhar Ahmad , Muhammad Hussain "An Approach towards Intrusion Detection using PCA Feature Subsets and SVM"
[7] I. Ahmad, M. Basheri, M.J. Iqbal, A. Raheem "Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection"
[8] Gong Shang-fu,Zhao Chun-lan "Intrusion Detection System Based on Classification"
[9] Nathan Shone, Tran Nguyen Ngoc, Vu Dinh Phai, and Qi Shi "A Deep Learning Approach to Network Intrusion Detection"
[10] Longjie Li, Yang Yu, Shenshen Bai, Ying Hou, and Xiaoyun Chen,"An Effective Two-Step Intrusion Detection Approach Based on Binary Classification and k-NN"
[11] Chuanlong Yin, Yuefei Zhu, Jinlong Fei, and Xinzheng He "Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks "
[12] Rajesh Wankhede, G. H. Raisoni "Intrusion Detection System using Classification Technique"
[13] Abdulla Amin Aburomman, Mamun Bin Ibne Reaz "A novel SVM-kNN-PSO ensemble method for intrusion detection system "
[14]H. Wang, J. Gu, S. Wang, "An effective intrusion detection framework based on SVM with feature augmentation, Knowledge-Based Systems", Volume 136, 2017, Pages 130-139, ISSN 0950-7051, https://doi.org/10.1016/j.knosys.2017.09.014.
[15]F. Kuang, X. Weihong , S. Zhang, A novel hybrid KPCA and SVM with GA model for intrusion detection, Applied Soft Computing,Volume 18,2014,Pages 178-184,ISSN 1568-4946, https://doi.org/10.1016/j.asoc.2014.01.028.
[16]A. A. Aburomman, M.B. Reaz, A novel SVM-kNN-PSO ensemble method for intrusion detection system, Applied Soft Computing, Volume 38, 2016, Pages 360-372, ISSN 1568-4946, https://doi.org/10.1016/j.asoc.2015.10.011.
[17]M.R. Raman, N. Somu, K. Kirthivasan, R. Liscano, V.S. Sriram, An efficient intrusion detection system based on hypergraph - Genetic algorithm for parameter optimization and feature selection in support vector machine, Knowledge-Based Systems, Volume 134, 2017, Pages 1-12, ISSN 0950-7051, https://doi.org/10.1016/j.knosys.2017.07.005.
[18] S. Teng, N. Wu, H. Zhu, L. Teng and W. Zhang, "SVM-DT-based adaptive and collaborative intrusion detection," in IEEE/CAA Journal of Automatica Sinica, vol. 5, no. 1, pp. 108-118, Jan. 2018. doi: 10.1109/JAS.2017.7510730.
[19] N.Farnaaz, M.A. Jabbar, Random Forest Modeling for Network Intrusion Detection System, Procedia Computer Science, Volume 89, 2016, Pages 213-217, ISSN.18770509,https://doi.org/10.1016/j.procs.2016.06

[20] Chih-Wei Hsu and Chih-Jen Lin, "A Comparison of Methods for Multiclass Support Vector Machines", IEEE Transaction on Neural Networks, 2002.
[21].Ahmad, F. Amin, "Towards feature subset selection in intrusion detection," 2014 IEEE 7th Joint International Information Technology and Artificial Intelligence Conference, Chongqing, 2014, pp. 68-73.
[22]S.M. Bamakan, H. Wang, T. Yingjie, Y. Shi, An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization, Neuro computing, Volume 199, 2016, Pages 90-102.
[23] J.Jayshree, and L. Ragha. "Intrusion detection system using support vector machine." International Journal of Applied Information Systems (HAIS)-ISSN (2013): 2249-0868
[24] C.C .Chang,.and C.J. Lin., 2011. LIBSVM: a library for support vector machines. ACM transactions on intelligent systems and technology (TIST), 2(3), p.27.

Authors Profile

Dr. P. Kumar is currently a Assistant Professor with the Centre for Information Technology and Engineering, Manonmaniam Sundaranar University.Tirunelveli. His research interests include computer Vision- Digital /Signal Image Processing -Cyber Security – Big Data Analytics, Remote Communication - Cloud Computing.

Mr.A.Anbarasa Kumar is currently a Research Scholar with the Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu, India His research interests include Cyber Security, Image Processing, Intrusion Detection

