JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452

Classification of Hybrid Intrusion Detection System Using Supervised Machine Learning with Hyper-Parameter Optimization

Priya R. Maidamwar
G H Raisoni University, Amravati
Dr. Mahip M. Bartere
G H Raisoni University, Amravati
Dr. Prasad P. Lokulwar
G H Raisoni College of Engineering, Nagpur

Received 2022 April 02**; Revised** 2022 May 20**; Accepted** 2022 June 18

Intrusion detection systems are the foundation of network security (IDS). In order to detect intrusions, IDSs keep a check on the system's activity and behaviour. Various IDS models, such as misuse detection and anomaly detection, can be used to identify attacks at all levels. For both known and undiscovered attacks, anomaly detection has a high rate of false positives, but misuse detection has a high rate of detection accuracy for only known assaults. This r presents an intrusion detection system that use machine learning to solve the shortcomings of current approaches.This research proposes the Hybrid IDS, which employs various supervised machine learning techniques in which Grid search hyper-parameter optimization for Binary and Multiclass classification systems with univariate feature selection is used. Random forest and the multi-layer perceptron neural network algorithm are utilised in supervised machine learning methods. UNSW-NB15, a dataset developed in 2015, is used to evaluate the suggested model's performance. Dataset splitting, data preprocessing, feature extraction and selection, and model training, hyper-parameter tuning, and classification are the four steps of the proposed hybrid intrusion detection algorithm. In terms of intrusion detection, the results obtained show that the suggested model is successful, and it is able to increase accuracy and minimise FAR. In addition, the time it takes to process a request is very minimal.

Keywords— Feature Selection;Intrusion Detection System;IDS;Multilayer Perceptron Neural Network(MLPNN);Random Forest(RF);UNSW-NB15 Dataset

1. INTRODUCTION

As the number of online services has increased at an exponential rate, so has the number of computing devices and people connected to computer networks and the Web. Security problems and intrusive behaviour have led in the leaking of sensitive data, interruptions and unauthorised access to web-based services and systems, as well as unauthorised use of scarce resources. Maintaining network security may be one of the most important considerations for preventing any unwanted actions. As well as safeguarding data and preventing potentially dangerous situations, it is important (Moustafa and Slay, 2017). For a long time, network security has been a top priority, and many configurations have been implemented to that end. The term "network interruption" refers to a disruptive event that disrupts the flow of information across an organisation. It's also the cause of periodic disruptions in network administration. When it comes

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452

to web digital security, startling anomalies occur frequently, causing enormous harm to the internet as a whole. As a result, the security architecture must be dependable, strong, and well-organized. There are two main types of network intrusion detection systems: signature-based and anomaly-based. It is possible to use signature-based detection systems to look for unusual bytes or packet sequences in network data.A major shortcoming of this method is that signature patterns are considerably easier to construct and comprehend if you know what network traffic pattern you are looking for. This form of attention has very significant drawbacks. They can only detect assaults for which a signature has been created. They are unable to identify any new threats because the detection technology does not recognise their signatures. Analyzing network traffic patterns and characteristics is part of an anomaly-based detection method. High-volume traffic, an increase in traffic to or from a particular host, and an imbalance in network load can all be used in this detection technique to spot unusual activity(Meftah et al., 2019). This approach has the drawback of not detecting malicious activity as an anomaly if it is part of normal network activity. When compared to signature-based approaches, this method has the advantage of being able to detect novel attacks that have no known signature.

Detecting intrusions is vital to network security, data confidentiality, classified data security, and preventing unwanted access to classified information. Several approaches to detecting network intrusions have been put forth. Anomaly network intrusion detection is a critical component of network security (Mebawondu et al., 2020). Anomaly's behaviour may appear similar to that of normal data utilisation. It's difficult to distinguish between normal and abnormal behaviour in an effective and efficient manner in anomaly detection. The idea of machine learning has been broadened in order to create an effective intrusion detection system. These days, machine learning is a vital part of current intrusion detection systems. Anomaly detection systems appear to benefit from the use of machine learning approaches that mix signature-based and behavior-based systems to boost classification performance and speed(Kamarudin et al., 2017).

This paper presents a hybrid IDS employing two supervised machine learning algorithm with a univariate feature selection and anomaly detection system. Given the challenges of previous IDSs, the novel feature selection approach has the potential to yield an optimal feature subset. The first novelty is the proposal of a new set of precise hyper-parameter values for supervised algorithm training in order to reduce false alarm rates while concurrently raising true positive rates, while also lowering the number of features to improve low learning and computing time. The second novelty is detecting anomalies by integrating feature optimization with Random Forest (RF) and Multi-layer Perceptron Neural Network (MLPNN). Because of its training speed and scalability, RF and MLPNN are strong candidates for classifiers among all Supervised Machine Learning algorithms. Previous research has also demonstrated that this approach performs well and has a greater detection accuracy than other supervised machine learning algorithms. To attain a high level of generalisation accuracy, the prediction output from base-level classifiers is used. This algorithm has the advantage of considerably improving the generalisation of the learning algorithm and so producing better outcomes.The remainder of the paper is laid out as follows: Section II reviews related research on existing IDS models, section III explains the suggested methodology, which is implemented using

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452

machine learning techniques, section IV exhibits experiments and comparison findings with other IDS models, and section V concludes the proposed system.

2. MATERIALS AND METHODS

2.1 UNSW-NB15 Dataset

From the University of New South Wales, the UNSW-NB15 dataset contains network intrusion data. DoS, malware, backdoors, and fuzzers are among the nine attacks. Figure 1 (Kamarudin et al., 2017)depicts the framework architecture to generate UNSW-NB15 Dataset. The collection includes raw network packets. It has a total of 175,341 records in the training set, and 82,332 records in the testing set(Kanimozhi and Jacob, 2019). As depicted in Figure 2(Kamarudin et al., 2017), the IXIA PerfectStorm was programmed in the Cyber Range Lab of UNSW Canberra to generate a hybrid of real modern normal activities and synthetic contemporary assault behaviours. tcpdump was used to capture 100 GB of traffic in raw form (e.g., Pcap files). This dataset contains nine different types of attacks: Analysis(A), Fuzzers(F), Backdoors(B), Exploits(E), Denial of Service(D), Reconnaissance(R), Generic(G), Worms(W), and Shellcode(S).

The Argus and Bro-IDS tools are used to generate 49 total characteristics with the class label, and twelve methods are developed (Primartha and Tama, 2018). These features are detailed in the UNSW-NB15 features.csv file. Additionally, the dataset information is described in Table I-II.

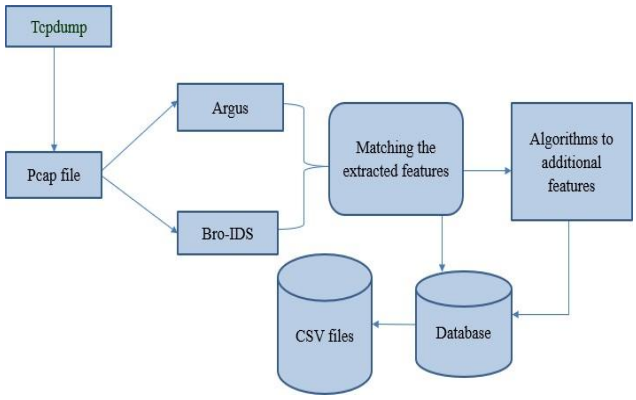


Figure 1: Framework Architecture to generate UNSW-NB15 Dataset

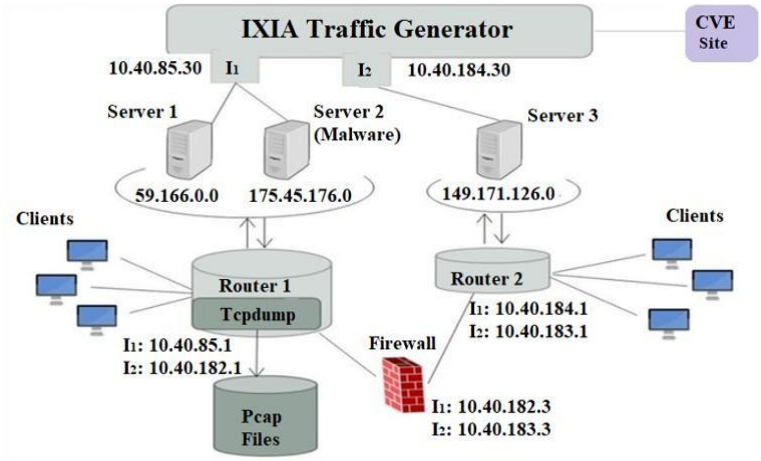


Figure 2: UNSW-NB15 TestBed

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452

TABLE I: UNSW-NB15 Dataset Distribution

Category	Training set	Testing set
Worms	130	44
Shellcode	1,133	378
Reconnaissance	10,491	3,496
Generic	40,000	18,871
Fuzzers	18,184	6,062
Exploits	33,393	11,132
DoS	12,264	4089
Backdoor	1,746	583
Analysis	2,000	677
Normal	56,000	37,000
Total Records	175,341	82,332

TABLE II: Statistics of UNSW-NB15 Dataset

Type	Records	Description
Worms	174	Attacker reproduces itself to spread to different PCs. Frequently, it utilizes a PC organization to spread itself, depending on security disappointments on the objective PC to get to it (Roy and Cheung, 2019).
Shellcode	1,511	A little piece of code utilized as the payload in the abuse of programming weakness (Moustafa et al., 2019).
Reconnaissance	13,987	Contains all Strikes that can recreate assaults that assemble data (Meftah et al., 2019).
Generic	215,481	A method neutralizes all block codes (with a given block and key size), without thought about the design of the block code(Roy and Cheung, 2019).
Exploits	44,525	The assailant is aware of a security issue inside a working framework or a piece of programming and use that information by taking advantage of the weakness (Moustafa et al., 2019).
DoS	16,353	A malignant endeavor to make a server or an organization asset inaccessible to clients, as a rule by briefly hindering or suspending the administrations of a host associated with the Web (Sonule et al., 2020).
Backdoors	2,329	A method wherein a framework security system is bypassed covertly to get to a PC or its information[9].
Analysis	2,677	It contains various assaults of port scan, spam and html records infiltrations (Moustafa et al., 2019).

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452

Fuzzers	24,246	Endeavoring to cause a program or organization suspended by taking care of it the arbitrarily produced information (Belouch et al., 2018).
Normal	2,218,761	Regular exchange information (Roy and Cheung, 2019).

2.2 **Methodology**

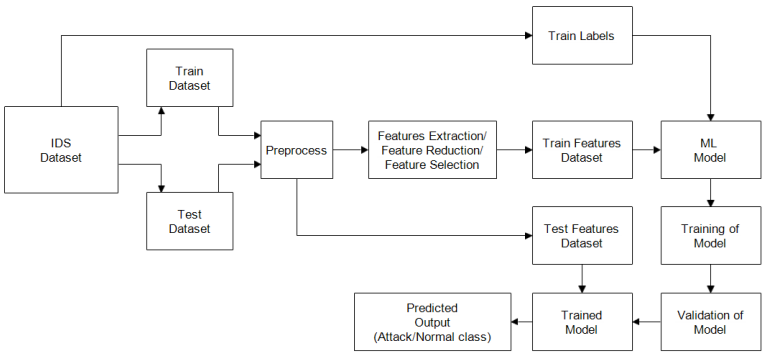


Figure 3: Proposed Block Diagram for Classification of Intrusion Detection

Using the UNSW-NB15 dataset, a new IDS classification model was trained and tested in Figure 3. The proposed approach incorporates the following steps:

(i) Dataset Splitting

To use a machine learning approach to train a model based on the IDS dataset, the data must be split into train and test sets. As a result, we adopted an 70:30 split ratio in our implementation, where 70% of the data was used for training and 30% for testing the model that was built from it.

(ii) Data Preprocessing

A thorough pre-processing procedure must be carried out before training because of the sheer number and size of the data. There is a chance that some data is missing or corrupted, so this is the first thing to look into(Elhefnawy et al., 2020). Only the "service" feature remains to be collected for UNSWNB 15, and it will be removed from the sample as a result of this finding in order to reduce noise.

(iii) Feature Extraction and Selection

Once the UNSWNB 15 dataset has been cleaned and formatted, a preliminary feature selection is needed to help guide the test of horizontal complexity. Preprocessing and feature extraction techniques are used to extract features from the training and testing datasets[14].

(iv) Model Training, Hyper Parameter Tuning and Classification

Random Forest (RF) and Multi-layer Perceptron Neural Network (MLPNN) are the two methods of supervised machine learning, are used to train the model. Ten-fold cross-validation of the random forest (RF) technique is utilised. It's possible to rank features based on the cleanliness of the nodes in Random Forest's tree-based method. In order to use RF, a feature is allocated a score when building multiple decision trees. Using this function on one or more tree nodes results in a reduction in the total forest pollution score. As a result of scaling, the significance of the feature

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452

can be calculated(Sumaiya Thaseen et al., 2020).

In order to teach trees, the Random Forest Training Algorithm employs techniques such as bootstrap aggregation and bagging. In this case, bagging takes random samples instead of the training set and fits the tree to these random samples, increasing the number of random samples in the training set[8]. Substituted samples and training samples from X and Y are available when b = 1. This is Xb, Yb. By summing all separate regression trees on x', you can predict the hidden sample x' after training:

$$\hat{f}=\frac{1}{B}\sum_{b=1}^{B} f_b\ (x')$$

A multilayer perceptron is a neural feedforward classifier that is fully connected. A minimum of three node layers comprise the MLP: an input layer, a hidden layer, and an output layer. The input node is the only node that employs a nonlinear activation function for all other nodes. Backpropagation, a supervised learning approach, is used to train MLPs. MLP is distinct from linear perceptrons because of its complexity and non-linear activation. The input vector x can be subjected to a set of fixed nonlinear transforms j to generalise these networks. For a single output network:

$$\mathbf{y(x, w) = g}\sum_{j=1}^{M} W_j \emptyset_j(x)$$

Effective parameters must be modified or adjusted to get the best classification result from the set while learning via hyperparameter tuning. The Grid Search Algorithm is used to optimise Hyperpaprameters..

Algorithms

Input:
Training and Testing instance set S, a vector of feature values and the class i.e. label value
Feature Set F(i) = {f1(i), f2(i),…..fn(i)}
Label Se L(i) = {Attack(1), NORMAL(0)}

ization:
Collect and Prepare feature data and label data from raw dataset values from UNSW Dataset.

essing Phase:
For each feature data
Calculate the normalized value of all features set.
Scale the all feature data into specific range.
Parameter Hyper tuning Phase
***Step3*:** Define the model for RF and MLP.
***Step4*:** Define the range of possible value for all hyperparameters of ML algorithms.
RF: {'C', 'random_state', 'penalty', 'n_jobs'}
MLP: { 'hidden_layer_sizes', 'max_iter' , 'activation', 'solver', 'alpha', 'learning_rate'}
Step5: Sampling of hyper parameters values using Grid Search CV Function.
Step6: Evaluate and find the best score among all hyper parameters value.
Step7: Validate the model using K-Fold Validation Learning Method.

Training Phase:
Step8: Initialize the parameter tuned for ML model of RF and MLP.
Step9: Initialize the feature data and label data for training dataset.
Step10: Train the model for respective ML algorithms.
Step11: Validate the model performance using K-fold cross validation method.
Step12: If validation successful then save the trained model TMrf, TMmlp and if not the repeat from step 8.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452

Testing Phase:

Step13: Initialize the feature data for testing dataset.

Step14: Load the trained model of ML algorithms.

Step15: Predict the results whether its Attack (1) or Normal (0).

Step16: Plot Confusion matrix between Actual Label Data and Predicted Label Data to check system accuracy.

Evaluation Phase:

Step 17: Evaluate performance of classification model C based on ROC, Confusion Matrix Parameters based TP, FP, TN and FN.

3. RESULTS AND DISCUSSION

3.1 Experimental Setup

The UNSW-NB15 dataset has been used in this research for classification of intrusion detection. An Intel i5 CPU running at 2.80 GHz, 16GB of RAM, and Windows 10 (64-bit) operating system were used for the classification, which was carried out exclusively with Pycharm IDE, Anaconda distribution, and Scikit Learn Machine Learning Toolkit.

3.2 Experimental Results and Performance Analysis

Random Forest (RF) and Multi-layer Perceptron Neural Networks (MLPNN) were evaluated on the proposed data set for identifying harmful events in several tests.

A variety of metrics, such as accuracy, precision, recall, false-positive rate, and ROC curves, are employed in the pursuit of this goal. True Positive (TP), True Negative (TN), False Negative (FN) and False Positive (FP) are the four terms used in these measures (FP). The terms TP, TN, FN, and FP represent the number of actual anomalous records that were detected as attacks, the number of actual legitimate records that were detected as normal, the number of actual anomalous records that were classified as normal, and the number of actual legitimate records that were classified as attacks (Moustafa et al., 2019).

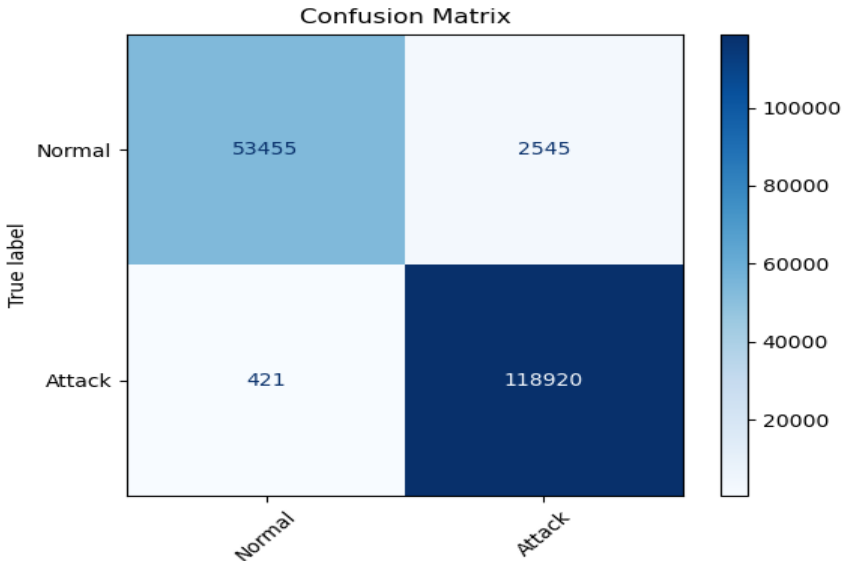
Table III shows the tuned parameters used to train the classification model using Random Forest and Multilayer Perceptron classifier. The classification report from Scikit Learn Toolkit, in which Precision, Recall, and F-score are evaluated and displayed in Table IV-V for both methods, was used to examine the parameters of the proposed model.

Table III: Hyper parameter tuning details for classifiers

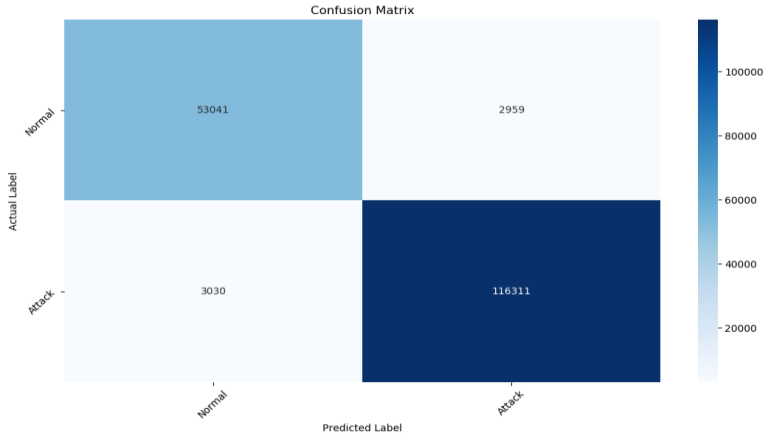
Classifiers	**Model Parameters**	**Search Range**	**Binary Classifier Selected Range**	**Multclass Classifier Selected Range**
Random Forest	n_estimators	[10, 100, 1000]	1000	10
	max_features	[10, 100, 500]	500	100
	max_depth	[10, 40, 70, 100]	70	40
	min_samples_split	[2, 5, 10]	10	5
	max_leaf_nodes	[50, 100, 200]	100	50
	random_state	[10, 40, 70,	100	100

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452

		100]		
Multilayer Perceptron	hidden_layer_sizes max_iter activation solver alpha learning_rate	[(100 , 50, 10) , (50,), (100,)] [500, 1000] ['tanh', 'relu'] [' sgd ' , ' adam ', ' lbfgs '] [0.0001, 0.05] [' constant ', ' adaptive ']	(100,50,10) 1000 Tanh sgd 0.0001 Adaptive	100 500 Tanh sgd 0.0001 Adaptive



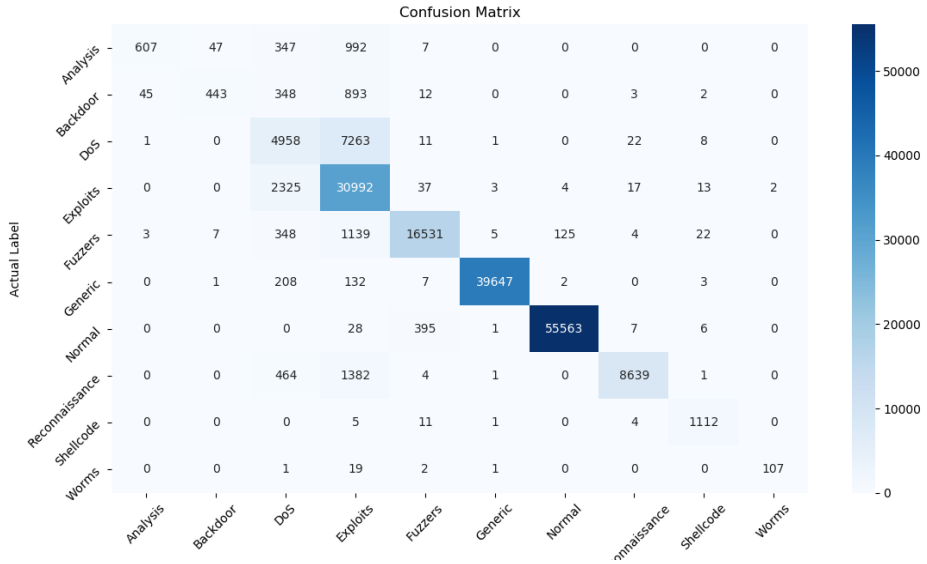
a)



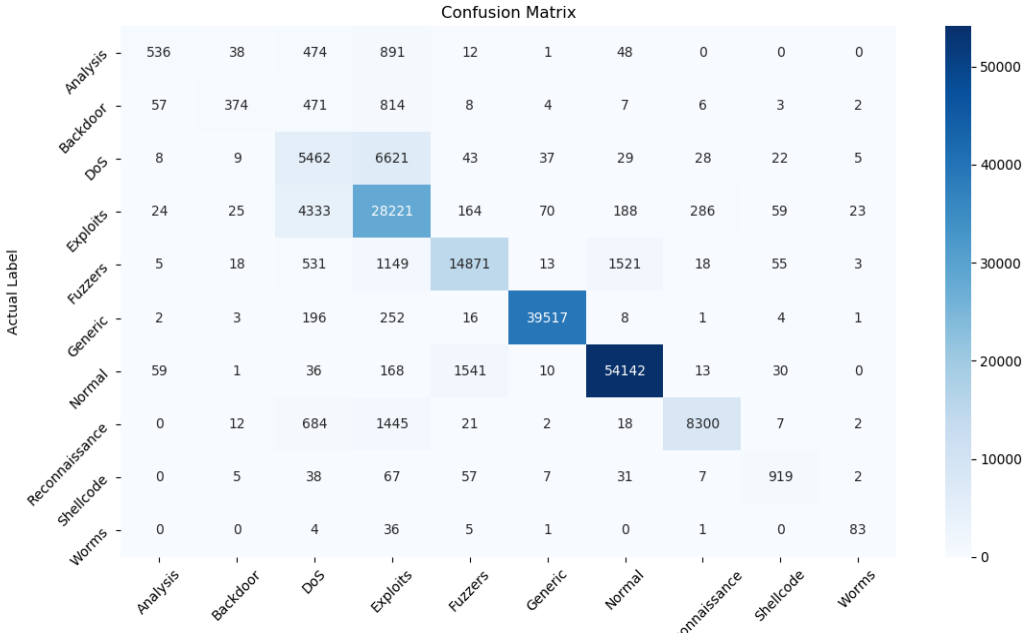
b)

Figure 4: Confusion matrix of Binary Classification using a) RF classifier b) MLP Classifier

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452



a)



b)

Figure 5: Confusion matrix of Multiclass Classification using a) RF classifier b) MLP Classifier

Figure 4-5 shows the confusion matrix for binary and multiclass classification using two classifiers, the proposed approach is applied to a UNSW-NB15 dataset and the predicted output as normal or malicious attack is compared to the actual label for various attacks.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452

In terms of precision, recall, and f-score, Table IV presents the classification report parameters for Binary classification for the normal and attack output categories. Random Forest algorithms are clearly superior to Multi-layer perceptron algorithms in terms of all parameter values. For multiclass classification, classification report parameters for 10 type of attacks has been displayed as shown in table V, from all type of attacks, Generic and Normal type is effectively categorized with maximum accuracy for both classifiers. Figure6 and 7 shows the graphical illustratation of performance of both classification system.

Table IV: Classification Report Parameter Values for Binary Classification

Classes	Precision		Recall		F-score	
	Random Forest	Multilayer Perceptron	Random Forest	Multilayer Perceptron	Random Forest	Multilayer Perceptron
Normal	99	95	99	95	99	95
Attack	99	98	100	97	100	97

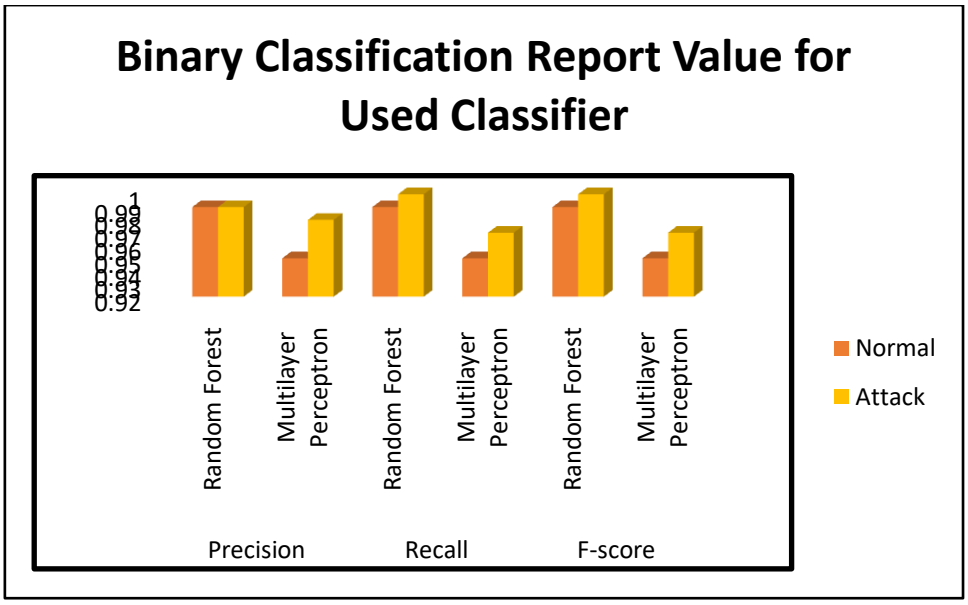


Figure 6: Classification Report Parameter Comparison for Binary Classification

Table V: Classification Report Parameter Values for Multiclass classification

Classes	Precision		Recall		F-score	
	Random Forest	Multilayer Perceptron	Random Forest	Multilayer Perceptron	Random Forest	Multilayer Perceptron
Analysis	93	78	30	27	46	40
Backdoor	89	77	25	21	39	34
DoS	55	45	40	45	47	45

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452

Exploits	72	71	93	85	81	77
Fuzzers	97	89	91	82	94	85
Generic	100	100	99	99	100	99
Normal	100	97	99	97	99	97
Reconnaissance	99	96	82	79	90	87
Shellcode	95	84	98	81	97	82
Worms	98	69	82	64	90	66

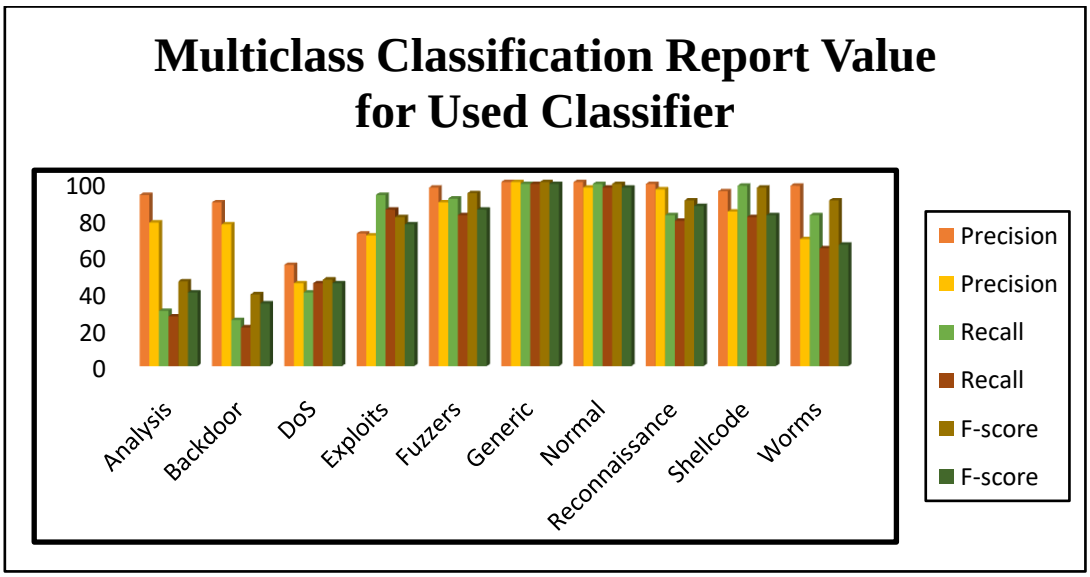


Figure7: Classification Report Parameter Comparison for MultiClass Classification

Table VI: Overall System Performance for Binary Classification

Evaluation Metrics	**Binary Classification System**	
	Random Forest	**Multilayer Perceptron**
Accuracy	99.34	96.58
Precision	99.34	96.59
F1 Score	99.34	96.58
Kappa Score	98.48	92.15
Matthews Correlation Coefficient	98.48	92.15
Recall	99.34	96.58

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452

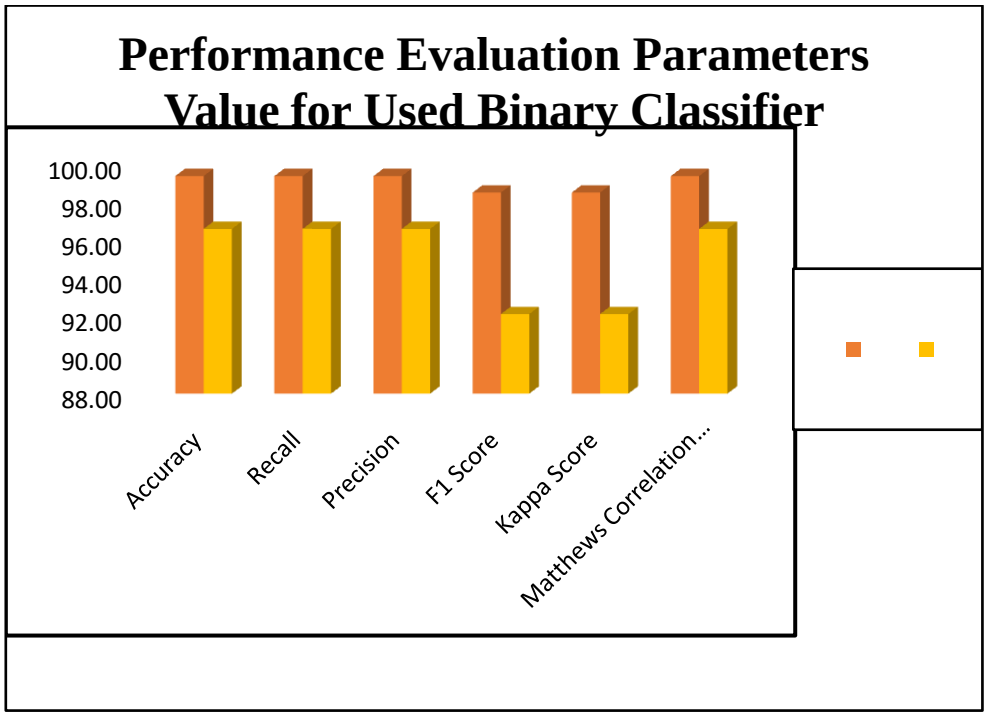


Figure 8: Overall System Performance Parameter for Binary Classification

The overall performance in terms of Accuracy, Matthews' Correlation Coefficient (MCC), and Kappa Score for binary and multiclass classification are shown in Table VI and VII. All performance parameters, Accuracy, Precision, F1 Score, Kappa Score, Matthews Correlation Coefficient and Recall are efficient for Random Forest algorithms for binary classification system. Figure 8 and Figure 9 shows the graphical relevance of overall performance of proposed

Table VII: Overall System Performance for MultiClass Classification

Evaluation Metrics	**Classifiers System**	
	Random Forest	**Multilayer Perceptron**
Accuracy	90.45	86.93
Recall	90.45	86.93
Precision	90.95	87.48
F1 Score	89.96	86.73
Kappa Score	87.82	83.36
Matthews Correlation Coefficient	88.02	83.45

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452

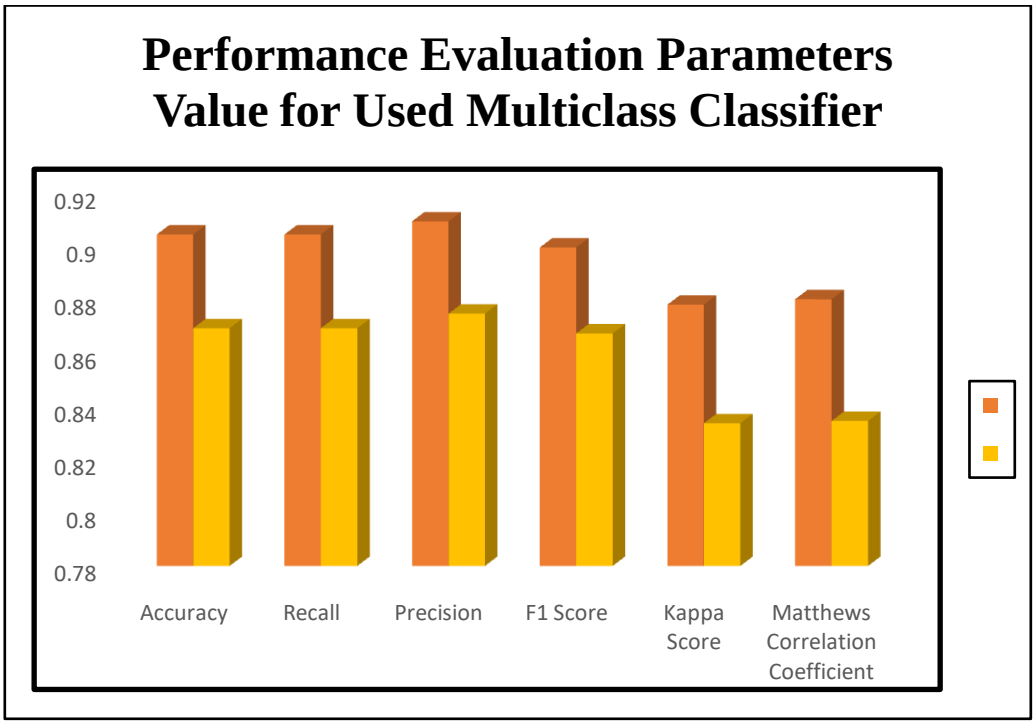


Figure 9: Overall System Performance Parameter for Multiclass Classification

Table 8 shows the system performance parameters for each class for binary classification using RF and MLP. This results shows that sensitivity and positive predictive value is significantly best using RF classifier than MLP. Table IX-1X shows the attackwise performance parameters in multiclass classification system. From this table, Generic, Normal and Shellcode are the best performing category using RF classifier. Figure 10, 11 and 12 shows the graphical performance of system for both type of classification system.

Table VIII: System performance parameter for each class for Binary Classification using RF and MLP

Evaluation Metrics	**Classifiers System**	
	Random Forest	**Multilayer Perceptron**
Sensitivity	99.65	97.46
Specificity	98.68	94.72
Positive Predictive Value	99.38	97.52
Negative Predictive Value	99.25	94.60
False Positive Rate	1.32	2.54
False Negative Rate	0.35	2.54

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452

Table IX: System performance parameter for each class for multiclass classification using RF

Evaluation Metrics	Random Forest									
	Analysis	**Backdoor**	**DoS**	**Exploits**	**Fuzzers**	**Generic**	**Normal**	**Reconnaissance**	**Shellcode**	**Worms**
Sensitivity	30.35	25.37	40.43	92.81	90.91	99.12	99.22	82.35	98.15	82.31
Specificity	99.97	99.97	97.52	91.65	99.69	99.99	99.89	99.97	99.97	100.00
Positive Predictive Value	92.53	88.96	55.10	72.34	97.14	99.97	99.76	99.34	95.29	98.17
Negative Predictive Value	99.20	99.25	95.61	98.19	98.96	99.74	99.63	98.89	99.99	99.99
False Positive Rate	0.03	0.03	2.48	8.35	0.31	0.01	0.11	0.03	0.03	0.00
False Negative Rate	69.65	74.63	59.57	7.19	9.09	0.88	0.78	17.65	1.85	17.69

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452

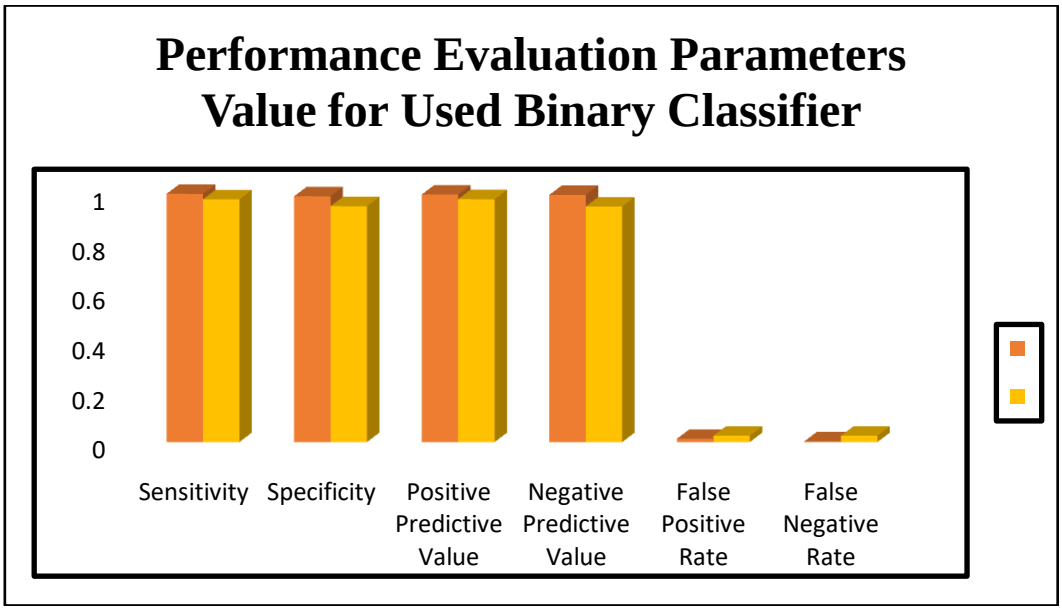


Figure 10: System performance Parameter for each class for Binary Classification

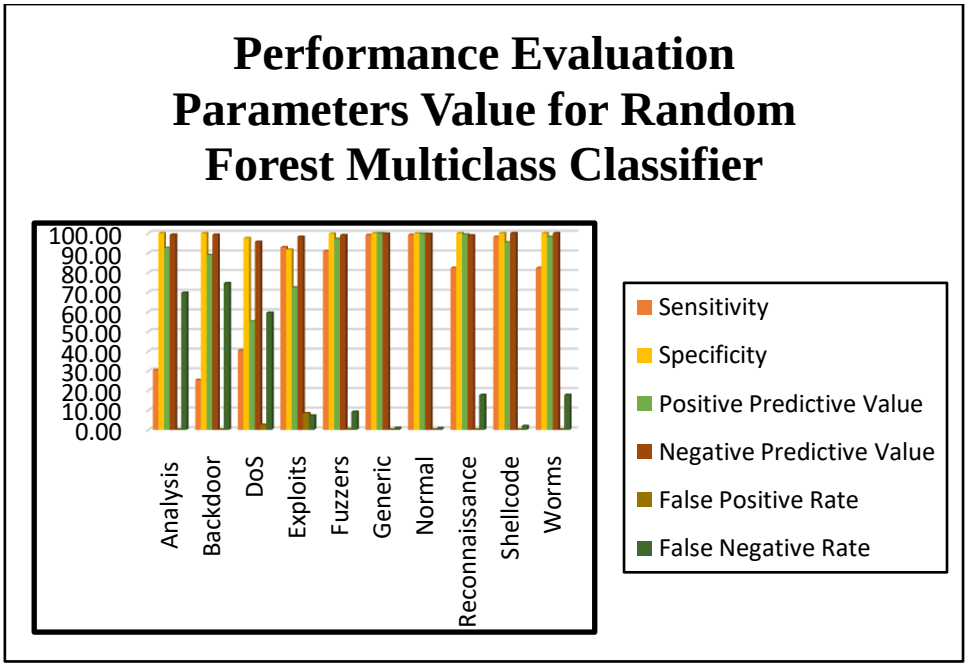


Figure 11: System Performance Parameter for each class for Multiclass Classification using RF

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452

Table X: System performance parameter for each class for multiclass classification using MLP

Evaluation Metrics	Multilayer Perceptron									
	Analysis	**Backdoor**	**DoS**	**Exploits**	**Fuzzers**	**Generic**	**Normal**	**Reconnaissance**	**Shellcode**	**Worms**
Sensitivity	26.80	21.42	44.54	84.51	81.78	98.79	96.68	79.12	81.11	63.85
Specificity	99.91	99.94	95.85	91.94	98.81	99.89	98.45	99.78	99.90	99.98
Positive Predictive Value	77.57	77.11	44.66	71.15	88.85	99.63	96.70	95.84	83.62	68.60
Negative Predictive Value	99.16	99.22	95.83	96.19	97.91	99.64	98.44	98.69	99.88	99.97
False Positive Rate	0.09	0.06	4.15	8.06	1.19	0.11	1.55	0.22	0.10	0.02
False Negative Rate	73.20	78.58	55.46	15.49	18.22	1.21	3.32	20.88	18.89	36.15

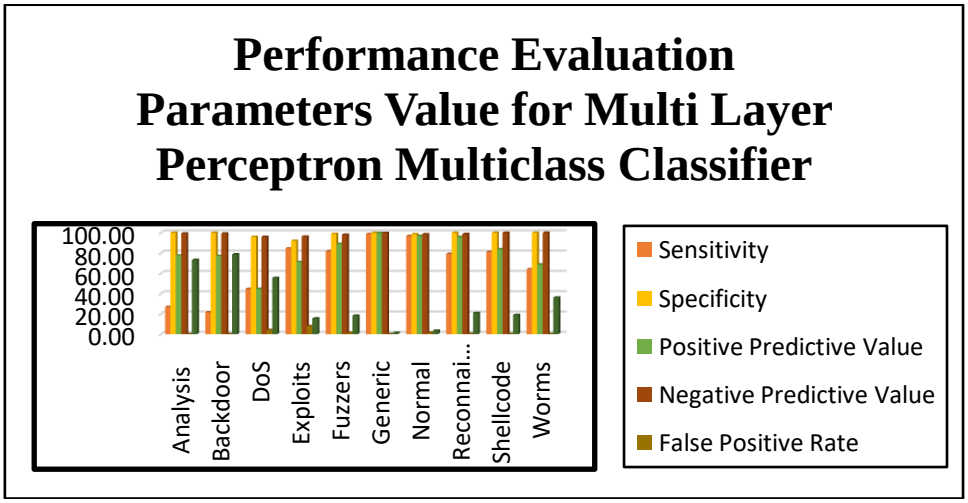
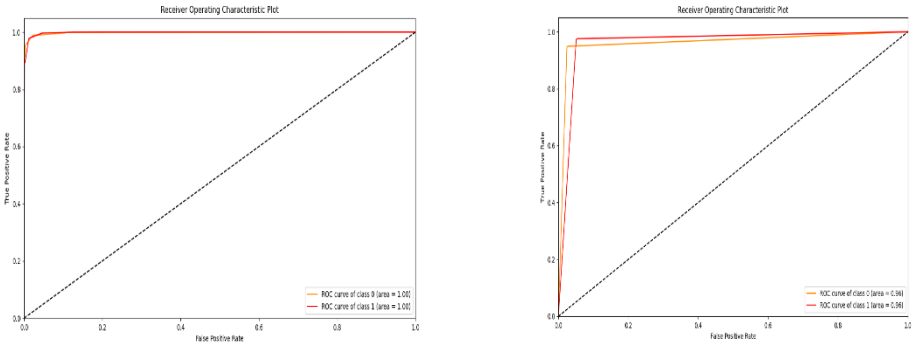


Figure 12: System performance Parameter for each class for Multiclass Classification using MLP

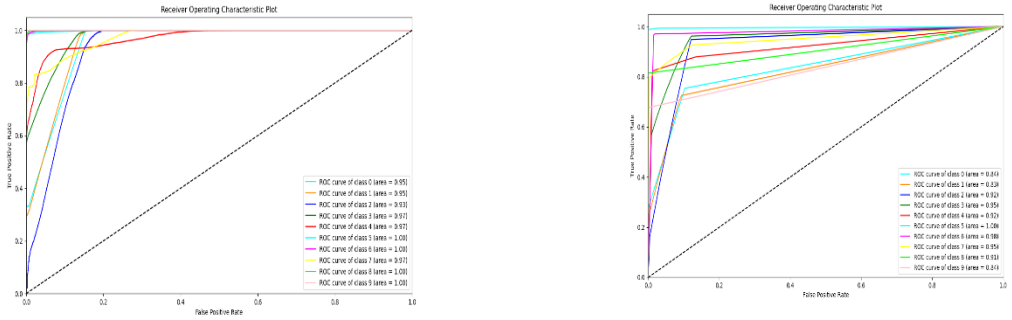
JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452

Figure 13-14 shows the a Receiver Operating Characterstics (ROC) graph for both binary and multiclass classification systems using two classifier RF and MLP. It is found that Area Under Curve (AUC) is marginally higher for binary classification system and in multiclass, class 5, 6 and 8, means Generic, Normal and Shellcode has higher AUC.



a) b)

Figure 13: ROC Graph for Binary Classification using a) RF b) MLP



a) b)

Figure 14: ROC Graph for Multiclass Classification using a) RF b) MLP

The performance of proposed best performing algorithm i.e. Random Forest with grid search hyper parameter tuning is compared with existing models in Table XI, which indicates the proposed system is efficient in comparison to existing approaches.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No.3, 2022, p.1532-1550
https://publishoa.com
ISSN: 1309-3452

Table XI: comparative analysis for Binary classification system

Models / Evaluation Metrics	**SVM**(Gharaee and Hosseinvand, 2017)	**RF [**(Primartha and Tama, 2018)	**DT+RF** (Belouch et al., 2018)	**DL** (Meftah et al., 2019)	**GFA** (Elhefnawy et al., 2020)	**HT-RF [Our Work]**
Accuracy	98.76%	95.5%	97.49%	82.11%	90.24%	99.34%
Sensitivity	-	-	93.53%	-	-	99.65%
Specificity	-	-	97.75%	-	-	98.68%
False Positive Rate	0.09%	7.22%	-	-	13.03%	1.32%
False Negative Rate	1.35%	-	-	-	-	0.35%

4. CONCLUSION

For training a Binary and Multi-class Classifier, more hyper-parameter adjustment is required than in previous studies, hence this study summarised the results of the most widely used benchmark intrusion detection dataset UNSW-NB15. The techniques proposed have used a Random forest Classifier and a Multi-layer Perceptron Neural Network to produce an excellent binary and multi-class classification. For the dataset, the proposed methods result in an intrusion detection system with a very high overall level of accuracy. As a consequence, it was found that the proposed method is significantly more efficient than the current strategy

CONFLICT OF INTEREST

In this manuscript entitled “Classification of Hybrid Intrusion Detection System Using Supervised Machine Learning with Hyper-Parameter Optimization” has no conflict of interest as declared by the Authors.For this manuscript, no animals or human being has affected. No organization has funded for the procedure.

REFERENCES

1. Belouch, M., Hadaj, S. El, Idhammad, M., 2018. ScienceDirect Procedia Computer Science Performance evaluation of intrusion detection based on machine learning using Apache Spark. Procedia Comput. Sci. 127, 1–6.
2. Elhefnawy, R., Abounaser, H., Badr, A., 2020. A hybrid nested genetic-fuzzy algorithm framework for intrusion detection and attacks. IEEE Access 8, 98218–98233. https://doi.org/10.1109/ACCESS.2020.2996226
3. Gharaee, H., Hosseinvand, H., 2017. A new feature selection IDS based on genetic algorithm and SVM. 2016 8th Int. Symp. Telecommun. IST 2016 139–144. https://doi.org/10.1109/ISTEL.2016.7881798
4. Kamarudin, M.H., Maple, C., Watson, T., Safa, N.S., 2017. A LogitBoost-Based Algorithm for Detecting Known and Unknown Web Attacks. IEEE Access 5, 26190–26200. https://doi.org/10.1109/ACCESS.2017.2766844
5. Kanimozhi, V., Jacob, P., 2019.

UNSW-NB15 dataset feature selection and network intrusion detection using deep learning. Int. J. Recent Technol. Eng. 7, 443–446.

6. Mebawondu, J. Olamantanmi, Alowolodu, O.D., Mebawondu, Jacob O., Adetunmbi, A.O., 2020. Network intrusion detection system using supervised learning paradigm. Sci. African 9, e00497. https://doi.org/10.1016/j.sciaf.2020.e00497
7. Meftah, S., Rachidi, T., Assem, N., 2019. Network based intrusion detection using the UNSW-NB15 dataset. Int. J. Comput. Digit. Syst. 8, 477–487. https://doi.org/10.12785/ijcds/080505
8. Moustafa, N., Slay, J., 2017. A hybrid feature selection for network intrusion detection systems: Central points 5–13. https://doi.org/10.4225/75/57a84d4fbefbb
9. Moustafa, N., Slay, J., Creech, G., 2017. Novel Geometric Area Analysis Technique for Anomaly Detection Using Trapezoidal Area Estimation on Large-Scale Networks. IEEE Trans. Big Data 5, 481–494. https://doi.org/10.1109/tbdata.2017.2715166
10. Moustafa, N., Turnbull, B., Choo, K.K.R., 2019. An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. IEEE Internet Things J. 6, 4815–4830. https://doi.org/10.1109/JIOT.2018.2871719
11. Primartha, R., Tama, B.A., 2018. Anomaly detection using random forest: A performance revisited. Proc. 2017 Int. Conf. Data Softw. Eng. ICoDSE 2017 2018-Janua, 1–6. https://doi.org/10.1109/ICODSE.2017.8285847
12. Roy, B., Cheung, H., 2019. A Deep Learning Approach for Intrusion Detection in Internet of Things using Bi-Directional Long Short-Term Memory Recurrent Neural Network. 2018 28th Int. Telecommun. Networks Appl. Conf. ITNAC 2018 1–6. https://doi.org/10.1109/ATNAC.2018.8615294
13. Sonule, A., Kalla, M., Jain, A., Chouhan, D.S., 2020. Unsw-Nb15 Dataset and Machine Learning Based Intrusion Detection Systems. Int. J. Eng. Adv. Technol. 9, 2638–2648. https://doi.org/10.35940/ijeat.c5809.029320
14. Sumaiya Thaseen, I., Poorva, B., Ushasree, P.S., 2020. Network Intrusion Detection using Machine Learning Techniques. Int. Conf. Emerg. Trends Inf. Technol. Eng. ic-ETITE 2020 30–35. https://doi.org/10.1109/ic-ETITE47903.2020.148
15. The UNSW-NB15 Dataset, https://research.unsw.edu.au/projects/unsw-nb15-dataset