RESEARCH ARTICLE

SAMRIDDHI Volume 14, Special Issue 2, 2022 Print ISSN : 2229-7111 Online ISSN : 2454-5767

Grading Method of Ensemble and Genetic Algorithm for Intrusion Detection System

D. P. Gaikwad[1*], S. V. Chaitanya[2]

[1*,2] AISSMS College of Engineering, Pune, India; e-mail*: dp.g@rediffmail.com

ABSTRACT

Intrusion Detection System is very important tool for network security. However, Intrusion Detection System suffers from the problem of handling large volume of data and produces high false positive rate. In this paper, a novel Grading method of ensemble has proposed to overcome limitation of intrusion detection system. Partial decision tree (PART), RIpple DOwn Rule (RIDOR) learner and J48 decision tree have used as base classifiers of Grading classifier. Optimzed Genetic Search algorithm have used for selection of features.These three base classifiers have graded using RandomForest decision tree as a Meta classifier. Experimental results show that the proposed Grading method of classification offers accuracies of 81.3742%, 99.9159% and 99.8023% on testing, training datasets and cross validation respectively. It is found that the proposed graded classifier outperform its base classifiers and existing hybrid intrusion detection system in term of accuracy, false positive rate and model building time.

Keywords: Grading Ensemble, RIDOR, Meta Classifier, Base Learner, AdaBoost**.**

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, (2022); DOI : 10.18090/samriddhi.v14spli02.11

INTRODUCTION

Recently, Internet has developed an vital part of human life for communication. Although internet serves the civilization in a better way, it also owns some serious threats in the form of cybercrime. The ubiquity of internet connectivity has empowered an increase in the pace and volume of cyber-attacks. Identifying the various kinds of cyber- attacks is an obvious key technical issue. The data of individuals, financial and other important organisation is very important. During Covid-19 pandemic, most of the companies are accepting working from home through Internet. Due to huge usages of networks, cyber-attacks, network attacks and the possibility of data stealing and destruction is rapidly increasing [1]. Internal Intruders and hackers in networks modify, destruct or steal private information. A notable development has been made in the field of internet security by issuing various directives and regulations. Apart from those regulations and policies, various security measures are needed to improve the technical aspects of internet security. Various Cyber security tools such as Firewall, Antivirus software, Penetration testing have been employed to tackle the cyber-attacks. Among these tools, Intrusion Detection System (IDS) play vibrant role in the information security ground. It can recognize an attack which might be an on-going invasion or an intrusion that has already happened. In fact, intrusion detection is regularly alike to a classification problem. The central inspiration of intrusion detection is to expand the accuracy of classifiers in successfully recognizing the intrusive behaviour. Intrusion Detection technique can be classified into two broad categories; Network

Corresponding Author : D. P. Gaikwad, AISSMS College of Engineering, Pune, India; e-mail : dp.g@rediffmail.com

How to cite this article : Gaikwad, D.P., Chaitanya, S.V. (2022). Grading Method of Ensemble and Genetic Algorithm for Intrusion Detection System.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, Volume 14, Special Issue (2), 262-270.

Source of support : Nil

Conflict of interest : None

Intrusion Detection System and Host Intrusion Detection system. NIDS are setup at a planned point within a network where it does an observation of the passing traffic on the subnet and contests the traffic to the collection of known attacks for anomaly detection. HIDS run on autonomous hosts on the network where it screens the incoming and outgoing packets for anomaly and alert the network administrator. Grounded on the Detection method, IDS is further considered into two types namely, signature based IDS, which detects the intrusions based on known signatures and Anomaly based IDS, which detects and classifies the incoming traffic as normal or anomaly based on the analysis of network behaviour [2]. The latter method has significant advantage over the former method in identifying new types of attacks, also called the zero day attack. Although, IDS are capable of detecting various anomalies in the network, it also suffers from various problems including generation of large number of false alarms, susceptible to protocol-based attacks, requirement of an experienced engineer to administer IDS. To overcome these problems existing in the traditional IDS system, Machine Learning (ML) techniques have been widely used to offer an intelligent approach to Intrusion Detection System. Many researchers have used unsupervised and supervised learning method lead by shallow learning classifiers like Random Forest, SVM and Naïve Bayes, Fuzzy logic and neural networks [3]. These classifiers are used to classify normal and abnormal data in network. The usages of these classifiers have offered improved detection accuracy. Single classifier based intrusion detection systems offers high false positives rate and the false negatives rate. In the past few years, deep learning based intrusion detection learning have exposed their effectiveness. But, these methods yield a big false negative rate, which affects the performance and strength of network security. Single classifier might not enough when numbers of attacks obtainable in network. Hybrid methods are used to use cascade supervised and unsupervised classifiers or joining supervised and unsupervised classifiers for IDS [4] [5].

Recently, ensemble classifiers are being proposed for IDS. Ensemble is a technique in which base classifiers can be combined using different combination rules. Specifically, there are four ways to ensemble classifiers. These four are widely known models are Bagging, Boosting, grading and Stacking. Bagging is used to combine multiple similar classifiers. It is used to deduce variance by averaging high variance of multiple similar classifiers. Boosting is a method of ensemble which is used to reduce bias by building multiple incremental models and keep small variance. Stacking is an ensemble method which syndicates multiple classifiers using a meta-classifier. In this ensemble method, base classifiers trained using training dataset. The meta-classifier is trained on the Meta feature outputs of the each base classifier. The meta-classifier is trained on the forecast class labels or likelihoods from the ensemble [6] [7]. Ensemble method such as Grading has recently generated substantial development in the field of network security. In current years, ensemble method has played a significant role in the fields of security. It offer high accuracy with low false positive rate. In this paper, a novel grading ensemble method for an intrusion detection system have proposed. The main purposes of this investigation work are as below:

- To select more relevant features using Genetic search algorithm.
- To obtain high classification accuracy and low false positive rates using Grading of base classifier.
- To reduce model building time.

The key offerings of this paper are outlined as follows:

- Grading ensemble classifier has used to implement IDS.
- The proposed model is evaluated in terms of three performance metrics namely Accuracy, Detection Rate and False Alarm Rate.
- Genetic Search Algorithm has used to select relevant features which help in reducing model building time.
- The proposed ensemble classifier is compared with various existing proposals.

The remaining part of the paper is prepared as follows. In section 2, some existing proposals have discussed. Methodology of the proposed intrusion detection system have discussed in section 3. Section 4 is used to present proposed architecture of IDS. Results and analysis of results have presented in section 5. Finally, in section 6, paper has concluded with future scope.

LITERATURE SURVEY

In this section, some existing research works on intrusion detection system using machine learning and ensemble approach are studied and discussed. The following are

some of these studies. George Violettas et.al. [8] have proposed ASSET intrusion detection system for the Routing over Low Power and Lossy Networks protocol. This system is used to mitigate attacks in Internet of Things environment. ASSET Intrusion detection system is inspired by network softwarization model which support extendable workflow and offer centralized intelligence. It is combination of three anomaly-detection and RPL specification tool. It has attacker identification process which help to mitigate multiple attacks. Asset supports an adaptable control, monitoring protocol and saves acceptable power consumption. Pooja T.S and Purohit Shrinivasacharya [9] have suggested intrusion detection system using deep learning. They have used Bi-direction LSTM deep learning technique for intrusion detection system. For training LSTM, authors have used KDDCUP- 99 and UNSW-NB15 datasets. Different activation functions have used to train neural network which offers up to 99.55% accuracy on training dataset. K.P. Sanal Kumara, S. Anu H. Nairb, Deepsubhra Guha Royc, Rajalingamd and Santhosh Kumar [10] have proposed federated machine learning method for IDS They have used Paillier Homomorphic Encryption for security of 5G network. For monitoring and classifying nodes, an artificial immune based intrusion detection system has implemented. It is capable to transfer data in network in and smooth manner. The proposed system is extra secure than the current edge security models. Narayana, Venkata Rao and Prasad Reddy [11] have proposed a novel hybrid technique using Sparse AutoEncoder and Deep neural network. Sparse AutoEncoder with L1 regularisation have used for dimension reduction of dataset. Deep neural network is for classification of multiple attacks in network. Deep neural network have trained using KDDCup99, NSL-KDD and UNSW-NB15 training dataset. The proposed system detect known and unknown attacks. Neha V. Sharma and Narendra Singh Yadav [12] have implemented three classifiers for intrusion detection system. Author has used Recursive Feature Elimination (RFE) method to remove irrelevant features from dataset. In future scope, author has suggested ensemble method using bagging, boosting and other method to optimize performance of detection system.

Jingmei Liu, Yuanbo Gao and Fengjie Hu [13] have proposed intrusion detection system LightGBM and ADASYN oversampling technology. In this proposal, the problem of data imbalance is resolved using oversampling method. Ensemble method using LightGBM have used for classification purpose. Ensemble classifier is trained on NSL-KDD, UNSW-NB15 and CI- CIDS2017 data sets. Training and detection time have reduced due to ADASYN oversampling technology and LightGBM. Samed Al and Murat Dener [14] have suggested hybrid deep learning for intrusion detection system. Authors have used Long Short-Term Memory and Convolution Neural network. Authors have used Synthetic Minority Oversampling method and STL was used to overcome data imbalance. They have used CIDDS-001 and UNS-NB15 data set for training and testing proposed classifiers. Elie Alhajjar, Paul Maxwell and Nathaniel Bastian [15] have proposed adversarial ML for intrusion detection. Authors have studied the nature of the adversarial problem in Network Intrusion Detection Systems. They have used evolutionary algorithm to generate adversarial attacks. Authors have used NSL-KDD and UNSW-NB15 dataset for training purpose.

Roseline Oluwaseun Ogundokuna et.al, [16] have implemented two classifier to classify anomalous activities in network. Particle Swarm Optimization (PSO) was used to reduce dimension of dataset. Decision tree and KNN algorithm were used as classifiers. KNN algorithm with Particle Swarm Optimization offered 96.2% accuracy which higher than Decision tree with Particle Swarm Optimization. Yesi Novaria, Siti Nurmaini, Deris Stiawan and Bhakti Suprapto [17] have proposed deep learning based classifier for intrusion detection system. They have used pre-training approach with deep learning (PTDAE) and deep neural network for attack classification. In this research work, authors have proposed automatic hyper parameter optimization technique using grid search method. Neha Gupta, Vinita Jindaland and Punam Bedi [18] have proposed three layer network intrusion detection system using Cost-Sensitive DL and Ensemble method. In first layer, Cost-Sensitive DNN is used for separating normal traffic from doubtful network traffic. In layer two, the eXtreme GB algorithm is used to identify doubtful samples into normal, majority attack and minority attack classes. In layer three, RF (Random Forest) is used to categorise the minority attacks. The proposed system achieves a high Attack Detection Rate for both majority attacks and minority attacks. Abdulla Amin and Mamun Ibne Reaz [19] proposed a novel ensemble classifier for intrusion detection system. In this research, authors have used Particle Swarm Optimization to implement ensemble classifier. The parameters of Particle Swarm Optimization have optimized using Local Unimodal Sampling technique. Six Support Vector machines and

six K-NN have used as base classifiers and PSO as a meta-classifier. These two ensemble classifiers outperform ensemble classifier using weighted majority algorithm. Authors have suggested other approach for ensemble classifiers. Nabila Farnaaz and Jabbar M. A [20] have used Random Forest ensemble classifier for detection of attacks. NSL_KDD dataset used training Random Forest ensemble classifier. The proposed method have compared with classifier J48 and found that Random Forest offered more accuracy than J48. Shraddha Khonde and Venugopal Ulagamuthal [21] have proposed hybrid technique for IDS which work in distributed environment. Authors have used semi-supervised machine learning based ensemble classifier. SVM and K-NN classifiers have used as base classifiers. NSL- KDD dataset have used for training base and ensemble classifier. This ensemble based classifier increases accuracy by 3% and drops false alarm rate by 0.05. Wathiq Laftah, Zulaiha Othman and Mohd Zakree Nazri [22] have proposed hybrid approach for an adaptive intrusion detection system. Authors have used multi-level hybrid SVM and ELM to implement IDS. The model is trained on KDDCup'99 dataset which contain records of Probe, R2L, and U2R attacks. Hariharan Rajadurai and Usha Gandhi [23] have proposed intrusion detection system using Graded ensemble classifier. The proposed classifier is built using Random Forest and GB Base Classifiers. The proposed Graded ensemble classifiers have trained using NSL-KDD dataset

METHODOLOGY OF THE PROPOSED INTRUSION DETECTION SYSTEM

In this section, methodology of the proposed IDS has presented. Basically, training dataset is essential for training any classifier. There are two types of dataset; primary and secondary dataset. Secondary dataset is a dataset which is pre-prepared and available on network. Primary dataset is created by individual researcher. In this paper, NSL-KDD secondary dataset have utilized for training and testing classifiers. The NSL-KDD dataset have pre-processed for selecting relevant features. The details of dataset pre-processing are given below. The algorithm of stacking process have also discussed in subsection.

NSL_KDD dataset

In intrusion detection system, KDD dataset is frequently used for training classifier. Original KDD dataset contains of redundant and invalid. In first part of dataset, all records of the dataset are included. In second part, 10% records of KDD are included in training dataset which consist of small instances and frequently used to train the classifiers. In last part, all corrected records have included in latest dataset. Redundant and invalid samples have removed from original KDD dataset. It has more than 1.25 records with 41 features and it contain four types of attacks along with normal packets. This cleaned without redundant dataset is known as NSL-KDD [21]. Specifically, NSL-KDD dataset consists of Denial of Service, Probe and R2L attacks. Denial of Service attacks used to shut down a computer or network and make it isolated to its target users. Probe attacks are intended to get additional information about the target system. R2L attacks are very dangerous than probe and DOS attacks which are used to give local access to target system. Still, NSL- KDD dataset is with many features which are not relevant for training classifiers. It also takes more time to train models and harder to visualize training set. For reducing training time and removing irrelevant features, dimensionality process is required to implement efficient intrusion detection system. This process must produce dataset which contains most characteristics of the raw data. Machine learning techniques can be used to decrease dimension of training dataset. Machine learning is used to find correlation between features in dataset and select all correlated features. In this paper, Genetic Search algorithm have used for selection of relevant and correlated features. Following parameters of Genetic Algorithm have set for selection of relevant features.

Size of Population: 20
Number of generations: 20
Probability of crossover: 0.5
Probability of mutation: 0.033
Report frequency: 20
Random seed number : 1

In Table 1, all chosen features by Genetic Search algorithm have listed.

Grading of Base Classifier

Meta learning is a method in which assembling of classifiers is done. The selection of best suitable base classifiers for a given problem is very important phase in Meta learning. Grading methof of classification was familiarized by Seewald and Furnkranz. It isencouraged by stacking first meta-classification procedure. In grading method, all tuples are characterized by each base classifier using cross-validation. In conventional Stacking, all classification results are used to generate

a new dataset where a meta-classifier is trained. The final result of stacking is depend on classification results of all the base learners. The outputs of all base classifiers are considered as input for meta-learning classifier. In this method, a meta-classifier is constructed for each basic classifier. Purpose of indivisual meta-classifier is to learn where a base learner is incorrect and where it is offering accurate results. The separate dataset is created for each classifier with similar samples to the original training dataset [24]. Every separate datasets is used to train meta- learner which is used at stage of classification. Both base classifiers and Meta classifiers are used at stage of classification. Next, each example is given to base classifier. Inclusion of output of base classifier in concluding prediction is rely on Meta classifier output of individual base classifier. The outcome result of base classifier is included in final decision if Meta classifier is confidence in base classifier. Meta classifier is capable to predict class probability distribution [25].

Table-1: List of Selected relevant features

Sr. No.	Name of Feature
1	Service
2	Flag
3	src_bytes
4	dst_bytes
5	wrong_fragment
6	logged_in
7	su_attempted
8	Count
9	serror_rate
10	srv_serror_rate
11	same_srv_rate
12	srv_diff_host_rate
13	dst_host_srv_diff_host_rate
14	dst_host_srv_serror_rate

METHODOLOGY OF THE PROPOSED INTRUSION DETECTION SYSTEM

In this section, the architecture of the proposed ensemble classifier for intrusion detection system has presented**.** Graded ensemble has capacity to enhance existing accuracy of intrusion detection system. Specifically, there are three ways to ensemble classifiers. These are widely known models are Bagging, Boosting and Stacking. *Bagging* is used to combine multiple similar classifiers. It is used to deduce variance by averaging high variance of multiple similar classifiers. Boosting is a method of ensemble which is used to reduce bias by building multiple incremental models and keep small variance. Graded ensemble classifier is built using heterogeneous algorithm to obtain better and accurate results. It is an ensemble method which syndicates different multiple classifiers using a meta-classifier. In this ensemble method, base classifiers trained using training dataset. The meta-classifier is fitted based on the Meta feature outputs of the each base classifier. The meta-classifier is qualified on the predicated class labels or probabilities from the ensemble [6] [7].

In this paper, we examine another technique which we call grading for intrusion detection system. The basic idea of grading of base classifiers is to learn to predict for each of the original base classifier whether its prediction for a particular sample is correct or not. PART, Ripple down Rule learner and J48 decision tree has used as base classifiers. These base classifiers have trained separately using 10-fold cross validation method. These Base Classifiers have graded using RandomForest tree as a Meta classifier. Then performance of base classifier has evaluated on test and trained dataset. The outputs of base classifiers have graded using grading classifiers and fed to Meta classifier for making final decision. Figure 1 depicts the system architecture of the proposed grading ensemble classifier.

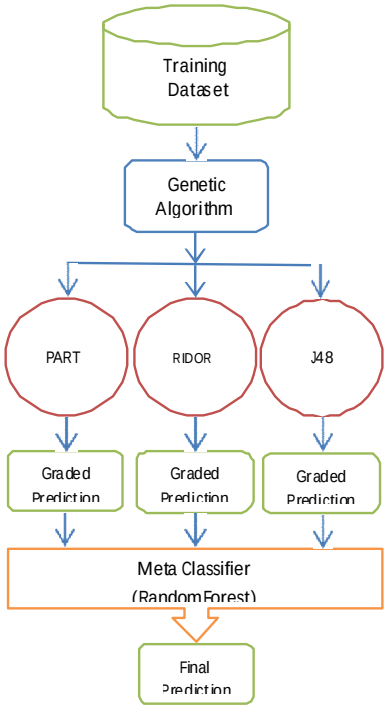

Figure 1: Architecture of the Proposed Grading Ensemble Classifier

ANALYSIS OF EXPERIMENTAL RESULTS

In this section, the results of all experiments have discussed. Base Classifiers and the proposed approach is trained and tested on lenova laptop with Intel Core-i5 CPU and 8 GB RAM. The proposed system has developed using Java Language with WEKA software. The performances of classifiers have evaluated using different metrics. These metrics are communicated in terms of true positive (TP), true negative (TN), false positive (FP) and false negative (FN). The classification accuracy, precision and recall values have used to measure overall performances of classifiers [23]. These metrics have expressed by equations 1 to 5.

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \quad ....(1)$$

$$\mathrm{Re}call = \frac{TP}{(TP + FN)} \quad ....(2)$$

$$FPR = \frac{FP}{(FP + TN)} \quad ....(3)$$

$$\mathrm{Pr}ecision = \frac{TP}{(TP + FP)} \quad .....(4)$$

$$F - Measure = \frac{(2 * \mathrm{Pr}ecision * \mathrm{Re}call)}{(\mathrm{Pr}ecision + \mathrm{Re}call)} \quad ...(5)$$

The performances in terms of accuracy, recall, precision, F-measure and model building time of the proposed Graded classifier and base classifiers on training dataset have listed in Table 2 and shown in Figure 2. From Table 2 and Figure 2, it can be concluded that the proposed Graded classifier for intrusion detection system offers accuracy of 99.9159 % on training dataset, which is more than accuracies of its all base classifiers and three existing classifiers.

Sr. No.	Name of Classifier	Performance Matrices	Accuracy of Training
1	Proposed Grading Ensemble classifier with RandomForest Meta Classifier	Accuracy	99.9159 %
		FP Rate	0.001
		Precision	0.999
		Recall	0.999
		F-Measure	0.999
		Model Building Time in Second	358.87
2	PART	Accuracy	99.892 %
		FP Rate	0.001
		Precision	0.999
		Recall	0.999
		F-Measure	0.999
		Model Building Time in Second	16.75
3	J48	Accuracy	99.8714 %
		False Positive Rate	0.001
		Precision	0.999
		Recall	0.999
		F-Measure	0.999
		Model Building Time	14.41
4	RIDOR	Accuracy	99.7841 %
		FP Rate	0.002
		Precision	0.998
		Recall	0.998
		F-Measure	0.998
		Model Building Time in Second	23.89
5	SVM+K-NN, Ref. [21]	Accuracy	98 .00%
		FP Rate	0.05
6	ELM-SVM, Ref.[22]	Accuracy	95.86%
		FP Rate	2.13
7	Random Forest + Gradient Boost, Ref. [23]	Accuracy	91.06%
		FP Rate	2.99

It can also be observed that the proposed Graded classifier offers higher percentage of precision, recall and F-measure values. The proposed Graded classifier and its all base classifiers require less training time on reduced training dataset using Genetic Algorithm. The classification accuracy on test dataset of any standard classifier is very important to decide the generalisation error which is the strength of that classifier. The accuracy and false positive rates of Base Classifier and the proposed Graded classifier on test dataset have shown in Table 3 and depicted in Figure 3. From Table 3 and Figure 3, it can be easily concluded that the proposed Graded classifier for intrusion detection system offers accuracy of 81.3742 % on test dataset, which is more accuracy than its all base classifiers. The proposed Graded classifier also provides less false positive rate of 0.15 which less than all its base classifiers.

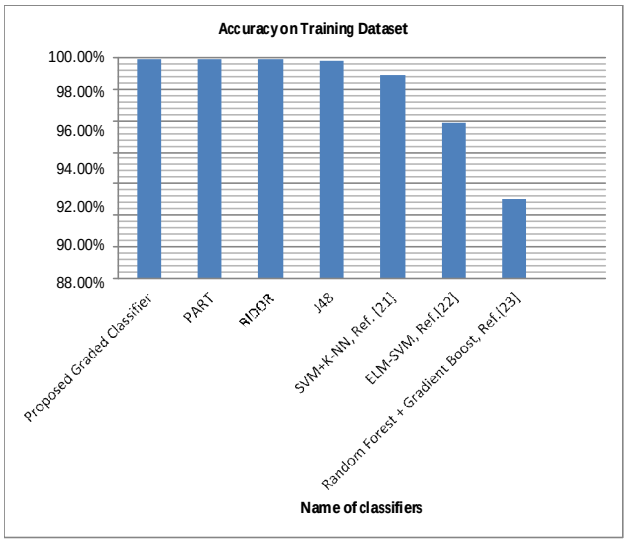

Figure 2: Accuracy of Proposed Classifier on Training Dataset.

Table-3: Performances of the Classifiers on Training Dataset on Test Dataset

Sr. No.	Name of Classifier	Performances Matrices	Accuracy of Test
1	Proposed Grading Ensemble classifierwith Random ForestMeta Classifier	Accuracy	81.3742 %
		FP Rate	0.15
		Precision	0.853
		Recall	0.814
		F-Measure	0.813
		Model Building Time in Second	339.65
2	PART	Accuracy	81.1879%
		FP Rate	0.164
		Precision	0.834
		Recall	0.812
		F-Measure	0.812
		Model Building Time in Second	17.04
3	J48	Accuracy	79.8838 %
		FP Rate	0.161
		Precision	0.844
		Recall	0.799
		F-Measure	0.798
		Model Building Time in Second	13.27
4	RIDOR	Accuracy	80.2874 %
		FP Rate	0.159
		Precision	0.846
		Recall	0.803
		F-Measure	0.802
		Model Building Time in Second	24.61

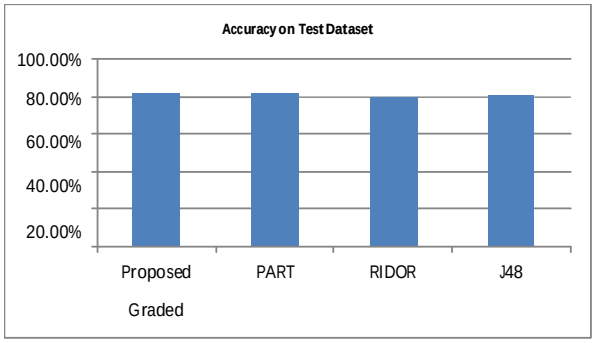

Figure 3: Accuracy of Proposed Classifier on Test Dataset

In literature survey, it is found that most of researchers have not provided classification accuracy of IDS on cross validation. The accuracy and false positive rates of Base Classifier and the proposed Graded classifier on cross validation have shown in Table-4. From above Table-4, it can be concluded that the proposed Graded classifier for IDS offers accuracy of 99.8023% which is more than its all base classifiers accuracy on 10-fold cross validation. It also provides less false positive rate of 0.002 which is approximately same to all base classifiers.

Table-3: Performances of the Classifiers on Training Dataset on Cross Validation

Sr. No.	Name of Classifier	Performances Matrices	Accuracy of CV
1	Proposed Grading Ensemble classifier with RandomForest Meta Classifier	Accuracy	99.8023 %
		FP Rate	0.002
		Precision	0.998
		Recall	0.998
		F-Measure	0.998
		Model Building Time in Second	350.3
2	PART	Accuracy	99.769 %
		FP Rate	0.002
		Precision	0.998
		Recall	0.998
		F-Measure	0.998
		Model Building Time in Second	19.28
3	J48	Accuracy	99.7531 %
		FP Rate	0.003
		Precision	0.998
		Recall	0.998
		F-Measure	0.998
		Model Building Time in Second	15.51
4	RIDOR	Accuracy	99.5626 %
		FP Rate	0.004
		Precision	0.996
		Recall	0.996
		F-Measure	0.996
		Model Building Time in Second	24.64

CONCLUSIONS AND FUTURE SCOPES

In this paper, a novel grading classifier for intrusion detection system has proposed. The proposed Graded classifier helps in enhancing performance of IDS. Three heterogamous Base Classifiers have used for graded using Meta Classifier. Partial Decision tree, Ripple down Rule learner and J48 decision tree have graded using RandomForest tree. This Graded classifier is helped to improve performance of IDS in terms of accuracy and detection rate. Genetic search algorithm have used to NSL-KDD training and testing dataset for selection of relevant features. Genetic search algorithm has decreased number of features of NSL-KDD dataset and it affect training time of classifier. Several experiments have conducted on base leaners and Graded classifier. Experimental results show that the proposed Graded classifier offers 81.3742%, 99.9159% and 99.8023% on testing, training dataset and cross validation respectively**.** Experimental results have compared with existing intrusion detection systems. From comparison with existing IDS, it is found that the proposed Graded classifiers outperform existing hybrid intrusion detection system in term of accuracy and false positive rate. Genetic algorithm helped to reduce the training time of the proposed Graded classifier by selecting suitable features in training dataset. Main limitation of the proposed IDS is that the proposed IDS have trained using available secondary training and testing dataset. In future works, the plan will be to implement real time intrusion detection system using real data networks.

REFERENCES

[1] Fatima Ezzahra, Samira Douzi, Khadija Douzi and Badr Hssina, "IDS-attention: an efficient algorithm for intrusion detection systems using attention mechanism," *Journal of Big Data*, 8:149, 2021.

[2] Ramadan R. Yadav K, "A novel hybrid intrusion detection system (IDS) for the detection of internet of things (IoT) network attacks," *Ann Emerging Technology Computer,"* 2020, https://doi.org/10.33166/aetic.2020.05.004.

[3] S. Fenanir, F. Semchedine and A. Baadache, "A Machine Learning-Based Lightweight Intrusion Detection System for the Internet of Thing," Revd Intelligence Artificial, vol. 33, no. 3, pp. 203–211, Oct. 2019, doi:10.18280/ria.330306.

[4] S. Alhaidari and M. Zohdy, "Hybrid Learning Approach of Combining Cluster-Based Partitioning andHidden Markov Model for IoT Intrusion Detection," Third *International Conference on Information System and Data Mining - ICISDM*, pp. 27–31, doi: 10.1145/3325917.3325939.

[5] B. Aboshosha, R. Ramadan and A. El-Sayed, "Encapsulate Sec: A Link-Layer Security Architecture for Wireless Sensor Networks," *WAS Sci. Nat*., vol. 1, 2019.

[6] Tang, J., S. Alelyani and H. Liu, "Data Classification: Algorithms and Applications," Data Mining and Knowledge Discovery Series, CRC Press, 2015, pp. 498-500.

[7] Wolpert, David H., "Graded generalization, *Neural networks* Vol. 5, No.2,1992, pp.41-259

[8] George Violettas, George Simoglou, Sophia Petridou and Lefteris Mamatas, "A Softwarized Intrusion Detection System for the RPL-based Internet of Things networks," Future Generation Computer Systems 125, 2021, pp. 698–714.

[9] Pooja T and Purohit Shrinivasacharya, "Evaluating neural networks using Bi-Directional LSTM for network intrusion detection systems in cyber security, "*Global Transitions Proceedings Vol.2,* 2021, pp.448–454.

[10] K. Sana et.al, "Security and privacy-aware Artificial Intrusion Detection System using Federated Machine Learning," Computers and Electrical Engineering, Vol. No. 96, 2021, 107440.

[11] Narayana Rao, Venkata Rao and Prasad Reddy, " A hybrid Intrusion Detection System based on Sparse AutoEncoder and Deep Neural Network," Computer Communications 180, 2021, pp.77–88.

[12] Neha Sharma and Narendra Yadav, "An optimal intrusion detection system using recursive feature elimination and ensemble of classifiers," Microprocessors and Microsystems 85, 2021, 104293.

[13] Jingmei Liu, Yuanbo Gao and Fengjie Hu, "A fast network intrusion detection system using adaptive synthetic oversampling and LightGBM," Computers and Security 106, 2021,102289.

[14] Samed Al and Murat Dener, "STL-HDL: A new hybrid network intrusion detection system for imbalanced dataset on big data environment," *computers and security* -110, 2021,102435.

[15] Elie Alhajjar, Paul Maxwell and Nathaniel Bastian, "Adversarial machine learning in Network Intrusion Detection Systems," *Expert Systems with Applications*-186, 2021, 115782.

[16] Roseline Ogundokuna et.al, "An Enhanced Intrusion Detection System using Particle Swarm Optimization Feature Extraction Technique," *10th International Young Scientists Conference on Computational* Science , Procedia Computer Science-193, 2021, 504–512.

[17] Yesi Novaria Kunang, Siti Nurmaini, Deris Stiawan and Bhakti Yudho Suprapto, " Attack Classification of an Intrusion Detection System using Deep Learning and Hyper parameter optimization," *Journal of Information Security and Applications-58*, 2021, 102804.

[18] Neha Gupta, Vinita Jindaland and Punam Bedi, "CSE-IDS: Using cost-sensitive deep learning and ensemble algorithms to handle class imbalance in network-based intrusion detection systems," *Computers & Security, Volume 112, 2022, 102499***.**

[19] Abdulla Aburomman and Mamun Reaz, "A novel SVM-kNN-PSO ensemble method for intrusion detection system," *Applied Soft Computing Volume 38*, January 2016, Pages 360-372.

[20] Nabila Farnaaz and Jabbar M, "Random Forest Modelling for Network Intrusion Detection System," *Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016)*, Procedia Computer Science 89, 213 – 217.

[21] Shraddha Khonde and Venugopal Ulagamuthal, "Hybrid Architecture for Distributed Intrusion Detection System Using Semisupervised Classifiers in Ensemble Approach," *Advances in Modelling and Analysis B,* Vol. 63, No. 1-4, 2020, pp. 10-19.

[22] Wathiq Al-Yaseen, Zulaiha Othman and Mohd Ahmad Nazri, "Real-time Multi-agent System for an Adaptive Intrusion Detection System," *Pattern Recognition Letters 85*, November 2016, DOI:10.1016/j.patrec.2016.11.018.

[23] Hariharan Rajadurai and Usha Devi Gandhi, "A Graded ensemble learning model for intrusion detection in wireless network," Neural Computing and Applications, 2020, https://doi.org/10.1007/s00521-020-04986.

[24] Gregor Stiglic and Peter Kokol, "Effectiveness of Rotation Forest in Meta-learning Based Gene Expression Classification," *Twentieth IEEE International Symposium on Computer-Based Medical Systems* (CBMS'07), IEEE Computer Society.

[25] Surendra Singhi and Huan Liu, "Error-Sensitive Grading for Model Combination," *CML 2005*, LNAI 3720, pp.724–732, 2005.c©Springer-Verlag Berlin Heidelberg 20.