iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VI **Month of publication:** June 2021

DOI: https://doi.org/10.22214/ijraset.2021.34922

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

A Study of Machine Learning Algorithms for DDoS Detection

Sheikh Shehzad Ahmed[1], Sagar R Shet[2]
[1, 2]*Department of Information Science and Engineering, RV College of Engineering, Bengaluru, India*

Abstract: ***The Internet is used practically everywhere in today's digital environment. With the increased use of the Internet comes an increase in the number of threats. DDoS attacks are one of the most popular types of cyber-attacks nowadays. With the fast advancement of technology, the harm caused by DDoS attacks has grown increasingly severe. Because DDoS attacks may readily modify the ports/protocols utilized or how they function, the basic features of these attacks must be examined. Machine learning approaches have also been used extensively in intrusion detection research. Still, it is unclear what features are applicable and which approach would be better suited for detection. With this in mind, the research presents a machine learning-based DDoS attack detection approach. To train the attack detection model, we employ four Machine Learning algorithms: Decision Tree classifier (ID3), k-Nearest Neighbors (k-NN), Logistic Regression, and Random Forest classifier. The results of our experiments show that the Random Forest classifier is more accurate in recognizing attacks.***

Keywords: Distributed Denial of Service (DDoS), Logistic Regression, K Nearest Neighbor (KNN), Decision Tree, Random Forest, Receiver operating characteristic (RoC).

I. INTRODUCTION

DDoS (Distributed Denial of Service) is a comparably simple but effective method of attacking the Internet and system resources. Multiple distributed agents instantly consume specific critical target resources and refuse to deliver services to authorized consumers. The network is frequently overcrowded on the route from the sender to the destination, affecting the normal functioning of the Internet and denying many legitimate users to provide services [7]. Because DDoS attacks may readily modify the ports/protocols utilized or how they function, the basic features of these attacks must be examined. It is difficult to discern between an attack and normal behaviour just on the protocol and service used. As a result, detecting a DDoS attack is difficult [6]. The techniques for identifying such attacks get more complicated as technology progresses and also because there are so many different types of attacks. These include ICMP flooding, SYN flooding, IP packet flooding, and so on. A detector based on machine learning is a suitable alternative for resolving this issue [5]. This paper evaluates the machine learning algorithms used for DDoS detection, including feature extraction, classification, and comparison, based on an extensive analysis of the current challenges confronting DDoS research. As part of this evaluation, certain machine learning approaches for detecting DDoS have recently been created, which will be used in this evaluation. Their performance will be evaluated using publicly available reference data sets. The DoS/DDoS dataset is employed for the studies, and machine learning algorithms such as decision tree, knn, logistic regression, and random forest are used [8].

The following contributions are made by this work:

A. Using the KDDCup99 dataset, the method efficiently classifies DoS attacks.
B. In comparison to current systems, the proposed approach reduces the number of features while providing higher correct prediction rates (accuracy).
C. It depicts the process of selecting training data and the accuracy of the various ML algorithms.

II. LITERATURE REVIEW

M.A.G. Quraishi et al. [1] proposed several methods for mitigating DDoS attacks. To detect and block DDoS attacks in an SDN network, the researchers examined several machine learning techniques, including J48, Random Forest, SVM, and K-NN. It entailed training and deciding on the best model for the proposed network used for attack detection and mitigation. The results demonstrated that J48 outperforms the other evaluated algorithms, particularly training and testing time. This paper sparked the idea of using machine learning to detect such attacks.

In the study, Nguyen et al. [2] used the K-NN algorithm to classify the network status as normal, pre-attack, and DDoS class status in order to predict DDoS attacks. Packet type (UDP, ICMP, TCP, SYN), source/destination IP address, and port number are used as features to categorize packets into two pre-attack phases, a third attack phase, and a fourth normal phase. Other algorithms, such as Naive Bayesian, C4.5, and K-Means, were investigated in the paper by Zekri.et.al to binary classify DoS attacks primarily targeting layers 3 and 4 of the OSI 7-layer model, and achieved accuracy of 91.4%, 98.8%, and 85.9%, respectively.

A. M. Mahfouz, D. Venugopal et al. [3] developed a Network Intrusion Detection System (NIDS) that can identify both existing and novel forms of DDoS attacks. The created NIDS's important feature was the use of ensemble models to mix several classifiers, with the assumption that each classifier may target different types of intrusions. IDS was created using many ML techniques, including KNN, MLP, DT, and SVM. MLP is a neural network-based method that takes a long time to process and requires a large amount of data for training. KNN, on the other hand, works with fewer data with greater accuracy, even when it is noisy. As a result, we presume KNN is one of the algorithms for this proposed model.

N. Apthorpe, R. Doshi, and N. Feamster [4] evaluated five different ML classifiers using a dataset of normal and DoS attack traffic collected from a sample IoT device network. The classifier was trained using 85 percent of the total normal and malign traffic, and accuracy was determined using the remaining traffic as a test set. The four classifiers' accuracies varied from around 0.91 to 0.99. The results show that the Random Forest has higher accuracy than KNN but is slower. As a result, we decided to employ both methods for our study.

III.METHODOLOGY

The following section primarily consists of a description of the steps taken, as shown in Fig. 1:

A. Data Gathering

Data gathering also called Data collection is the method of obtaining and analysing information from a wide range of sources.

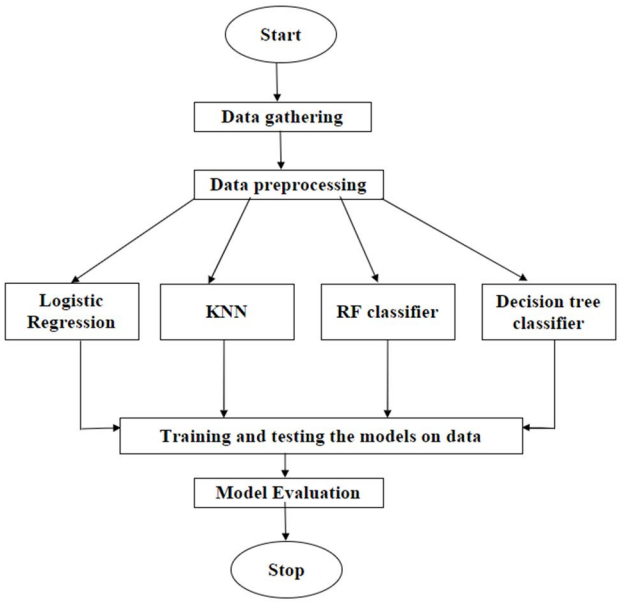


Fig. 1 Workflow of the methodology

The KDDCup99 dataset was used in this study, which is a 10% stratified subsample of the data from the 1999 ACM KDD Cup. It has 42 features, some of which are listed in the Fig. 2 below.

Feature Name	Feature Name
duration	num_failed_logins
protocol_type	is_host_login
service	srv_rerror_rate
src_bytes	srv_count
dst_bytes	count
logged_in	dst_host_count

Fig. 2. List of features

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

B. Data Pre-processing

The method of cleaning the collected raw data and transforming it into a clean data collection is known as data pre-processing [14]. The data collected from several sources is obtained in a raw format that is unsuitable for analysis. As a result, the data is cleaned up and transformed into a new data set. The following pre-processing steps were done:

1) The tuples of ICMP packets were extracted from the dataset and stored in a new data frame.
2) The features relevant to the detection were extracted as "priori" for processing.
3) The normal results and the classes of attack were replaced with 0 and 1 respectively.

In our case, 70% of the data was utilized for training and the rest 30% for testing.

C. Machine Learning Algorithms

The basic goal is to use the pre-processed data to train the highest performing model feasible. It is a classification problem, where the output variable is a type, such as "disease" or "no disease," or "spam" or "not spam," or, in our case, "DDoS attack" or "normal" [14]. Because our primary goal is to determine whether or not the network is vulnerable to DDoS attacks, the issue falls within the categorization area (binary classification). The machine learning algorithms used are:

1) *Logistic Regression*: Logistic regression is the best regression strategy to use when the dependent variable is dichotomous (binary). Like other regression studies, logistic regression is a statistical study. Logistic regression is a method used to describe and illustrate the relationship between one dependent binary variable and one or more independent variables.
2) *K-Nearest Neighbour:* The K-NN algorithm [7] is a similarity-based learning method that is extremely effective in various problem domains, including classification problems. The k-NN algorithm, given a test element dt, determines its k nearest Neighbours from the training elements (dt's neighbourhood). The class for dt is determined by majority voting among the elements in the community.

$$d(x, y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$$

Fig. 3 Distance Calculation [5]

3) *Decision Tree:* Decision Trees [9] are supervised learning techniques that sort the tree from root to leaf nodes. The classification, which is represented by the label names, is provided by the leaf node. Because Decision Trees are not prone to outliers, less data processing is required. ID3 stands for Iterative Dichotomiser 3 and is so named because the method splits features into two or more groups iteratively (repeatedly) at each stage. ID3 builds a decision tree using a top-down greedy technique and is only applicable for classification issues using nominal features. It employs Information Gain to determine the optimal feature.
4) *Random Forest:* The Random Forest classifier [9] is a collection of decision trees chosen randomly from a subset of the training set. The votes from these trees are then uniformly aggregated to decide the final class of the item evaluated. The parameters that give this classifier's best accuracy score are 100 number of estimators, minimum sample leaves as 1, minimum sample split as two, and the Gini criteria is used to quantify the split quality.

D. Training and Testing the Models

To train a model, we first separate the data into two sets: training data and testing data. The classifier is then trained with a training data set and then assess its performance on an unknown 'test data set'.

E. Model Evaluation

It aids in determining which model is best suited to represent our data and how well that model will perform in the future. In data science, evaluating model performance using the data used for training is unacceptable because it produces over-optimistic and overfitted models. A confusion matrix is a method for evaluating a model based on four parameters: 'True Positives', 'False Positives', 'True Negatives', and 'False Negatives' [15], which is used to determine accuracy using the formula:

Accuracy = (True Positives +True Negatives) / (Total number of classes)

The ROC (receiver operating characteristic) curve is a graph that shows how well a classification model does over all categorization levels. Two parameters are depicted in this graph: Rate of True Positives and Rate of False Positives. It enables classification models to be compared. The ROC curve compares the false positive rate on the X-axis (the likelihood of target=1 when its true value is 0) to the true positive rate on the Y-axis (the probability of target=1 when its true value is 1).

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

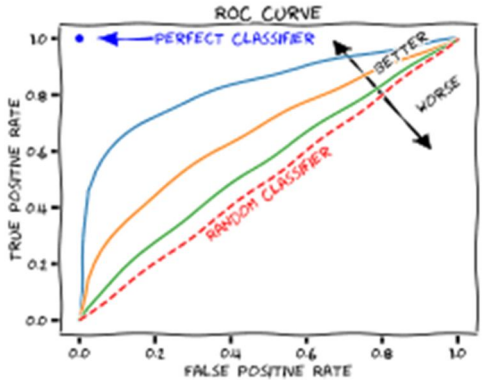


Fig. 4 The ROC curve for a "better" and "worse" classifier

IV. RESULTS

The accuracy score for each of the methods achieved on the test dataset is shown in Table I. Among the Machine Learning algorithms, the Logistic regression model has an accuracy score of 99.93% on the dataset which is the lowest accuracy score among all the algorithms given in section III. Besides, the accuracy score for k-NN classifier is 99.993% which is higher than that of LR.

The performance of Random Forest is slightly better or almost equal as it has better or same accuracy score than that of Decision Tree classifier on the test dataset. The accuracy score for RF is 99.997974% whereas that of ID3 is 99.997953% which is 0.000021% higher than MLP. Thus, the accuracy score obtained for Random Forest on the Test dataset is higher than any other algorithm presented in section III. The accuracy score for each of the algorithms is consistent with the F1-Score which is shown in Table II and the RoC Curve which is shown in Fig. 5.

Logistic Regression (LR) has an accuracy score of 99.93% which is shown in Table I. It is around 0.063% lower than k-Nearest Neighbor (k-NN) and approximately 0.07% lower than Decision Tree (ID3). Besides, the accuracy score of LR is the lowest among all the algorithms mentioned in Table I. In addition, Table II shows the F1-Score for each of the DDoS cyberthreats. The F1-Score for ICMP attack is 0.93 which means it can perfectly detect the cyberthreats on the system. For Benign Traffic, the F1-Score is 0.85 which shows that the algorithm can differentiate well between Normal and abnormal traffic. By the analysis of RoC Curve for Logistic Regression as shown in Figure 4 it is clear that for malignant traffic have a lower area under the curve which is consistent with the F1-Score obtained in Table II. The macro-average for LR is 0.92 which worse than k-NN and Decision Tree.

TABLE I

ACCURACY SCORE OF MACHINE LEARNING MODELS

Algorithm	Accuracy Score
Logistic Regression	99.93%
K-Nearest Neighbor	99.993%
Decision Tree	99.997953%
Random Forest	99.997974%

The accuracy score for K-Nearest Neighbor is 99.93% which is higher than LR by approximately 0.063%. In addition, the F1 Score for Decision Tree is much better for all the benign traffic. The F1-Score is 0.95 which is better than the F1-Score of LR (0.85). This algorithm can detect malignant traffic perfectly.

TABLE II

F1-SCORE OF MACHINE LEARNING MODELS

Class	LR	K-NN	DT	RF
Normal	0.85	0.95	0.99	1.00
Attack	0.93	0.98	1.00	1.00

In Figure 5, the RoC Curve for both traffic types for k-NN, from the figure it is evident that most of the attack type the area under the curve is 0.991 as seen in the top left corner and the macro-average is 0.99 which is slightly better than that of LR. Random forest is the best among all the four models.

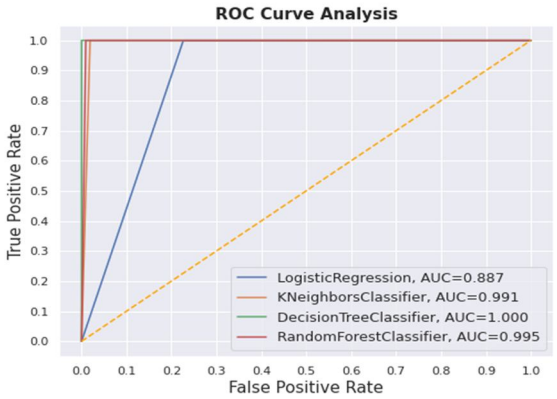


Fig. 5 False vs true positive rate

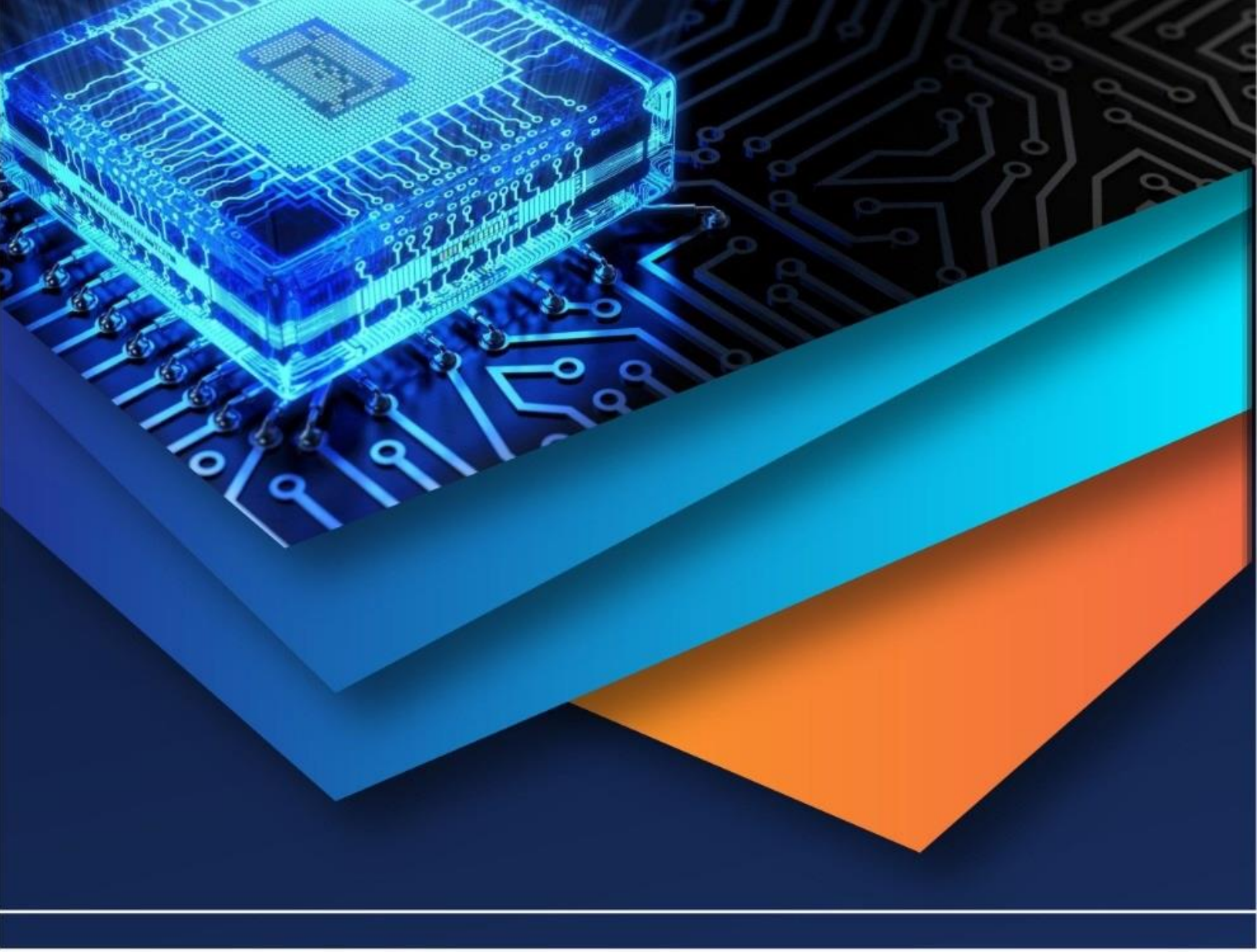
V. CONCLUSION

The detection for DDoS Cyberthreat was performed by using different ML algorithms and each of the threats was individually identified and validated by using different metrics. The results show that the performance of the Random Forest and Decision Tree classifiers is similar to that of an ideal classifier, as the area under the curve for both classifiers for the different types of traffic equals 1.00. Furthermore, both the micro and macro averages have a perfect score of 1.00, indicating that both classifiers perform like ideal classifiers on this dataset.

The detection of DDoS attacks and the accuracy evaluation of ML algorithms has been successfully accomplished, which is the fundamental purpose of our study. In the future, we hope to use ML algorithms to deploy multiple solutions for each of the attack types in order to defend the network from such attacks. Furthermore, several AI algorithms such as MLP and LSTM can be employed effectively to detect such cyberthreats. This work will be expanded to create a system capable of detecting DDoS Cyberthreats and deploying countermeasures to prevent critical Cybersecurity risks.

REFERENCES

[1] O. Rahman, M. A. G. Quraishi and C. Lung, "DDoS Attacks Detection and Mitigation in SDN Using Machine Learning," 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 2019, pp. 184-189.
[2] H. V. Nguyen and Y. Choi, “Proactive Detection of DDoS Attacks Utilizing k-NN Classifier in an Anti-DDos Framework”, International Journal of Computer and Information Engineering, Vol:4, No:3, 2010.
[3] S. Das, A. M. Mahfouz, D. Venugopal and S. Shiva, "DDoS Intrusion Detection Through Machine Learning Ensemble," 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C), Sofia, Bulgaria, 2019, pp. 471-477.
[4] R. Doshi, N. Apthorpe and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, 2018, pp. 29-35.
[5] S. Shanmuga Priya, M. Sivaram, D. Yuvaraj and A. Jayanthilaldevi, “Machine Learning based DDOS Detection”, International Conference on Emerging Smart Computing and Informatics (ESCI), IEEE, 12-14 March 2020, Pune, India.
[6] Jiangtao Pei, Yunli Chen, Wei Ji, “A DDoS Attack Detection Method Based on Machine Learning”, IOP Conf. Series: Journal of Physics: Conf. Series 1237 (2019) 032040, doi:10.1088/1742-6596/1237/3/032040.
[7] Manjula Suresh and R. Anitha, “Evaluating Machine Learning Algorithms for Detecting DDoS Attacks”, Communications in Computer and Information Science book series (CCIS, volume 196).
[8] Shreekhand Wankhede and Deepak Kshirsagar, “DoS Attack Detection using Machine Learning and Neural Network”, 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 16-18 Aug 2018, Pune, India, doi: 10.1109/ICCUBEA.2018.8697702.
[9] Harleen Kaur Taunque and Somesh Kumar Gupta,” A Study of AI and ML Algorithms for DDoS Cyberthreats Detection”, University of Waterloo, Waterloo, ON, CA, N2L.
[10] Q. Li, L. Meng, Y. Zhang, and J. Yan, Ddos attacks detection using machine learning algorithms," in Digital TV and Multimedia Communication (G. Zhai, J. Zhou, P. An, and X. Yang, eds.), (Singapore), pp. 205-216, Springer Singapore, 2019.
[11] E. Balkanli, J. Alves, and A. N. Zincir-Heywood, “Supervised learning to detect ddos attacks”, 2014 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), pp. 1-8, 2014.
[12] P. Khuphiran, P. Leelaprute, P. Uthayopas, K. Ichikawa and W. Watanakeesuntorn, "Performance Comparison of Machine Learning Models for DDoS Attacks Detection", 2018 22nd International Computer Science and Engineering Conference (ICSEC), Chiang Mai, Thailand, 2018, pp. 1-4.
[13] N. Pise and P. Kulkarni, "Algorithm selection for classification problems", 2016 SAI Comuting Conference (SAI), London, 2016, pp. 203-211.
[14] Ayush Pant (2019) towardsdatascience website. [Online]. Available: https://towardsdatascience.com/introduction-to-machine-learning-for-beginners-eed6024fdb08
[15] Rosario Silipo (2019) towardsdatascience website. [Online]. Available: https://towardsdatascience.com/confusion-matrix-and-class-statistics-68b79f4f510b



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY