Date available online: 13-02-2025
Vol. 2, Issue 2 (June - December 2024)
This is an open-access article.

DDoS Attack Detection System Using Machine Learning Techniques

Muhammad Zunnurain Hussain[1*], Muhammad Zulkifl Hasan[2], Khawaja Qasim Maqbool[1], Aisha Nazir[1], Hafiz Muhammad Furqan Farid[1]

[1]Bahria University Lahore Campus
[2]Universiti Putra Malaysia

[*]Corresponding author: Muhammad Zunnurain Hussain (e-mail: zunnurain.bulc@bahria.edu.pk)

***Abstract*—** Distributed Denial of Service (DDoS) attacks are the major issues that introduce disruption of accessibility and reliability of the network services. The purpose of this paper is to demonstrate an overall recognized machine learning based system that can efficiently identify and classify DDoS attacks using a rich dataset allowing us to work with various installation network traffic attributes, we have developed an automated classification pipeline the Random Forest Classifier which is known for its high performance in handling large datasets and heterogeneous data. These learnt models were then combined with Decision Tree, Gradient Boosting, and Logistic Regression models to provide a better way analyze the product. An important step involved in this framework is the data preprocessing pipeline that involves one-hot encoding of categorical features to numerical features and scaling for the numerical features, leading to model input optimization. Efficiency of our models is assessed through metrics just as accuracy, precision, recall, and F1-score and it is further validated using cross-validation techniques. The top models are being evaluated by powerful tools, which include feature importance visualization, confusion matrices, precision-recall curves, and calibration curves, for a deeper understanding of their predictive ability as well as their decision-making processes, within those models. A feedback loop mechanism for the iterative betterment and adaptation of the model is accounted which learns from new patterns actively. This approach demonstrates good evaluation and robust in identifying DDoS attacks that are threat of cybersecurity defenses using machine learning.

Index Terms—Decision Tree, Gradient Boosting Classifier, Logistic Regression, Feedback Loop system, Network traffic, DDoS Attack, Network Security, Cross Validation.

I. INTRODUCTION

In the cyber security field, the Distributed Denial (DDoS) of service attacks is the main obstacle that is preventing many of the system's productivity by jamming it with packets of traffic from different sources. Despite the evolution of the DDoS technique, it remains a top concern of cyberattack sector and every subtle shift can present significant outcome. Besides a cross-border level of investigation, the team of investigators additionally may encounter the leading problem as the practice of flooding the objective from several places becomes usual. Even though not any security system usually proves to be effective all the time when fighting this two-edged sword given its commonness and complexity, the ability to adapt to the newest technological developments can help the situation. Though traditional deterrence systems are not sufficient for the interception of such sorts of malicious attacks since they can generally provide only a shock and awe which leads to the inability of dynamicity and adaptivity while encountering enveloping threats. The ML algorithm working hands on with conjunctive rules implementation can be regarded as a machine minded learning from the data and trace the most foolish patterns that are always attacking the cyber universe.

ML is one of the most effective techniques of the past that had been very successful when it comes for instance, to the decision making since it does not require any kind of training and instructions and so decision making happens on its own only. In contrast to the learning algorithms which leave the system free to detect the variations to the standard while working in the network traffic pattern by using any means which go beyond the normal range. The system will be developed by combining two, different types of approaches namely - machine learning and deep learning. This provides a DDoS detection and classification function to detect multiple types of DDoS attacks. In future, such systems could be also applied to some network and then be assured of their completion as well as protection against attacks. The foundation of our super-multi-model machine learning pipeline is the team itself. This support allows all algorithms to arise, Random Forest Classifier, Decision Tree, Gradient Boosting, and Logistic Regression models. In addition, the models chosen should be for withstanding computer applications with different types of data, also the models should be able to adapt to real-time traffic conditions in networks.

This work first involves the development and consequent deployment of a DDoS attack defense system, based on machine learning, to be presented. The model will include different steps, which are data acquiring and preprocessing, models training, evaluation, and optimization. The theme of work is data preprocessing providing the data quality and data model fitting, and we offer the reasons of listed models and methods for model evaluation and selection.

Furthermore, the architecture is expected to continue to be effective with the implementation of the feedback mechanism, which is a feature that comes with the employment of systems that constantly change as they adapt to new threats keeping having a high detection accuracy over time. Such an ability to adjust is of particular importance for the system in which there is the endless process of digital transformations going on with considerable difficulty connected to effectiveness of the measures updated and their being relevant.

This paper not only suggests the development of system against the DDoS attacks, but also enhance the deployment of effective measurements based on the application of machine learning techniques which are required for the progress of the academic purposes. Our approach to the initial cleaning up, feature engineering and then the incorporation of machine learning algorithms will target optimizing a model capable of identifying normal and malicious traffic competently. Hence, such kind of measures will help in development of new approaches and organizations of more advanced attacks detecting and implementing of unified legitimate monitoring systems.

II. Related Works

The area of Distributed Denial of Service attack recognition has been spared by constantly active research communities trying to propose new ML and DL methods able to strengthen the cybersecurity utilities. Herein, there is the discussion of milestone achievements among the researchers, through various systematic techniques, data sets used and the goal of higher accuracy in detection.

[1] This Research aims to classify DDoS attack packets using the botnet dataset obtained from IoT using PCA as well as Decision Tree, Random Forest, and SVM algorithms. Species of PCA are applied to reduce dimension of dataset, that would not only increase computing power but also preserve the variability, the essential aspect of classification accuracy. It turned out that the Decision Tree and Random Forest methods have more suited for the case of handling unbalanced data then Support Vector Machine. Therefore, they have shown better performance in terms of accuracy and speed. [2] And this study used a DNN model, which was put into a SDN environment, to enhance the accuracy in detection of DDoS attacks. As for the protocol, an algorithm with a new and specially designed flow collector module is applied which, in turn, aids the extraction of features from the network flows. The DNN exploits these attributes and demonstrates its power to address difficulties faced by conventional machine learning models as it accurately recognizes complicated patterns and attacks in the network stream.[3] The approach using LSTM Recurrent Neural Networks is aimed at creating models of network traffic patterns for detecting abnormalities This model goes past pattern recognition and relies on self-learning for future threats. Such model is dynamic as it can recognize and adjust to new attack vectors that are not known today. The AUC of 0.84 means that the trained LSTM RNN can differentiate between normal and abnormal grid systems effectively, which implies that LSTM RNNs have the capability to learn and adapt continuously and are suitable for security systems. [4] The question as to what machine learning algorithms are the most efficient to detect DDoS attacks coming from consumer IoT devices is being focused on in this work. Through this combination of some of Algorithms like K-Nearest Neighbors, Support Vector Machine, Decision Trees, Random Forests, and Neural Networks, the study shows Neural Networks which are fast and precise give the best detection capability. It presents that the observance of special features by specific devices in the IoT might be essential in timely detection of DDoS attacks. [5] Using Random Forest and a Splunk software tool, this report focuses on the identification of "Ping of Death" DDoS attacks. Collaborating the machine learning with Splunk's capability in real time data monitoring, this study does a good job of achieving incredibly high detection accuracy which is 99.8%. By this way, the biggest advantages of hybrid usage of advanced analytical tools in combination with machine learning techniques is proved, which aims at improvement of detection and monitoring of network- based attacks. [6] Research-based learning about LSTM, SVM, and logistic regressions is used in the paper to detect DDoS attacks and models are assessed on their performance using conventional methods. LSTM model has put up a quite strong show of it. The said model not only has good accuracy but also low false positive rate. This proves the excellence of LSTM in the sequence problems prediction, which makes it very convenient for application in dynamic and constantly evolving areas of cybersecurity. A low-weight detector technique is proposed using the Random Forest algorithm and decision tree algorithms-boundary split as well as decision stumps that classify the systems as severe likely. Testing on CICIDS2017 data illustrates that the PDT, especially, allows models to attain both very high accuracy and computational efficiency, which makes the PDT a nice model when the available computational resources, especially, are limited. [8] The testing makes usage of Artificial Neural Networks (ANNs) to enhance the classifier using Mutual Information, which assists in better selection of features; because of this, detection of DDoS attacks is made more efficient and accurate. The ANN's model capability, where the ER of 89.62 percent is achieved, well prove how much feature selection could improve the neural network performance in cybersecurity applications, particularly in differentiating between the ordinary and malicious activities. [9] Deploy CNNs on this research and as a result you will receive 99% accuracy of DDoS traffic identification and files classification. Model

CNN, that can process the data both spatially and temporally, is a perfect tool for dealing with complicate network communication issues in Mobile Cloud Computing (MCC) environments. This result confirms that the model acts the best rather than other typical classifiers and this might be a positive sign for the advanced network security setups. [10] This model was implemented with different types of machine learning algorithms, and it has been demonstrated to produce an intrusion detection system that is effective, using the CICIDS-2017 dataset. The study shows that hereby the Random Forest algorithm exhibits superiority with regards to detecting DDoS attacks, by being capable to process large datasets and since it is well-functioning in handling the balance between bias and variance so that it has a high accuracy and high recall rate. [11] We implement a unique multi-classifier algorithm that unites a complex pyramid of deep neural networks involving CNN, LSTM, and GRU to get hold of numerous types of DDoS attacks including singular and mixed type ones. This ensemble approach leverages the strengths of each model type: For example, applying CNNs to spatial information, LSTM to sequence of temporal recurrence, and GRU with fewer parameters compared to LSTM, for modeling of sequences. Employing an ensemble model merges different models of traffic patterns improvement in detection rates and lessening false positives as it captures more intricate designs and abnormalities in network traffic. [12] This research is about applying a CNN modified particularly for use in IoT environments that are meant to prolong the process of detecting and stopping DDoS attacks. In the deep neural network, the traffic data of the network is processed to point out the malicious activities by learning the complicated structure that can be easily seen from the traditional machine learning methods. The deep model provides the network with the ability to detect tiny irregularities from big amount of data that clearly is more precise in the case of IoT networks, where the behavior of devices may be very different from each other. [13] The model designed to solve the problem of unbalanced network data is presented and can lead to poor machine learning performance. It is guided by a plethora of algorithms, including Random Forest and Convolutional Neural Networks (CNN), to achieve data balance and then training. Iterative and repeated partitioning of data can be helpful in spotting the attack types, mostly missed in skewed labeled sources. The research let us know, that application of model training on balanced dataset has been proved effective and investigate the possible roles of CNNs in extracting the complex pattern to discriminate between normal and anomalous data. [14] One of the approaches is by using multiple linear regression to analyze data attributes characterizing network traffic and setting up typical traffic behavior model of data prediction and comparing it with the observed data, and then, identifying abnormal patterns. The regression analysis is particularly good for doing the job since it can be very fast in the calculation and interpretation of the results, which is a great advantage for environments where the fastest reaction is necessary. Application of PCA-based feature selection allows models to perform more efficiently by removing a number of variables from model without losing necessary information. [15] The authors provide a two-phase detection approach based on the use of linear regression to distinguish routine inbound traffic peaks against a DDoS attack. In the first phase, namely the training phase, the model is developed where historical data is used for understanding the typical traffic patterns typified as the compliance with traffic laws. The prediction phase in this model is designed to match actual traffic behavior and prompt the identification of statistical deviations that exceed the standard limit as possible DDoS attempts. Thus, this model greatly reduces false positives and improves the reliability of such networks in the real world [16] Anomaly is carrying on the research on extracting a particular set of network traffic features that are more useful than others for web-based attacks detection algorithms such as Support Vector Machines (SVC), Random Forest (RF), and Logistic Regression (LR). Innovative design which is capable to highlight the patterns that demonstrate a malicious behavior of web traffic creates a possibility of implementing real-time detection with a higher accuracy, and thus, overcoming the typical limitations of datasets in common use. This study will review the classifiers effectiveness in the detection of DDoS attacks and will pay special attention to feature engineering to improve model efficiency. Targeting only the most representative characteristics of attack traffic allows the models, and especially Random Forest, to efficiently attain a high rate of success. Such an approach centers around the fact that the quality of detection systems is enhanced by the detailed options of features. MC- CNN model, namely DAD-MCNN, employs multiple channels for processing network data, catches DDoS attacks more precisely. Such an approach facilitates the processing of different types of network data in parallel, thus providing the model with improve in accuracy and speed of attack detection. Incremental training is involved to constantly re-train the model with new data, thus allowing it to become more familiar to new attack vectors. [19] It merges signature-based and anomaly-based techniques with LSTM deep learning models to build a customized IDS for IoT ecosystems. This hybrid approach enables the system to detect known attacks using signatures as well as to identify the novel or unknown attacks by means of the behavioral anomalies that LSTM type models detect. [20] It describes the TaxoDaCML framework which uses both Decision Tree and Random Forest models to create a taxonomy-based system of DDoS attacks classification. Such an organized approach enables quick and accurate detection of all known DDoS attack types, improving the system’s responsiveness towards attacks based on their specific shapes, patterns, and mechanisms. [21] Designs a bio-inspired model which employs the bat algorithm to effectively detect the Application Layer DDoS attacks within the shortest possible time. The originality of this method is similar to the echolocation behavior of bats to detect changes in network traffic, which allows quick DDoS attacks mitigations. The real-time detection effect of the model makes it as a promising alternative for the common detection methods This research work also includes developing a DDoS detection system for OpenStack-based private clouds to evaluate the suitability of traditional algorithms such as Decision Trees and more advanced methods such as Deep Neural Networks. The research shows that DNN is superior and adaptable in dealing with different variations of attacks outgoing in the dynamic cloud in terms of detection capabilities. [23] Exposes the AIMM framework, which amalgamates neural networks to a large garden KNN as an effective mechanism of identifying DDoS attacks at their early stages. This method blends the evidencing feature of AI with the convenience of k-NN to produce a powerful detection system. Its high effectiveness in strange situations testifies to the framework's ability to identify even the most intricate of attacks accurately. [24] Suggests the E-HAD architecture, a (creative and distributed) scheme, which is based on Hadoop, correctly manages big volumes of data with the target of early detection of high-speed DDoS attacks. The application of the Shannon metric in network traffic monitoring not only steers the system to have more precision but, in the process, increases the accuracy level fitting the system for use in big networks. [25] Efforts to reveal a shield mechanism against DDoS attacks in SDN and deep learning using fog computing, especially in LSTM modeling are underway now. What is more, the strategy creates obstacle for sending and establishing legitimate traffic that is later on forwarded in the optimal way while blocking anything malicious, thus, providing a good security solution for fog networks. [26] In this work, two models combining LSTM with Random Forest (RF) as well as entropy measure and attribute threshold are applied to not only locate the possible Malicious Attack Behavior, but also to detect DDoS which further improves the detection accuracy. The application of this methodology is built on a foundation of long short-term memory (LSTM) network to process time series information and an ensemble of Random Forest for the robust decision-making. Having employed such a hybrid method, detection accuracy of wrong positives, if any, has been noticeably decreased which is demonstrative of a successful direction towards the development of fully functional network security solutions. This research presents an SDN environment framework that connects multiple kind classifiers KNN, Decision Trees, SVS, Logistic Regression, and XGBoost. Within this architecture, classifiers are integrated to create the final hybrid predicting model. This approach is all about handling the creation of an experimental SDN to let these algorithms conduct processing of traffic data from the network. It is this setting that both features are enabled as well, the real- time attack detection is precisely made, and malicious and legitimate traffic are distinguished effectively. The use of XGBoost what is actual for high performance, to be specific, to obtain first-class precision and recall rates, is an example of its benefit. [28] Random Forest and XGBoost classifiers are initially evaluated in the context of this research, followed by the introduction of a new XGBoost classifier modification targeting improving detection performance in DDoS instances. Through using CICDoS2019 dataset, study purposely test and compare the performance of these models in a well-controlled laboratory environment, which brought about a huge increase in effectiveness such as precision, accuracy, and recall. The modified XGBoost classifier signifies a more customized approach having consideration for the peculiarities of DDoS attack traffic and offers a more exact and fitful detection mechanism. [29] The paper analyzes the capacity of LSTM, SVM, and Logistic Regression models, focusing on their ability to process and foretell malicious activities. The core strength of the LSTM architecture is its capability to accurately recall patterns across time even where the attack signatures can change. The SVM (Support Vector Machine) and Logistic Regression, possess excellent classification capabilities, and are therefore suitable for instances where instant decisions are necessary. The study not only contrast these models, but also investigates their association and how that might affect the overall reliability of detection.[30] Powered by a trimodal combination of Random Forest, Gaussian Naive Bayes, XGBoost, and K-Nearest Neighbors, the study overshoots toward the network traffic classification and helps protect against DDoS attacks. Using the NF-UQ-NIDS-v2 dataset, that covers broadly multiple network traffic scenarios, researching strength of the feature of the algorithms at handling different zones of the data is the point of highlight. Among all models, Random Forest got the highest accuracy, which explicitly verifies its ability to manage large data processing and find key features that are crucial for detecting DDoS activities. [31] This study will mainly put the supervised learning technique into practice with three of them namely Random Forest, Logistic Regression, and K Neighbors Classifier on NSL-KDD dataset with purpose to detect DDoS attacks. Through preprocessing the data and exploiting these classifiers, the analysis demonstrates its outcomes through different performance metrics like accuracy, precision, recall, and F1-score. The analysis clarifies the advantages and disadvantages of each model together with the comparative view that informs better decision-making regarding the use of the most effective strategies in practical applications to the network security infrastructures. The cyber security field is majorly benefited by this study by uplifting the supervised learning techniques as well as their practical application in DDoS threat detection.

Prior work is taken as a foundation to the current research, with machine learning-based DDoS detection examined in several works, including integrating multiple classification techniques and feature importance analysis. For example, some of the easiest models that have been applied previously are Support Vector Machines (SVM) and Decision Tree, the issue with such models is the scalability and their ability to handle new dynamic attacks. As such, this study adds to the literature by applying ensemble learning techniques including Random Forest and Gradient Boosting to enhancing the received detection accuracy. Nevertheless, it is suggested that the proposed approach may need more thorough testing in managing more diverse and complex cyber threat phenomenons than those emerging from recent deep learning frameworks. For that, the deeper comparative discussion is provided here in order to emphasize what particular strengths and weaknesses are implied by this approach in contrast to the current procedures.

Contribution

This work also proposes an adaptive machine learning over a variety of algorithms' based DDoS detection framework with feedback mechanism. As opposed to previous studies that are concerned with concerted categorical models only, our model pays much attention to performance assessment on an ongoing basis and dynamic optimization in real life. Further, involving an extensive variable selection procedure to improve the model interpretability and the computational cost is minimized. The current work enriches the proposed methodology for cybersecurity studies in terms of reproducibility and scalability with account for practical implementation.

Methodology

This paper deals with detecting DDoS attacks using machine learning methods. The initial part of our system comprises the data collection, cleaning and analysis, feature extraction, model selection and evaluation, followed by a structured algorithm to implement our detection models.

A. DATASET

This paper utilizes dataset from Kaggle. The dataset utilized in this work is a large repository of more than 100,000 network traffic records tailored to empower the detection and classification of the Distributed Denial of Service (DDoS) assaults, which are designed for user operating system. Each line of the dataset refers a unique network flow and includes 23 attributes with an extensive number of components warranting monitoring of the network traffic during routine activity and exceptional conditions. Main attributes involve **dt** (simply the time when the traffic was monitored); **src** and **dst** (popular for indicating IP addresses); **pkt-count** and **bytecount,** detailing the packets and bytes respectively; **dur** (duration in seconds); and **tot-dur** (a cumulative count when several time related attributes are considered). Further, the dataset contains columns specifying the communication protocol used (e.g., TCP, UDP) and flows recording the count of flows observed during the capture interval and **tx_bytes** and **rx_bytes**, indicating the bytes transmitted and received as respective fields of the dataset.

B. DATA PREPROCESSING

At the pre-processing stage in our project, we aimed to improve data quality in the format as well as offering high efficiency and accuracy in detection of DDoS attack. First, we began by imputing the missing values as numerical values for the columns **'rx kbps'** and **'tot kbps'** to replace the blank ones. The imputer that worked for this problem well with that strategy was **SimpleImputer** and it being used to handle the null case with median which preserved the distribution tendency of the dataset. So, median value allowed to mitigate the issue highly relevant for the network dataset due to high frequency of certain outliers. Moreover, the features used in the data represented as string variables such **as 'Src', 'Dst'** and **'Protocol'** were converted into one hot vector using **OneHotEncoder** for the machine learning algorithms to work them as binary values. For improving the data quality, we apply **RobustScaler**, which is useful to handle those columns that are with the numerical data type since it helps to avoid the using of extremes. Similarly to this, the other empty values are simply taken as the median to make the information more reliable. Therefore, we used an 80-20 ratio for training and for validation of the model to ensure that even during the training stage we stay unbiased while during test we provide the model with the opportunity to stay unbiased too. As a result, the signature, which is used as an advantageous processing, implies that no data that can provide input is left, and the dataset completely catches all the discrimination.

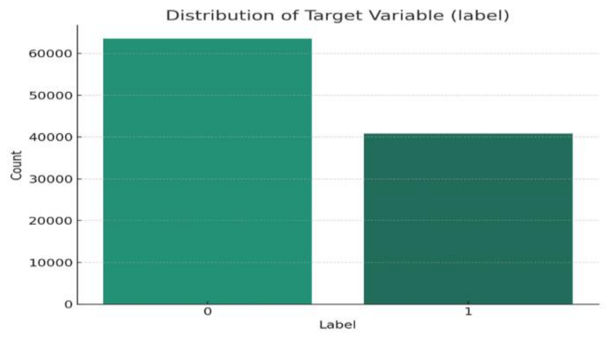

FIGURE 1. The chart showing the target variable distribution indicates that the dataset is somewhat unbalanced between these two types (0 stands for the normal traffic, and 1 for the DDoS attack). The resulting stimulation implies one of the possible learning methods that might lead to detection of both normal and malicious traffic.

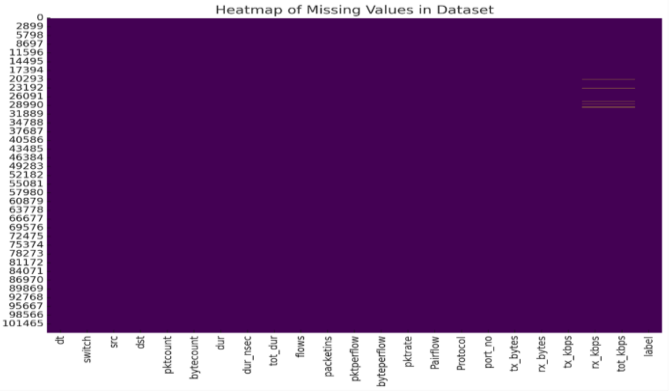

FIGURE 2. The Missing Value Heatmap indicates a minimum level of missing values represented by yellow patterns across features. Consequently, the process of median imputation is applied to ensure a pertinent and thorough dataset for subsequent data analysis.

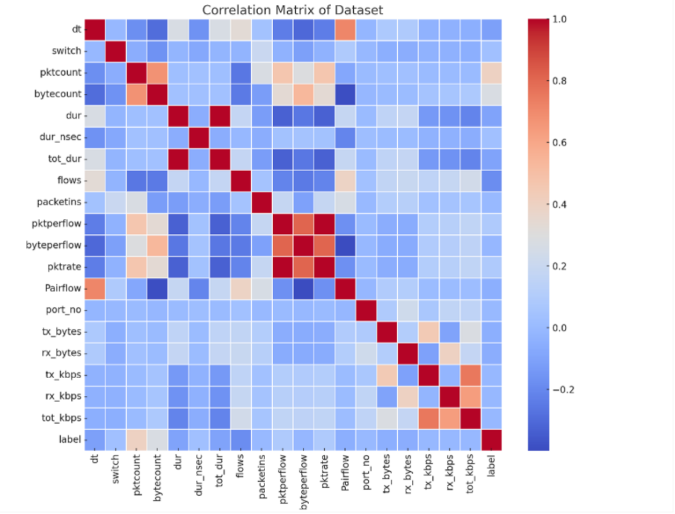

FIGURE 3. The correlation heatmap from blue to red shows the correlation range beginning from low to high. The matrix reveals a potential multicollinearity between features like 'bytecount' and 'pktcount', which further correlate with a label that indicates a DDoS attack.

C. FEATURE ANALYSIS

An integral part of our methodology involved analyzing the dataset to identify and select features critical for distinguishing between normal traffic and malicious DDoS attacks. This process was crucial in refining our models, inputs for optimal performance.

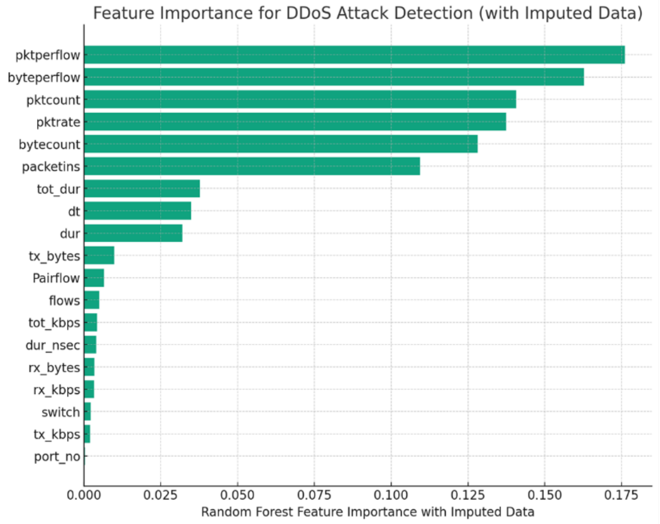

FIGURE 4. The bar chart shows the top feature importances, as identified by the Random Forest Classifier of DDoS Attack Detection after data imputation of missing data. The length of each bar shows how the features 'pktperflow', 'byteperflow' and 'pktcount' matter in the predictive model which plays a big role.

D. MODEL SELECTION

In this paper, we used a few machine learning techniques and those were selected from others for being the most appropriate for classifying the data.

Performance: Accuracy of the model in appropriately categorizing network traffic.

Complexity: Models which can find some compromise between the predictive power and the computational efficiency.

Interpretability: The clarity that the model decisions can be explained.

Robustness: Models of general type that deal with problems such as imbalance which is another network traffic characteristic.

E. PROPOSED MODEL

We have chosen four specified algorithms which are Decision Tree, Logistic Regression, Random Forest Classifier, and Gradient Boosting Classifier, because they are all effective classification algorithms. For evaluating, we utilize the Accuracy, Precision, Recall, F1 Score and AUC Metrics to comprehensively measure individual model levels of performance.

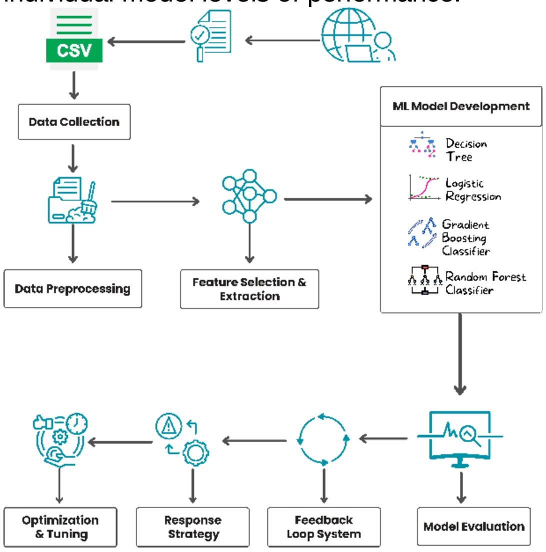

FIGURE 5. System Flowchart

We utilized machine learning algorithms renowned for their classification effectiveness. The Decision Tree offers a clear visualization of decision-making paths and is utilized for its ease of interpretation and capability to handle non-linear data. The Logistic Regression model was chosen for its simplicity and interpretability, providing a benchmark for the project. The Random Forest Classifier was selected for its robustness in handling complex tasks and its feature importance capability. Lastly, the Gradient Boosting Classifier was incorporated due to its sequential error minimization, making it highly adaptive and efficient for varied data types. The Decision Tree these times its visualization force comes from decision levels and paths which in turn ensure that it is used in its ability to deal with the data which is non-linear. The Logistic Regression model is very easy to interpret. We found the Random Forest Classifier function to be more determinant and effective compared to other algorithms that we considered for large or complicated tasks and the feature importance functionality that it presents. Secondly, Gradient Boosting Classifier is the most significant instrument of the designed model which is sequential error minimizing and efficient for diverse data types.

F. MODEL TRAINING

Four machine learning algorithms are engaged in solving the problem of detecting DDoS attack, each algorithm due to its characteristics being the best match for a classification task.

Logistic Regression: For this case, we will start the Logistic Regression modeling with max_iter = 1000 in order to make enough iterations for the model convergence. This model is essentially a starting point which a relatively plain but a powerful way to distinguish between traffic types representing normal or malicious. Random Forest Classifier: The Random Forest model which is a well-known accurate algorithm on handling even the most complex datasets, are configured and 100 trees resources are assigned. The algorithm gains this feature with the help of performing a feature importance testing, using which we find out the primary attributes that are indicative of DDoS attacks.

To prevent from over-fitting the Decision Tree model, it is limited to a depth of 10. The model goes through a preprocessing phase where numerical features are median-imputed and scaled, while categorical features are imputed with the most frequent values and one-hot encoded. Built-in into the pipeline with the preprocessor. Gradient Boosting Classifier: Considering the Gradient Boosting classifier as one that is adaptable and using a sequential error correction technique it is possible to benefit from this. This model that is very good at bot fixing previous trees faults is a more advanced approach to model training.

G. *MODEL EVALUATION*

We split our dataset into train and test as later we will be using cross validation to validate our results. Accordingly, we will make certain that our model is not overfitting to the training data and that our outputs are generalized. Evaluation of the model using the metrics such as accuracy, precision, recall as well as F1 score and advanced evaluations measures like ROC curves and precision-recall curves. Also, we use confusion matrix to represent the performance of our classifier in the traffic detection process as well.

III. Results

We got the important points from the evaluation of the machine learning models training for DDoS attack detection, showing that our method is working and is a reliable tool.

A. *MODEL PERFORMANCE*

The model's performances were evaluated using a suite of metrics: they are, accuracy, precision, recall, and F1 score. The Random Forest algorithm achieved an accuracy of 99.97%, which confirms it as the most reliable model for DDoS detection in our experiments. The Decision Tree and Gradient Boosting models exhibited the scores as 99.65% and 99.63 %, both of which were highly impressive. However, Logistic Regression timed in with an accuracy of 84.53%, lower than other models and far from being an ideal option for such a complex task.

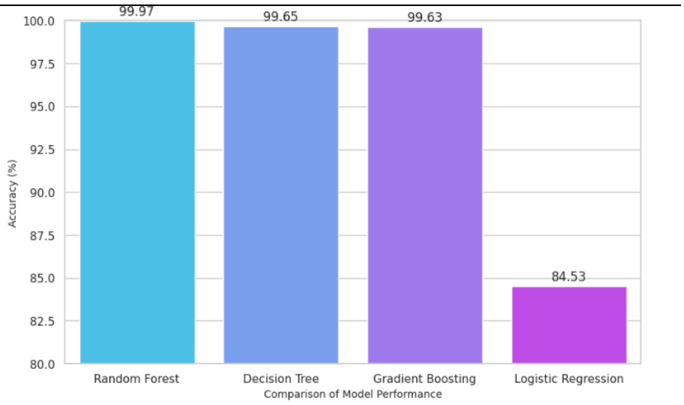

FIGURE 6. Model's Performance

Table 1. Model Performance Metrics

Model	Accuracy	Precision	Recall	F1-Score
Gradient Boosting	99.64%	100%	100%	100%
Decision Tree	99.65%	100%	100%	100%
Logistic Regression	84.53%	0.85%	0.90%	0.88%
Random Forest	**99.98%**	**100%**	**100%**	**100%**

A. *COMPARISON*

When comparing the machine learning models for DDoS attack identification, the random forest classifier beats most of the other models by showing its power through 99.97% accuracy by employing ensemble methods which can especially handle complex data. Those two classifier models show high accuracy as well 99.65% by decision tree and 99.63% by Gradient Boosting according to the result. This reflects on their efficiency in the classification task. Linear Logistic Regression models, which demonstrated an accuracy of 84.53%, come just behind thus hinting that linear models might be having problems coping with the complexity of the technical security data. This analysis asserts that those ensemble techniques outperform others in terms of cyber threat identification amongst network traffic.

B. *INSIGHTS*

The Feature Importance analysis by the Random Forest model helps to understand what the most important predictors of DDoS attacks would be as well as to suggest the effective measures for the networks. High precision and recall scores remain across models, thus, confirming good ability to properly identify the real DDoS attacks, avoid false positives, which is very important, because of the avoiding of unnecessary defensive actions that could disrupt service.

C. *ROC CURVE AND AUC SCORE*

A ROC curve and AUC demonstrate the general potential of the model to classify things using threshold value. The Random Forest model has a high true positive rate, and finally it was able to obtain an AUC close to 1 meanwhile the false positive rate was low, which represents the highest model performance.

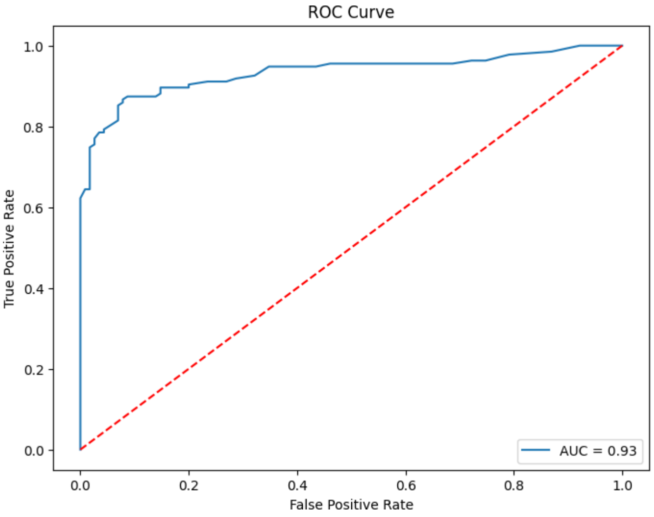

FIGURE 7. The red dashed once is that of a random accurate estimation, which contrasts with the ROC curve of the model near these diagonal lines in a distance because is far from them. The AUC of 0.932 shows a similar picture which is some kind of measure of how accurate the model is; the closer the AUC outcome is to 1, the better the model is in correctly predicting as true positives and is capped at false positives. AUC 0.93 indicate that the model matches with the given data well.

D. FEATURE IMPORTANCE

The important roles of the attributes such as packet count, byte count and particular protocol activities confirmed by the analysis from the Random Forest model have a direct bearing on the enhancements of future features of engineering as well as their selection to achieve improved model accuracy. The outcome of this analysis on the most important variables in the DDoS attack detection. 'Feature 12', 'Feature 2', and 'Feature 5' emerged as major, allowing the modified algorithm of features engineering and construction to reach better performance of the model.

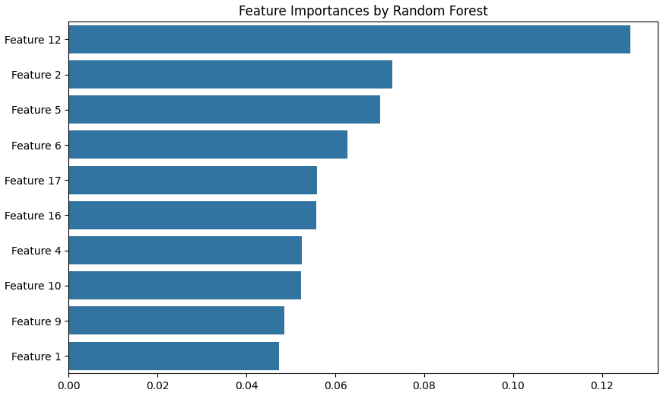

FIGURE 8. Feature Importance by Random Forest, Feature importance ranking based on Random Forest classification, illustrating key network attributes influencing DDoS detection. Higher-ranked features contribute more significantly to attack classification.

E. CONFUSION MATRIX

Visual inspection by using confusion matrix for our models, especially the Random Forest, could indicate the extremely rare misclassification result and such process will reinforce the capability of model usage in real cases. The deep and detailed values of these metrics highly demonstrate accomplishments of our model, which seems to be wired for the accurate identification of DDoS attacks, that is why sources for future profound research and application in network security solutions are built.

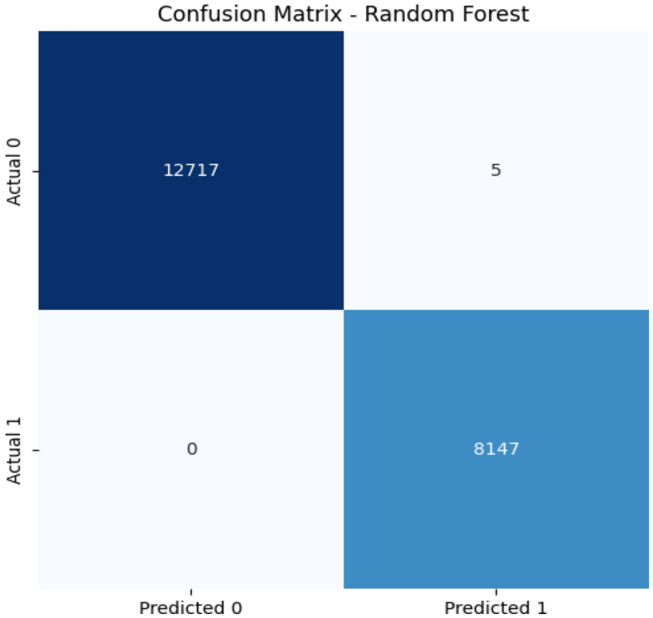

FIGURE 9. The matrix represents a confusion matrix for a Random Forest classifier, which shows the final outcome of class predictions on classifying problems. The number of correct predictions made by the model is represented by the large numbers on the diagonal of the matrix: 8,147 true positive cases (Actual 1, Predicted 1) and 12,717 true negative cases (Actual 0, Predicted 0). The off-diagonal numbers represent the few errors made by the model: 5 actual 0 and 1 predicted, 0 actual 1 and 0 predicted. This means that the model is capable of precisely predicting both cases, and that it is even more reliable in correctly predicting all positive cases with no cases of false negatives being present. Confusion matrix for Gradient Boosting, providing a detailed breakdown of true positive, false positive, true negative, and false negative classifications.

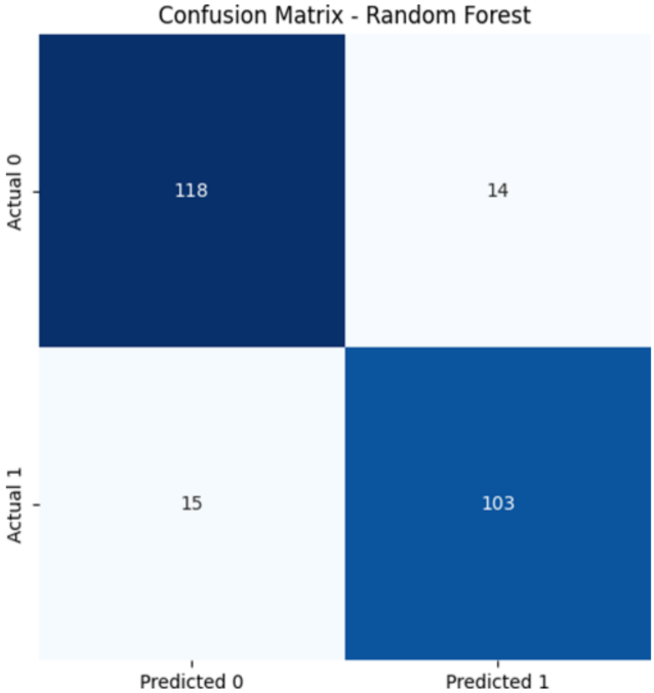

FIGURE 10. This confusion matrix serves as a visual depiction of Random Forest classifier capabilities in the investigation. It shows four key metrics: We have the total of 118 true negatives and 103 true positives. The number of these actual outcomes makes me feel that the prediction is right for both negative and positive classes. An odd reality together with 14 false positives and 15 false negatives evidence when network does not classify the correct target.

IV. Feedback Loop System

The feedback loop system in our study serves as a core that tunes the detection and prediction models for DDoS attacks in real time. These models adjust the accuracy description against real outcomes to obtain an improved model behavior. When differences occur, the model, which is automatically modified to reach higher results in any future predictions; thus, rather than being one-dimensional toward a certain attack type, it is now able to adapt to new and emerging patterns of cyber threats. Whenever disruptions occur, the model is going to be adjusted automatically to the future model for the purpose of improvement, which implies that the model will progress with new attack patterns. Therefore, this ability to improve our model is the vital trait possessed by our defense mechanism in the practical environment to overcome DDoS attacks. It provides the room for the development of the system that can maintain the transformation in the dynamic space of network threats. The Feedback loop in the model is not only bringing into account the amplified precision of the model over the time but also, this learning loop is making the model secure through integrating the hands-on experience in the model's operational system.

Technically, it's the ability to respond to the feedback actively and automatically meaning that it's much easier for such a system to be efficient where the speed and the accuracy are the most vital. This approach provision that our predictive models remain at the bleeding edge of technology so that we are capable of countering the existing and the new threats.

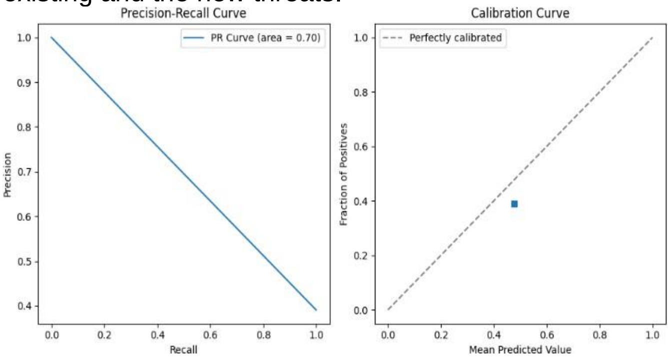

FIGURE 11. Feedback Loop Evaluation: The left panel shows the Precision-Recall Curve and the model balance by assigning the PR AUC of 0.70 that is indicating moderate precision-recall balance. The right side shows the Calibration Curve, a method to check the model prediction reliability; closeness to the dashed line shows that the loop adjustment improved the model's prediction calibration.

V. Response Strategy

Our project employs a differentiated response strategy based on the classification of network traffic into three categories: whitelist, graylist, and blacklist. This approach that we have quite actively followed toward our cybersecurity measures is particularly essential in mitigating the DDoS attack ineffectiveness very effectively.

1) WHITELIST

The traffic on the whitelist is positive and passes through the network without any obstacles. Therefore, internet traffic is trusted and allowed freely. It has on this list already trusted domains which have been confirmed and from which there is no personal data threat. The modeling process is arranged so that security procedures wouldn't disrupt the normal processes of business, always providing access to trusted entities and places.

2) GRAY LIST

The traffic that is listed gray is recognized as suspicious but meanwhile, does not provide conclusive evidence of malicious code. This go-through is basically for more rigorous evaluation and surveillance with advanced processes like throttling or more flexible check. Another intermediary takes a broader view of the situation, thus, helps to exclude possible false positives but not to do that, at the same time, with accurate informers.

3) BLACKLIST

Blacklist is the list of those sources which are judged as malicious, and their traffic is blocked right away. This final action is a key factor for avoiding threats and a most important defense against known and active attack vectors.

VI. System Responsiveness

It was evaluated how fast the system is analyzing and labeling traffic in real-time. It takes 0.5 seconds on average. This processing time is key and proves the applicability of the models to real-time security applications ready for action within a relatively short period.

VII. Conclusion

This project has clearly shown the justification and feasibility of implementing machine learning techniques which detect and classify DDoS attacks. This study was based on a sophisticated multi-model machine learning pipeline which was developed by integration between four models, i.e., a Random Forest, another Decision Tree, Gradient boosting Machine and a Logistic Regression, on an immense dataset of about 100,000 network traffic entries. This study was proven to have the capability to distinguish most of the normal and malicious network traffic high reliability. The Random Forest Classifier turned out to be the best model because of its capability of finding an accurate solution in a complex dataset and its capability of delving into feature importance metrics.

We arrived at the conclusion that machine learning solution is developing unlike the old, static system based on rules and keeps learning as new rules emerge in the cybersecurity world. For feedback to be more effective, the system must improve over time on newly provided data, which automatically leads to more accuracy and reliability of service providers. The ability to continuously learn and adapt already exists in cybersecurity which, among many other things, proves to be vital since the attack vector is constantly changing and developing. Categorizing the different traffic streams into three fine categories: whitelist, gray list, and the blacklist, will give the system its unique response intended to ensure the least number of false positives.

However, the research had its own difficulties as well. There are many challenges, one of them is computational load of analyzing immense network data in real-time which could make the deployment of such systems in environments with limited resources very difficult. Similarly, although the models were great in detecting known patterns of DDoS attacks their performance decreased when it came to the complex attacks simulating the legitimate traffic, indicating a requirement for improvement in feature extraction the integration of anomaly detection which doesn't rely on system signature-based detection.

VIII. Limitation

It is required to note certain weaknesses of the proposed models: Firstly, higher accurate detection of DDoS attacks is achieved including its certain limitations. First, the datasets selected may contain limited diversification of actual network traffic, and thus the generalization of results could be a problem. It is acknowledged that the results may have been influenced by biases arising from data collection mechanisms, for instance, considering preferred types of attacks would lead to model overfitting. Further, the nature of the created models may include certain levels of computational burdens which may limit its applicability for for real-time high throughput networks. Further research shall be conducted in a sequel of this work to evaluate the efficiency of the models under attack scenarios in addition to identifying ways of increasing the preciseness of the models.

IX. Future Work

Moving ahead, improvement of the DDoS detection system contains several emerging research and development fields. High-level feature engineering is a vital component of the process, because more detailed variables that provide better representation of the global image of the network traffic and precise attack techniques are necessary for the models to perform the right task and identify the legitimacy of network traffic stream and malicious attacks. Deep learning systems might be able to develop the ability to replace the human feature-engineering process by automatically detecting even the most variety patterns and the interactions within the data. Additionally, runtime modification of models for the purpose of analyzing real-time data is considered a vital aspect of practical implementation, emphasizing the necessity to lower the number of computations to enhance data processing speed. Moreover, combining this machine learning system with existing security structures may provide a more integrated defense and utilizes the best inherent characteristics of both the old and the new security procedures for network defense. In all, this project secures defenses against DDoS because of the advanced machine learning techniques applied to the real cyber security challenges and, we can proudly claim that it has academic contribution as well. The system shall continue building on this foundation and if the process continues, we can be looking at an increased number of security measures that will address the current concerns as well as those that will emerge as time passes.

REFERENCES

[1] D. Nanthiya, P. Keerthika, S. B. Gopal, S. B. Kayalvizhi, T. Raja, and R. S. Priya, "SVM Based DDoS Attack Detection in IoT Using Iot-23 Botnet Dataset," in 3rd IEEE International Virtual Conference on Innovations in Power and Advanced Computing Technologies, i-PACT 2021, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/i-PACT52855.2021.9696569.

[2] W. Zhao, H. Sun, and D. Zhang, "Research on DDoS Attack Detection Method Based on Deep Neural Network Model in SDN," in Proceedings - 2022 International Conference on Networking and Network Applications, NaNA 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 184–188. doi: 10.1109/NaNA56854.2022.00038.

[3] B. J. Radford, L. M. Apolonio, A. J. Trias, and J. A. Simpson, "Network Traffic Anomaly Detection Using Recurrent Neural Networks," Mar. 2018, [Online]. Available: http://arxiv.org/abs/1803.10769

[4] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer internet of things devices," in Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018, Institute of Electrical and Electronics Engineers Inc., Aug. 2018, pp. 29–35. doi: 10.1109/SPW.2018.00013.

[5] C. Murukesh, B. Kishore Kannan, A. Thilak kumar, B. Venkat, and V. Haris kumar, "Detection of Distributed Denial of Service Attack using Random Forest Algorithm," in International Conference on Automation, Computing and Renewable Systems, ICACRS 2022 - Proceedings, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 382–386. doi: 10.1109/ICACRS55517.2022.10029249.

[6] M. V. Uma, M. Vishnukumar, P. Meganathan, and C. M. Shyamsunder, "Detection and Mitigation of DDoS Attacks in Network Traffic Using Machine Learning Techniques," in 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation, ICAECA 2023, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICAECA56562.2023.10200383.

[7] M. I. Kareem and M. N. Jasim, "DDOS Attack Detection Using Lightweight Partial Decision Tree algorithm," in Proceedings of the 2nd 2022 International Conference on Computer Science and Software Engineering, CSASE 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 362–367. doi: 10.1109/CSASE51777.2022.9759824.

[8] J. Dalvi, V. Sharma, R. Shetty, and S. Kulkarni, "DDoS Attack Detection using Artificial Neural Network," in ICIERA 2021 - 1st International Conference on Industrial Electronics Research and Applications, Proceedings, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/ICIERA53202.2021.9726747.

[9] A. R. Shaaban, E. Abd-Elwanis, and M. Hussein, "DDoS attack detection and classification via Convolutional Neural Network (CNN)," in Proceedings - 2019 IEEE 9th International Conference on Intelligent Computing and Information Systems, ICICIS 2019, Institute of Electrical and Electronics Engineers Inc., Dec. 2019, pp. 233–238. doi: 10.1109/ICICIS46948.2019.9014826.

[10] S. S. Panwar, Y. P. Raiwani, and L. S. Panwar, "An Intrusion Detection Model for CICIDS-2017 Dataset Using Machine Learning Algorithms," in 2022 International Conference on Advances in Computing, Communication and Materials, ICACCM 2022, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ICACCM56405.2022.10009400.

[11] M. I. Sayed, I. M. Sayem, S. Saha, and A. Haque, "A Multi-Classifier for DDoS Attacks Using Stacking Ensemble Deep Neural Network," in 2022 International Wireless Communications and Mobile Computing, IWCMC 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 1125–1130. doi: 10.1109/IWCMC55113.2022.9824189.

[12] B. B. Gupta, A. Gaurav, V. Arya, and P. Kim, "A Deep CNN-

based Framework for Distributed Denial of Services (DDoS) Attack Detection in Internet of Things (IoT),” in 2023 Research in Adaptive and Convergent Systems RACS 2023, Association for Computing Machinery, Inc, Aug. 2023. doi: 10.1145/3599957.3606239.

[13] D. Kwon, R. M. Neagu, P. Rasakonda, J. T. Ryu, and J. Kim, “Evaluating Unbalanced Network Data for Attack Detection,” in SNTA 2023 - Proceedings of the 2023 on Systems and Network Telemetry and Analytics, Association for Computing Machinery, Inc, Jul. 2023, pp. 23–26. doi: 10.1145/3589012.3594898.

[14] S. Sambangi and L. Gondi, “Multiple Linear Regression Prediction Model for DDOS Attack Detection in Cloud ELB,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Oct. 2021. doi: 10.1145/3492547.3492567.

[15] S. Barbhuiya, P. Kilpatrick, and D. S. Nikolopoulos, “Linear Regression Based DDoS Attack Detection,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Feb. 2021, pp. 568–574. doi: 10.1145/3457682.3457769.

[16] J. Yang, H. Wang, and Y. Lu, “Web Attack Detection through Network-Traffic-Based Feature Engineering and Machine Learning,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Dec. 2020, pp. 103–108. doi: 10.1145/3444370.3444555.

[17] A. Alharthi, A. Eshmawi, A. Kabbas, and L. Hsairi, “Network traffic analysis for DDOS attack detection,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Nov. 2020. doi: 10.1145/3440749.3442637.

[18] J. Chen, Y. tao Yang, K. ke Hu, H. bin Zheng, and Z. Wang, “DAD- MCNN: DDoS attack detection via multi-channel CNN,” in ACM International Conference Proceeding Series, Association for Computing Machinery, 2019, pp. 484–488. doi: 10.1145/3318299.3318329.

[19] M. Shurman, R. Khrais, and A. Yateem, “DoS and DDoS attack detection using deep learning and IDS,” International Arab Journal of Information Technology, vol. 17, no. 4A Special Issue, pp. 655– 661, 2020, doi: 10.34028/iajit/17/4A/10.

[20] O. Thorat, N. Parekh, and R. Mangrulkar, “TaxoDaCML: Taxonomy based Divide and Conquer using machine learning approach for DDoS attack classification,” International Journal of Information Management Data Insights, vol. 1, no. 2, Nov. 2021, doi: 10.1016/j.jjimei.2021.100048.

[21] I. Sreeram and V. P. K. Vuppala, “HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm,” Applied Computing and Informatics, vol. 15, no. 1, pp. 59–66, Jan. 2019, doi: 10.1016/j.aci.2017.10.003.

[22] K. B. Virupakshar, M. Asundi, K. Channal, P. Shettar, S. Patil, and D. G. Narayan, “Distributed Denial of Service (DDoS) Attacks Detection System for OpenStack-based Private Cloud,” in Procedia Computer Science, Elsevier B.V., 2020, pp. 2297–2307. doi: 10.1016/j.procs.2020.03.282.

[23] A. Jaszcz and D. Połap, “AIMM: Artificial Intelligence Merged Methods for flood DDoS attacks detection,” Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 10, pp. 8090–8101, Nov. 2022, doi: 10.1016/j.jksuci.2022.07.021.

[24] N. V. Patil, C. Rama Krishna, K. Kumar, and S. Behal, “E-Had: A distributed and collaborative detection framework for early detection of DDoS attacks,” Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 4, pp. 1373–1387, Apr. 2022, doi: 10.1016/j.jksuci.2019.06.016.

[25] R. Priyadarshini and R. K. Barik, “A deep learning based intelligent framework to mitigate DDoS attack in fog environment,” Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 3, pp. 825–831, Mar. 2022, doi: 10.1016/j.jksuci.2019.04.010.

[26] S. Vattikuti, M. R. Hegde, M. Manish, V. Bodduvaram, and V. Sarasvathi, “DDoS Attack Detection and Mitigation using Anomaly Detection and Machine Learning Models,” in *CSITSS 2021 - 2021 5th International Conference on Computational Systems and Information Technology for Sustainable Solutions, Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/CSITSS54238.2021.9683214.

[27] R. Raj and S. Singh Kang, “Mitigating DDoS Attack using Machine Learning Approach in SDN,” in *Proceedings - 2022 4th International Conference on Advances in Computing, Communication Control and Networking, ICAC3N 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 462–467. doi: 10.1109/ICAC3N56670.2022.10074307.

[28] S. Santhosh, M. Sambath, and J. Thangakumar, “Detection of DDOS Attack using Machine Learning Models,” in *Proceedings of the 1st IEEE International Conference on Networking and Communications 2023, ICNWC 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICNWC57852.2023.10127537.

[29] D. Satyanarayana and A. S. Alasmi, “Detection and Mitigation of DDOS based Attacks using Machine Learning Algorithm,” in *International Conference on Cyber Resilience, ICCR 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ICCR56254.2022.9995773.

[30] G. Sujatha, Y. Kanchal, and G. George, “An Advanced Approach for Detection of Distributed Denial of Service (DDoS) Attacks Using Machine Learning Techniques,” in *3rd International Conference on Smart Electronics and Communication, ICOSEC 2022 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 821–827. doi: 10.1109/ICOSEC54921.2022.9951944.

[31] A. Kumar and I. Sharma, “Employing Supervised Learning Techniques for DDoS Attack Detection,” in *International Conference on Innovative Data Communication Technologies and Application, ICIDCA 2023 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 684–688. doi: 10.1109/ICIDCA56705.2023.10099834.

[32] Institute of Electrical and Electronics Engineers. Turkey Section. and Institute of Electrical and Electronics Engineers, *HORA 2020 : 2nd International Congress on Human-Computer Interaction, Optimization and Robotic Applications : proceedings : June 26-27, 2020, Turkey.*

[33] F. Nazarudeen and S. Sundar, “Efficient DDoS Attack Detection using Machine Learning Techniques,” in *2022 IEEE International Power and Renewable Energy Conference, IPRECON 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/IPRECON55716.2022.10059561.

[34] IEEE Staff, *2019 Amity International Conference on Artificial Intelligence (AICAI)*. IEEE, 2019.

[35] N. T. Bhutia, H. Verma, N. Chauhan, and L. K. Awasthi, “DDoS Attacks Detection in ‘Internet of Medical Things’ Using Machine Learning Techniques,” in *2022 IEEE Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation, IATMSI 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/IATMSI56455.2022.10119428.

[36] N. Chavan, M. Kukreja, G. Jagwani, N. Nishad, and N. Deb, “DDoS Attack Detection and Botnet Prevention using Machine Learning,” in *8th International Conference on Advanced Computing and Communication Systems, ICACCS 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 1159–1163. doi: 10.1109/ICACCS54159.2022.9785247.

[37] M. A. Mahmood and A. M. Zeki, “Securing IOT Against DDOS Attacks Using Machine Learning,” 2020.

[38] S. Thota and D. Menaka, “Importance of Machine Learning Algorithms to Detect Botnet DDoS Attacks,” in *Proceedings - International Conference on Augmented Intelligence and Sustainable Systems, ICAISS 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 900–903. doi: 10.1109/ICAISS55157.2022.10011016.

[39] R. Pandey, M. Pandey, and A. Nazarov, “Enhanced DDoS Detection using Machine Learning,” in *2023 6th International Conference on Information Systems and Computer Networks, ISCON 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ISCON57294.2023.10112033.

[40] M. Kavitha, M. Suganthy, A. Biswas, R. Srinivsan, R. Kavitha, and A. Rathesh, “Machine Learning Techniques for Detecting

DDoS Attacks in SDN," in *International Conference on Automation, Computing and Renewable Systems, ICACRS 2022 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 634–638. doi:10.1109/ICACRS55517.2022.10029110.

[41] A. U. Sudugala, W. H. Chanuka, A. M. N. Eshan, U. C. S. Bandara, and K. Y. Abeywardena, "WANHEDA: A Machine Learning Based DDoS Detection System," in *ICAC 2020 - 2nd International Conference on Advancements in Computing, Proceedings*, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 380– 385. doi: 10.1109/ICAC51239.2020.9357130.

[42] V. Deepa and B. Sivakumar, "Detection of DDoS Attack using Multiple Kernel Level (MKL) Algorithm," in *2022 International Conference on Innovative Trends in Information Technology, ICITIIT 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ICITIIT54346.2022.9744225.

[43] Institute of Electrical and Electronics Engineers. Turkey Section. and Institute of Electrical and Electronics Engineers, *HORA 2020 : 2nd International Congress on Human-Computer Interaction, Optimization and Robotic Applications : proceedings : June 26-27, 2020, Turkey.*

[44] C. Sathvika, V. Satwika, Y. Sruthi, M. Geethika, S. Bulla, and K. Swathi, "DDoS Attack Detection on Cloud Computing Services using Algorithms of Machine Learning: Survey," in *Proceedings - 7th International Conference on Computing Methodologies and Communication, ICCMC 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 1094–1100. doi: 10.1109/ICCMC56507.2023.10083549.

[45] R. Bhargava, Y. Pal Singh, and N. S. Narawade, "Implementation of Machine Learning Based DDOS Attack Detection System," in *2022 3rd International Conference for Emerging Technology, INCET 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/INCET54531.2022.9824036.

[46] Francis Xavier Engineering College and Institute of Electrical and Electronics Engineers, *Proceedings of the International Conference on Smart Systems and Inventive Technology (ICSSIT 2018) : Francis Xavier Engineering College, Tirunelveli, India, date: December 13-14, 2018*.

[47] A. Kazin, "DDoS SDN dataset." 15-Dec-2021.

[48] A. Sebbar and K. Zkik, "Enhancing resilience against DDoS attacks in SDN -based supply chain networks using machine learning," in 2023 9th International Conference on Control, Decision and Information Technologies (CoDIT), 2023, pp. 230–234.

[49] A. Gaurav, B. B. Gupta, K. Tai Chui, V. Arya, and E. Benkhelifa, "A DDoS attack detection system for industry 5.0 using digital twins and machine learning," in 2023 IEEE 12th Global Conference on Consumer Electronics (GCCE), 2023, pp. 1019–1022.

[50] A. Sharma and H. Babbar, "Evaluation and analysis: Internet of things using machine learning algorithms for detection of DDoS attacks," in 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), 2023, pp. 1203–1208.

[51] B. Ozcam, H. H. Kilinc, and A. H. Zaim, "Detecting TCP flood DDoS attack by anomaly detection based on machine learning algorithms," in 2021 6th International Conference on Computer Science and Engineering (UBMK), 2021, pp. 512–516.

[52] N. Jyoti and S. Behal, "A meta-evaluation of machine learning techniques for detection of DDoS attacks," in 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), 2021, pp. 522–526.

[53] R. S. Devi, R. Bharathi, and P. K. Kumar, "Investigation on efficient machine learning algorithm for DDoS attack detection," in 2023 International Conference on Computer, Electrical & Communication Engineering (ICCECE), 2023, pp. 1–5.

[54] Y. Sun, Y. Han, Y. Zhang, M. Chen, S. Yu, and Y. Xu, "DDoS attack detection combining time series-based multi-dimensional sketch and machine learning," in 2022 23rd Asia-Pacific Network Operations and Management Symposium (APNOMS), 2022, pp. 01–06.

[55] M. Kavitha, M. Suganthy, A. Biswas, R. Srinivsan, R. Kavitha, and A. Rathesh, "Machine Learning Techniques for Detecting DDoS Attacks in SDN," in International Conference on Automation, Computing and Renewable Systems, ICACRS 2022 - Proceedings, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 634–638. doi: 10.1109/ICACRS55517.2022.10029110.

[56] Kumar and I. Sharma, "Employing Supervised Learning Techniques for DDoS Attack Detection," in International Conference on Innovative Data Communication Technologies and Application, ICIDCA 2023 - Proceedings, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 684–688. doi: 10.1109/ICIDCA56705.2023.10099834.