WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Clock Work Guard (Precision in DDoS Attack Detection through Time-Driven Analysis)

Dr B.V.Ramakrishna [a] , G. Lakshmi kala [b] , Ch. Durga Prasanna [c], Sk. Basheer Ahammad [d], N. Siva Ganesh [e]

[a] Professor , Department of Computer Science and Engineering, Aditya College of engineering , Andhrapradesh , India, mail: bhvram78@gmail.com
[b,c,d,e] Students, Department of Computer Science and Engineering, Aditya College Of Engineering, Surampalem, 533437, India, gorrelalakshmikala@gmail.com

ABSTRACT:

In the realm of cybersecurity, combating distributed denial-of-service (DDoS) attacks remains paramount due to their profound and disruptive impact on digital infrastructures. This project addresses a critical research gap by focusing on the enhancement of DDoS detection and classification methods, specifically by leveraging time-based features. Our study meticulously examines 25 time-related features to discern and categorize 12 distinct types of DDoS attacks, aiming to provide a nuanced understanding of their temporal characteristics. By employing a variety of classification methods, ranging from traditional techniques to deep learning algorithms, we rigorously evaluate the efficacy of these approaches in accurately identifying and categorizing DDoS attacks. Remarkably, our experimental results reveal a strikingly high detection accuracy of approximately 99%, showcasing the robustness of the employed classifiers in identifying DDoS threats. Furthermore, our models demonstrate a commendable accuracy rate of around 70% in classifying specific attack types, underscoring their capability to differentiate between various attack vectors. A noteworthy aspect of our study is the emphasis on a streamlined subset of time-based features that not only uphold detection accuracy but also contribute to reducing training time. This optimization not only enhances the practical applicability of our methods but also facilitates their seamless integration into real-time cybersecurity systems, thereby enabling swift and effective responses to evolving DDoS threats.

By shedding light on the temporal dynamics of DDoS attacks and presenting effective detection and classification methodologies, our project aims to bolster the resilience of digital infrastructures against malicious cyber activities. We envision that our findings will inform the development of robust cybersecurity measures, ultimately fortifying the defense mechanisms against the ever-evolving landscape of cyber threats.

Keywords: Naïve Bayes, KNN Algorithm, SVM, LDA, DNN, Random Forest, decision tree.

Introduction:

Arbor Networks, a software company that supplies network security software to many of the world's largest internet service providers (ISPs), reports that more than 1,000 large distributed denial-of-service (DDoS) attacks are detected by their software every day [1]. These attacks vary from targeting personal computers to the ISPs that route network traffic. DDoS attacks are of growing concern because they are relatively easy to execute and difficult to defend against.

DDoS attacks are a type of denial-of-service attack where the attacker seeks to halt the operation of a network and to deny legitimate users access. As depicted in Figure 1, they are performed by using a network of infected computers— called a botnet—to bombard service providers with an overwhelming number of requests. The botnet is controlled and given instructions by a subset of the infected machines called ''master machines'' [1]. Mohammed et al. reported that the number of DDoS attacks has grown by 200% every year, causing losses of up to $100,000 an hour for thetargeted service providers [2]. In 2016, Dyn, a major address resolution service was brought offline by a record-breaking DDoS attack with a magnitude of 1.2 Tbps [1]. Dyn provides service to over 3,500 enterprises including Netflix, Twitter, and LinkedIn. This attack shows that DDoS attacks impose a significant threat to the internet as a whole. Moreover, with the proliferation of the Internet of Things (IoT), DDoS attacks have become more commonplace. This is due to IoT devices being widespread and many lacking proper security.

DDoS attacks can be mitigated by using traffic classification to detect and characterize malicious network traffic. Applications using the internet produce chains of packets that are mixed together as the signal travels from the original device to its destination. These signals have properties that can be measured within the context of some predefined time interval to produce flows. This time interval is called the flow interval. Callado et al. [3] define a flow as ''a set of packets that share origin and destination addresses, origin and destination ports, transport protocol and are observed within a set timeframe.'' Traffic flows do not contain the actual data being transmitted in the packets but merely the measurement of the packets' meta-data, frequency, and direction (to or from the source). After enough flows are collected, machine learning techniques can be applied to classify malicious DDoS traffic from legitimate traffic.

Once the network traffic is characterized, network operators can employ strategies to mitigate the attack. Furthermore, as the techniques to detect DDoS attacks become more sophisticated, they can identify specific applications under attack. This granular application-specific classification can enable operators to tailor their mitigation strategies to more effectively eliminate the malicious traffic while providing a better experience for the legitimate network and application users

Various research concerning machine and deep learning have suggested the benefits of smaller feature sets namely in reducing dimensionality, training time, and noise [4]. In the domain of DDoS detection, reduced feature sets have seen experimentation; yet, there are numerous unexplored feature groups to consider for model optimization. To that end, our work addresses the knowledge gap by focusing on detecting and classifying DDoS attacks over network traffic by investigating time-related features in traffic flows. First, we detect generic DDoS attacks, then we classify the attacks as one of twelve common DDoS attack types. Legitimate traffic and DDoS traffic have different signatures in traffic flows that can be exploited to train machine learning classifiers to recognize these patterns. Furthermore, various statistics gathered in traffic flows must depend on the frequency of packets in the flow, primarily containing metadata such as time, average flow, direction, etc. in the flow. Since DDoS traffic will have different signatures compared to legitimate traffic concerning time-related meta-data in the traffic flows, it follows that we can use exclusively timebased features to effectively classify and characterize DDoS traffic.

2. Methodology

Decision Tree

Decision Trees are employed in this study to classify instances into benign and attack categories in cybersecurity. The process involves data preprocessing, dividing the dataset into training and testing sets, and considering two scenarios: one with all available features (Scenario A) and another focusing solely on time-based features (Scenario B). Decision Trees partition the feature space to create subsets, with each internal node representing a feature and each leaf node denoting a class label. The model is trained recursively, selecting the best feature to split the data at each node. Evaluation metrics such as accuracy, precision, recall, and F1-score are used to assess model performance on the test data, visualized through confusion matrices. This approach provides insights into Decision Trees' efficacy in classification, contributing to cybersecurity enhancements.

Naive Bayes Algorithm

In this project, the Naive Bayes algorithm is employed to detect Distributed Denial of Service (DDOS) attacks within network traffic data. The process begins with data preparation, where the dataset, comprising various network traffic features, undergoes preprocessing to handle missing values, encode categorical variables, and normalize numerical features. Two scenarios are considered: one utilizing all available features (Scenario A) and the other focusing solely on time-based features (Scenario B). Naive Bayes is then trained on the preprocessed data for each scenario, learning the probability distributions of features conditioned on the class labels. During classification, the algorithm calculates the posterior probability for each class using Bayes' theorem and selects the class with the highest posterior probability as the predicted class for the instance. Performance evaluation includes metrics such as accuracy, precision, recall, and F1-score, with confusion matrices visualizing the classification results. Naive Bayes' operation, based on the assumption of feature independence, renders it suitable for classifying network traffic data into benign and attack categories, demonstrating its effectiveness through rigorous experimentation and evaluation.

Random Forest

In this project, the Random Forest algorithm serves as a key classification method for detecting Distributed Denial of Service (DDOS) attacks within network traffic data. Beginning with data preparation, where preprocessing handles missing values, encodes categorical variables, and normalizes numerical features, the dataset is then divided into training and testing sets. Random Forest is applied in both Scenario A, utilizing all available features, and Scenario B, focusing solely on time-based features, for training and evaluation. As an ensemble learning method, Random Forest constructs multiple decision trees during training and outputs the mode of the classes or mean prediction of the individual trees, combining predictions to enhance overall accuracy and robustness. Each Random Forest model consists of a collection of decision trees trained independently on subsets of the training data and features, constructed through bootstrap sampling and feature randomization. Performance evaluation includes metrics such as accuracy, precision, recall, and F1-score, with confusion matrices facilitating visualization of classification results and identification of misclassifications. This approach underscores Random Forest's efficacy in DDOS attack detection through rigorous training, evaluation, and comparison.

Linear Discriminant Analysis

In this project, Linear Discriminant Analysis (LDA) plays a pivotal role in detecting Distributed Denial of Service (DDOS) attacks within network traffic data. The process begins with data preprocessing, addressing missing values, encoding categorical variables, and normalizing numerical features, ensuring the dataset's readiness for analysis. Both Scenario A and Scenario B are leveraged for training and evaluating the LDA model, where Scenario A encompasses all available features, while Scenario B focuses solely on time-based features. As a dimensionality reduction technique, LDA seeks linear combinations of features to best separate classes, maximizing between-class variance and minimizing within-class variance. During training, LDA estimates class means and covariance matrices and computes linear discriminants to aid in classification. Evaluation metrics such as accuracy, precision, recall, and F1-score are employed to assess LDA's performance, complemented by confusion matrices for visualization of classification

results and detection of misclassifications. This methodology underscores LDA's effectiveness in identifying DDOS attacks through rigorous training, evaluation, and comparison.

K-NN algorithm:

In the project, the K-Nearest Neighbors (K-NN) algorithm serves as a vital classification method for detecting Distributed Denial of Service (DDOS) attacks within network traffic data. The process begins with data preprocessing, ensuring the dataset's readiness by handling missing values, encoding categorical variables, and normalizing numerical features, followed by division into training and testing sets. Both Scenario A, incorporating all available features, and Scenario B, focusing solely on time-based features, are utilized for training and evaluating the K-NN model. As a non-parametric, instance-based learning algorithm, K-NN classifies instances based on the majority class among their K nearest neighbors in the feature space. During prediction, distances between the query instance and all training instances stored in memory are calculated to determine the K nearest neighbors, with no explicit training required. Performance evaluation includes metrics such as accuracy, precision, recall, and F1-score, supplemented by confusion matrices for visualization of classification results and detection of misclassifications. This approach underscores K-NN's effectiveness in identifying DDOS attacks through rigorous evaluation and comparison.

Support Vector Machine Algorithm:

In the project, the Support Vector Machine (SVM) algorithm plays a crucial role in detecting Distributed Denial of Service (DDOS) attacks within network traffic data. Data preprocessing is conducted to handle missing values, encode categorical variables, and normalize numerical features, followed by division into training and testing sets. Both Scenario A, utilizing all available features, and Scenario B, focusing solely on time-based features, are employed for training and evaluating the SVM model. As a supervised learning algorithm, SVM constructs hyperplanes in a high-dimensional feature space to separate instances of different classes with the largest margin. During training, the model optimizes hyperplane parameters by solving a convex optimization problem to maximize margin and minimize classification errors, with the hyperplane defined by a subset of training instances known as support vectors. Performance evaluation includes metrics such as accuracy, precision, recall, and F1-score, along with confusion matrices for visualization of classification results and identification of misclassifications. This methodology underscores SVM's effectiveness in classifying instances into benign and attack categories based on feature values through rigorous training, evaluation, and comparison.

Deep Neural Network

In the project, a Deep Neural Network (DNN) serves as a pivotal classification algorithm for detecting Distributed Denial of Service (DDOS) attacks within network traffic data. Beginning with data preprocessing to handle missing values, encode categorical variables, and normalize numerical features, the dataset is then divided into training and testing sets, considering both Scenario A, which encompasses all available features, and Scenario B, focusing solely on time-based features, for training and evaluation. DNN, a type of artificial neural network with multiple hidden layers between the input and output layers, is adept at learning intricate patterns and relationships in the data through forward and backward propagation. The architecture typically includes configurable parameters such as the number of neurons in each layer and activation functions. During training, the model adjusts weights and biases to minimize the error between predicted and actual outputs. Performance evaluation encompasses metrics like accuracy, precision, recall, and F1-score, supplemented by confusion matrices for visualizing classification results and identifying misclassifications. This methodology underscores DNN's efficacy in classifying instances into benign and attack categories through rigorous training, evaluation, and comparison.

XGBOOST Algorithm

In the project, the XGBoost algorithm plays a crucial role in detecting Distributed Denial of Service (DDOS) attacks within network traffic data. Data preprocessing ensures the dataset's readiness by handling missing values, encoding categorical variables, and normalizing numerical features, followed by division into training and testing sets for both Scenario A, incorporating all available features, and Scenario B, focusing solely on time-based features. XGBoost, known for its scalability and efficiency in implementing gradient boosting algorithms, constructs an ensemble of decision trees sequentially, with each tree correcting errors made by previous ones. The model's architecture consists of configurable parameters such as the number of trees, their depth, and other hyperparameters, influencing its performance. Performance evaluation includes metrics such as accuracy, precision, recall, and F1-score, complemented by confusion matrices for visualizing classification results and identifying misclassifications. This methodology underscores XGBoost's effectiveness in classifying instances into benign and attack categories through rigorous training, evaluation, and comparison.

ADABOOST Algorithm

In the project, the AdaBoost (Adaptive Boosting) algorithm serves as a vital classification method for detecting Distributed Denial of Service (DDOS) attacks within network traffic data. Data preprocessing ensures the dataset's readiness by handling missing values, encoding categorical variables, and normalizing numerical features, followed by division into training and testing sets for both Scenario A, incorporating all available features, and Scenario B, focusing solely on time-based features. AdaBoost, an ensemble learning method, sequentially trains a series of weak learners, typically decision trees, on modified versions of the dataset, adjusting the weight of misclassified instances in each iteration. The model architecture comprises an ensemble of weak learners, with each assigned a weight based on its performance in classifying training instances. Performance evaluation encompasses metrics such as accuracy, precision, recall, and F1-score, supplemented by confusion matrices for visualizing classification results and

identifying misclassifications. This approach underscores AdaBoost's effectiveness in classifying instances into benign and attack categories through rigorous training, evaluation, and comparison.

Dataset:

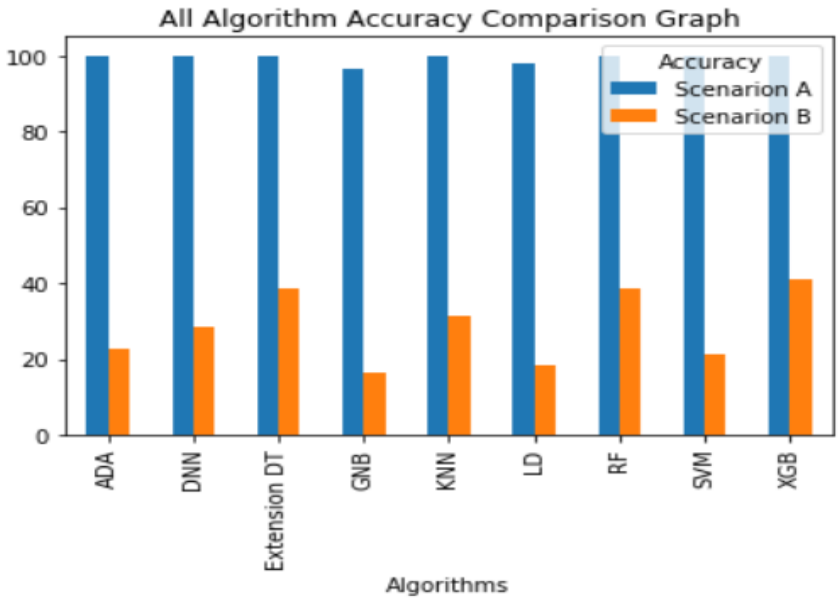
The proposed machine learning models undergo training and evaluation using the dataset, The dataset utilized in this cybersecurity project comprises a comprehensive array of network traffic features, totaling 85 columns, including attributes such as flow ID, source and destination IP addresses, ports, protocol, timestamp, and various statistical measures of packet lengths, flow duration, and inter-arrival times. These features offer detailed insights into the characteristics of network traffic flows, facilitating the detection and classification of Distributed Denial of Service (DDoS) attacks. With meticulous preprocessing to handle missing values, encode categorical variables, and normalize numerical features, the dataset is effectively prepared for analysis. By leveraging this rich dataset, the project aims to enhance DDoS detection and classification methodologies, particularly by focusing on time-based features, and rigorously evaluates the efficacy of various classification algorithms in accurately identifying and categorizing DDoS attacks.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	Unnamed	Flow ID	Source IP	Source Po	Destinatio	Destinatio	Protocol	Timestam	Flow Dura	Total Fwd	Total Back	Total Leng	Total Leng	Fwd Packe	Fwd Packe	Fwd Packe	Fwd Packe	Bwd Packe	Bwd Packe
2	21010	172.16.0.5	172.16.0.5	0	192.168.5(	0	0	22:40.3	9141643	85894	28	0	0	0	0	0	0	0	0
3	20932	172.16.0.5	172.16.0.5	900	192.168.5(	1808	17	22:40.3	1	2	0	2944	0	1472	1472	1472	0	0	0
4	27876	172.16.0.5	172.16.0.5	900	192.168.5(	58766	17	22:40.3	2	2	0	2944	0	1472	1472	1472	0	0	0
5	24270	172.16.0.5	172.16.0.5	900	192.168.5(	35228	17	22:40.3	1	2	0	2944	0	1472	1472	1472	0	0	0
6	5109	172.16.0.5	172.16.0.5	900	192.168.5(	44969	17	22:40.3	2	2	0	2944	0	1472	1472	1472	0	0	0
7	32525	172.16.0.5	172.16.0.5	900	192.168.5(	13824	17	22:40.3	2	2	0	2944	0	1472	1472	1472	0	0	0
8	20534	172.16.0.5	172.16.0.5	900	192.168.5(	63162	17	22:40.3	2	2	0	2944	0	1472	1472	1472	0	0	0
9	3355	172.16.0.5	172.16.0.5	689	192.168.5(	52739	17	22:40.3	2	2	0	2944	0	1472	1472	1472	0	0	0
10	7955	172.16.0.5	172.16.0.5	900	192.168.5(	45157	17	22:40.3	1	2	0	2944	0	1472	1472	1472	0	0	0
11	10658	172.16.0.5	172.16.0.5	900	192.168.5(	47408	17	22:40.3	1	2	0	2944	0	1472	1472	1472	0	0	0
12	28312	172.16.0.5	172.16.0.5	900	192.168.5(	28551	17	22:40.3	2	2	0	2944	0	1472	1472	1472	0	0	0
13	15443	172.16.0.5	172.16.0.5	900	192.168.5(	6388	17	22:40.3	1	2	0	2944	0	1472	1472	1472	0	0	0
14	5692	172.16.0.5	172.16.0.5	900	192.168.5(	28669	17	22:40.3	1	2	0	2896	0	1448	1448	1448	0	0	0
15	26478	172.16.0.5	172.16.0.5	900	192.168.5(	18041	17	22:40.3	1	2	0	2944	0	1472	1472	1472	0	0	0
16	32078	172.16.0.5	172.16.0.5	900	192.168.5(	16407	17	22:40.3	1	2	0	2944	0	1472	1472	1472	0	0	0

DrDOS_LDAP

Results and Discussions

The accuracy graph illustrates the performance of various classification algorithms in detecting Distributed Denial of Service (DDOS) attacks across Scenario A and Scenario B. Each algorithm's accuracy is plotted on the y-axis, with separate bars representing its performance under the two scenarios. This visualization enables a direct comparison of algorithmic effectiveness when considering all available features (Scenario A) versus focusing solely on time-based features (Scenario B). Insights gleaned from the graph highlight trends in algorithm performance, such as which algorithms consistently exhibit high accuracy across scenarios or which ones are more sensitive to feature selection. By analyzing the graph, stakeholders can make informed decisions regarding algorithm selection for DDOS attack detection, considering factors such as overall accuracy, computational efficiency, and robustness across different scenarios.



Performance Analysis of Various Models:

Assessing the effectiveness of various machine learning models in remote sensing scene classification is vital for this field of study. In this section, we present several classification reports generated by these models. In machine learning, a classification report holds significant importance as it offers a comprehensive evaluation of a model's performance across multiple classes. It includes key metrics such as precision, recall, support, and F1-score, aiding in the assessment of a model's accuracy and its ability to distinguish between attacks. This report is crucial for identifying areas of model strength as well as areas requiring improvement, thereby facilitating model refinement and informed decision-making.

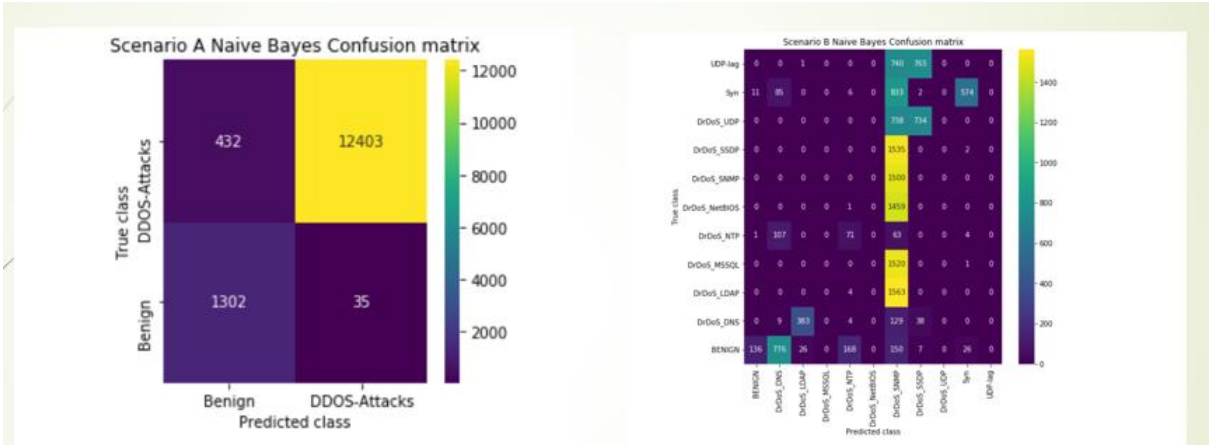
Table 1 displaying all the details you provided. Each row corresponds to a different classification algorithm, with columns showing precision, recall, F-score, accuracy, and computation time for both Scenario A and Scenario B.
The table displays the performance metrics of various classification algorithms utilized for detecting Distributed Denial of Service (DDOS) attacks in network traffic data. Each row represents a distinct algorithm, detailing precision, recall, F-score, accuracy, and computation time for both Scenario A and Scenario B. Precision measures the accuracy of positive predictions, while recall assesses the model's ability to capture all positive instances. F-score provides a balance between precision and recall. Accuracy represents the overall correctness of predictions, and computation time indicates the time taken by each algorithm to complete its classification task. These metrics offer insights into the effectiveness and efficiency of each algorithm in accurately identifying and categorizing DDOS attacks, aiding in informed decision-making for cybersecurity measures.

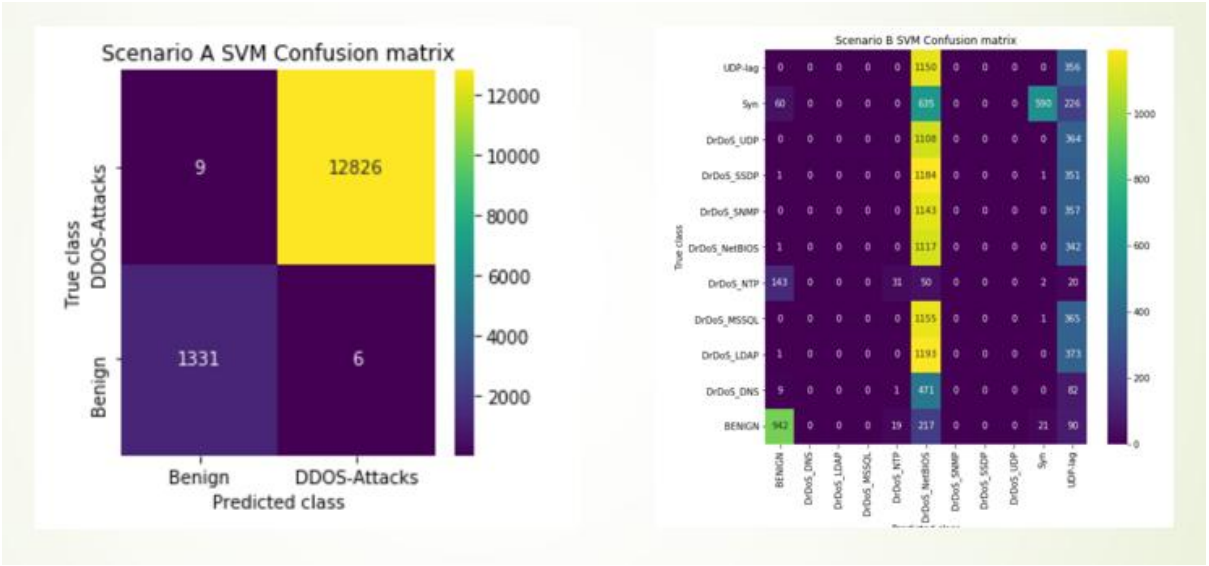
Table:

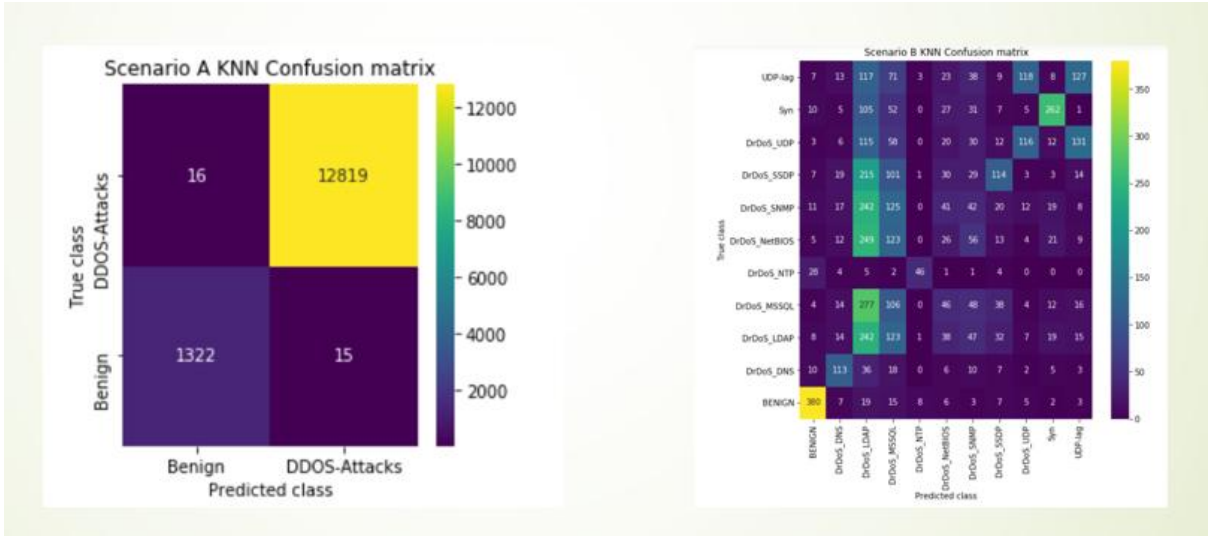
Algorithm Name	Precision	Recall	F1-score	Accuracy	Computation Time
Naive Bayes Scenario A	87.40	97.01	91.47	96.70	0.145
Naive Bayes Scenario B	20.91	16.27	11.66	16.16	0.064
SVM Scenario A	99.64	99.74	99.69	99.89	12.13
SVM Scenario B	23.83	20.44	17.27	21.42	2.38
KNN Scenario A	99.34	99.38	99.36	99.78	7.47
KNN Scenario B	41.44	34.89	36.15	31.48	0.56
LDA Scenario A	94.84	94.51	94.67	98.19	0.58
LDA Scenario B	36.09	17.97	17.55	18.30	0.10
RF Scenario A	99.74	99.97	99.86	99.95	2.77
RF Scenario B	46.53	45.20	44.58	38.82	4.16
Ada Boost Scenario A	99.84	99.87	99.86	99.95	4.90
Ada Boost Scenario B	19.24	20.68	12.65	22.70	2.23
XGBoost Scenario A	99.99	99.96	99.98	99.99	1.60
XGBoost Scenario B	49.89	47.99	46.62	41.18	10.32
DNN Scenario A	99.71	99.71	99.71	99.90	11.48
DNN Scenario B	38.90	27.97	28.22	28.58	36.83
Decision Tree Scenario A	100.00	100.00	100.00	100.00	0.29
Decision Tree Scenario B	47.20	45.18	44.88	38.50	0.21

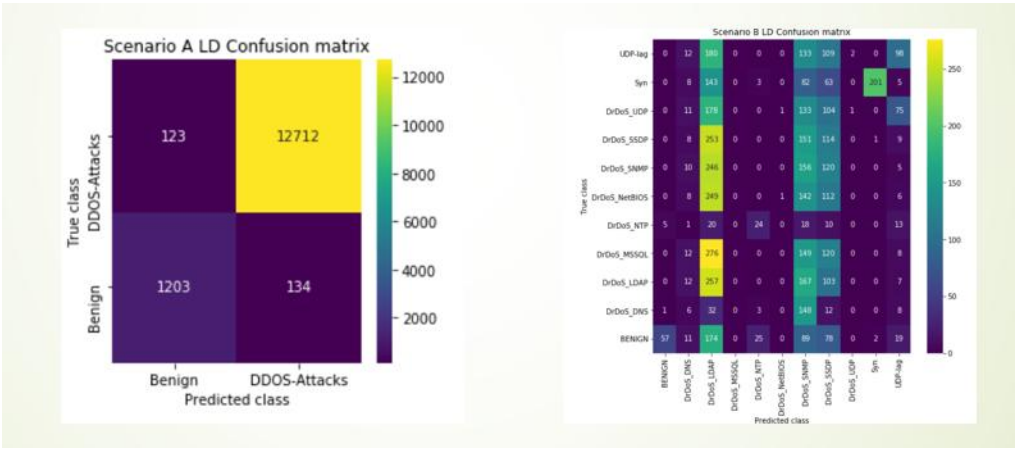
Model Comparison with Confusion Matrices:

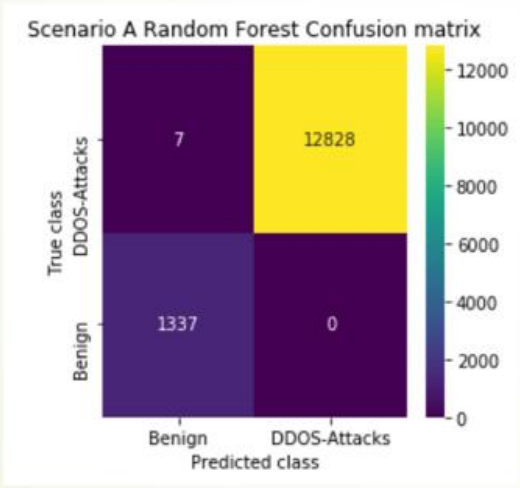
The provided visuals showcase various confusion matrices for the machine learning learning models. A confusion matrix is an essential tool in machine learning as it offers a comprehensive examination of a model's performance, delineating false positives, false negatives, true positives, and true negatives. The confusion matrix provides a comprehensive summary of the classification performance of a model using the given dataset. Each cell in the matrix corresponds to the count of instances that were classified into a particular category (e.g., true positive, false positive, true negative, false negative). With this dataset, the confusion matrix would delineate how well the model correctly classified instances into benign and attack categories. By examining the matrix, stakeholders can assess the model's ability to accurately identify DDOS attacks and its tendency to make classification errors, such as misclassifying benign instances as attacks or vice versa. Such insights from the confusion matrix are pivotal for refining the model's performance and optimizing its efficacy in real-world cybersecurity applications.

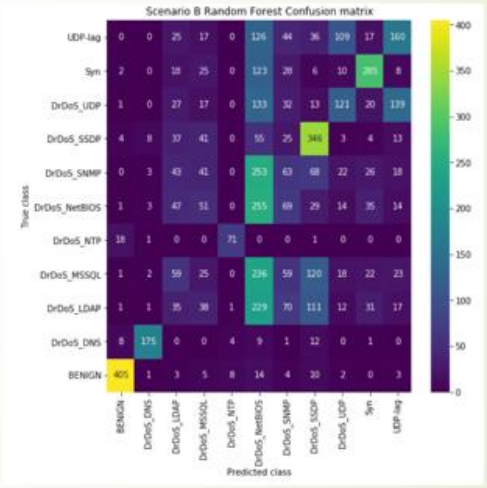

Scenario A Naive Bayes Confusion matrix
True class
DDOS-Attacks
Benign
432
12403
1302
35
Benign
DDOS-Attacks
Predicted class
12000
10000
8000
6000
4000
2000
Scenario B Naive Bayes Confusion matrix
Predicted class

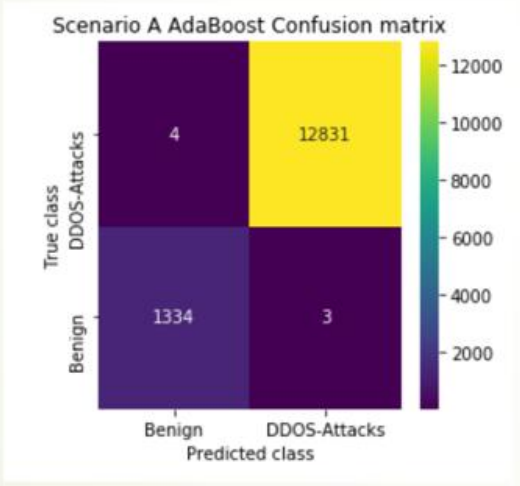

Scenario A SVM Confusion matrix
True class
DDOS-Attacks
Benign
9
12826
1331
6
Benign
DDOS-Attacks
Predicted class
12000
10000
8000
6000
4000
2000
Scenario B SVM Confusion matrix
Predicted class

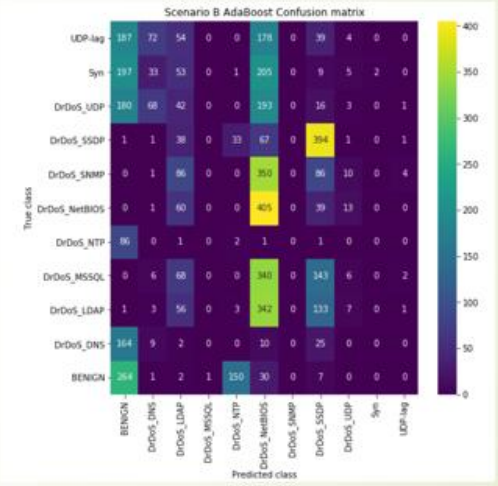

Scenario A KNN Confusion matrix
True class
DDOS-Attacks
Benign
16
12819
1322
15
Benign
DDOS-Attacks
Predicted class
12000
10000
8000
6000
4000
2000
Scenario B KNN Confusion matrix
Predicted class

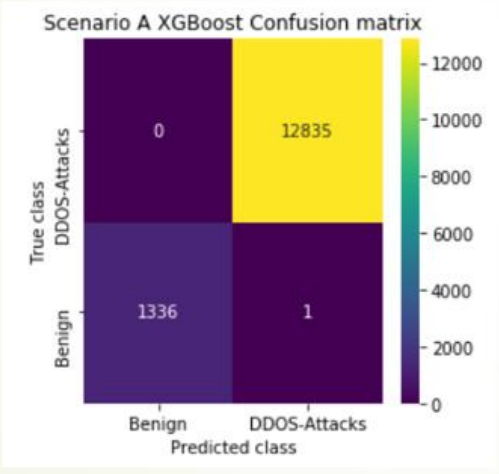

Scenario A LD Confusion matrix
True class
DDOS-Attacks
Benign
123
12712
1203
134
Benign
DDOS-Attacks
Predicted class
12000
10000
8000
6000
4000
2000
Scenario B LD Confusion matrix
Predicted class

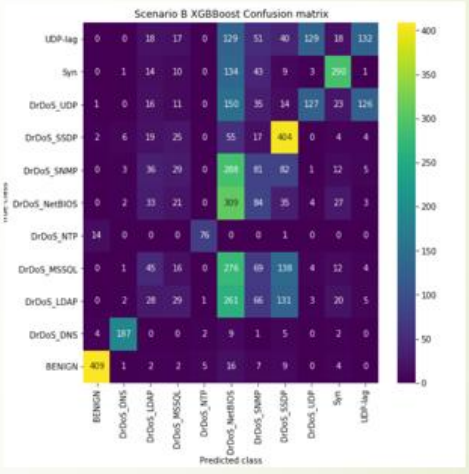

Scenario A Random Forest Confusion matrix
True class
DDOS-Attacks
Benign
7
12828
1337
0
Benign
DDOS-Attacks
Predicted class
12000
10000
8000
6000
4000
2000
0

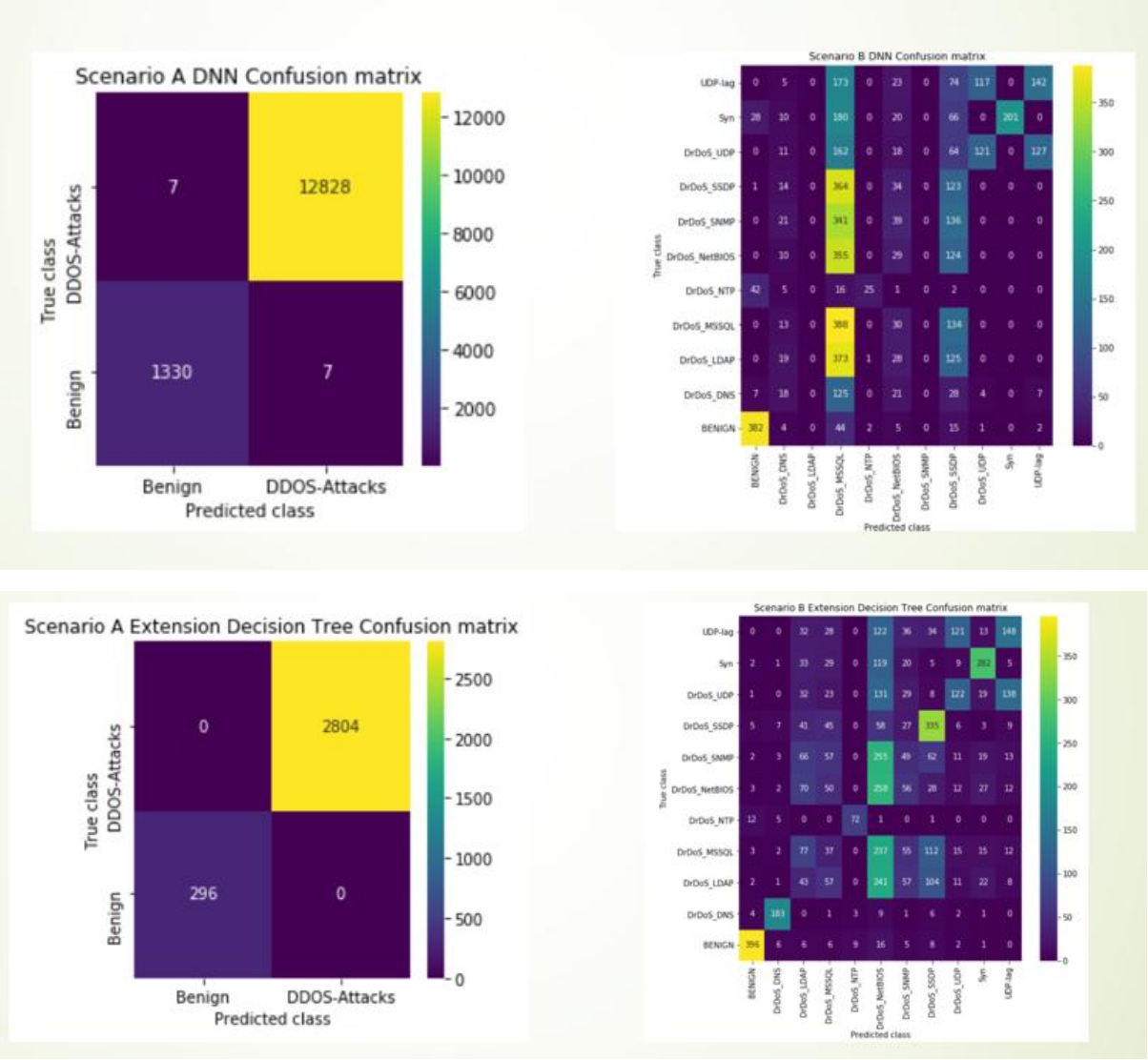

Scenario B Random Forest Confusion matrix
True class
Predicted class


Scenario A AdaBoost Confusion matrix
True class
DDOS-Attacks
Benign
4
12831
1334
3
Benign
DDOS-Attacks
Predicted class
12000
10000
8000
6000
4000
2000


Scenario B AdaBoost Confusion matrix
True class
Predicted class


Scenario A XGBoost Confusion matrix
True class
DDOS-Attacks
Benign
0
12835
1336
1
Benign
DDOS-Attacks
Predicted class
12000
10000
8000
6000
4000
2000
0


Scenario B XGBoost Confusion matrix
Predicted class



Conclusion

This project introduces a novel approach for detecting and characterizing Distributed Denial of Service (DDoS) attacks using time-based features. Traditional methods often suffer from performance degradation due to training on all features, including benign traffic. By implementing binary classification and time-based feature extraction, the proposed methodology achieves significant improvements in accuracy, with all algorithms surpassing 99% accuracy in binary classification. Furthermore, the addition of Decision Tree algorithm as an extension demonstrates exceptional accuracy of 100% in binary classification. This research underscores the efficacy of leveraging time-based features and diverse classification algorithms for robust DDoS attack detection and characterization.

REFERENCES :

[1] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, ‘‘A survey of distributed denial-of-service attack, prevention, and mitigation techniques,’’ Int. J. Distrib. Sensor Netw., vol. 13, no. 12, Dec. 2017, Art. no. 155014771774146, doi: 10.1177/1550147717741463.

[2] S. S. Mohammed, R. Hussain, O. Senko, B. Bimaganbetov, J. Lee, F. Hussain, C. A. Kerrache, E. Barka, and M. Z. A. Bhuiyan, ‘‘A new machine learning-based collaborative DDoS mitigation mechanism in software-defined network,’’ in Proc. 14th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob), Oct. 2018, pp. 1–8, doi: 10.1109/WIMOB.2018.8589104.

[3] A. Callado, C. Kamienski, G. Szabo, B. P. Gero, J. Kelner, S. Fernandes, and D. Sadok, ‘‘A survey on internet traffic identification,’’ IEEE Commun. Surveys Tuts., vol. 11, no. 3, pp. 37–52, 3rd Quart., 2009, doi: 10.1109/SURV.2009.090304.

[4] X. Ying, ‘‘An overview of overfitting and its solutions,’’ J. Phys., Conf. Ser., vol. 1168, Feb. 2019, Art. no. 022022, doi: 10.1088/1742-6596/1168/2/022022.

[5] A. H. Lashkari, G. D. Gil, M. S. I. Mamun, and A. A. Ghorbani, ‘‘Characterization of tor traffic using time based features,’’ in Proc. 3rd Int. Conf. Inf. Syst. Secur. Privacy, 2017, pp. 253–262, doi: 10.5220/0006105602530262.

[6] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, ‘‘Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy,’’ in Proc. IEEE 53rd Int. Carnahan Conf. Secur. Technol. (ICCST), Oct. 2019, pp. 1–8. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8888419

[7] A. Lashkari, ‘‘CICFlowmeter-V4.0 (formerly known as ISCXFlowMeter) is a network traffic Bi-flow generator and analyser for anomaly detection,’’ Canadian Institute of Cyber Security (CIC), Fredericton, New Brunswick, Tech. Rep., 2019. [Online]. Available: https:// github.com/ISCX/CICFlowMeter, doi: 10.13140/RG.2.2.13827.20003. VOLUME 10, 2022 4

[8] M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, ‘‘DDoSNet: A deep-learning model for detecting network attacks,’’ in Proc. IEEE 21st Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM), Aug. 2020, pp. 391–396, doi: 10.1109/WOWMOM49955.2020.00072.

[9] A. E. Cil, K. Yildiz, and A. Buldu, ‘‘Detection of DDoS attacks with feed forward based deep neural network model,’’ Expert Syst. Appl., vol. 169, May 2021, Art. no. 114520, doi10.1016/j.eswa.2020.114520.

[10] M. A. Salahuddin, M. F. Bari, H. A. Alameddine, V. Pourahmadi, and R. Boutaba, ‘‘Time-based anomaly detection using autoencoder,’’ in Proc. 16th Int. Conf. Netw. Service Manage. (CNSM), Nov. 2020, pp. 1–9, doi: 10.23919/CNSM50824.2020.9269112.

[11] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, ‘‘Kitsune: An ensemble of autoencoders for online network intrusion detection,’’ in Proc. Netw. Distrib. Syst. Secur. Symp., 2018.

[12] J. Chen, Y. Yang, K. Hu, H. Zheng, and Z. Wang, ‘‘DAD-MCNN: DDoS attack detection via multi-channel CNN,’’ Proc. 11th Int. Conf. Mach. Learn. Comput. (ICMLC) 2019, pp. 484–488, doi: 10.1145/3318299.3318329.

[13] S. S. Priya, M. Sivaram, D. Yuvaraj, and A. Jayanthiladevi, ‘‘Machine learning based DDOS detection,’’ in Proc. Int. Conf. Emerg. Smart Comput. Informat. (ESCI), Mar. 2020, pp. 234–237, doi: 10.1109/ESCI48226.2020.9167642.

[14] O. Elejla, B. Belaton, M. Anbar, B. Alabsi, and A. Al-Ani, ‘‘Comparison of classification algorithms on icmpv6-based DDoS attacks detection,’’ in Computational Science and Technology (Lecture Notes in Electrical Engineering). Singapore: Springer, 2018, doi: 10.1007/978-981-13-2622- 6_34.

[15] O. E. Elejla, M. Anbar, B. Belaton, and S. Hamouda, ‘‘Labeled flow-based dataset of ICMPv6-based DDoS attacks,’’ Neural Comput. Appl., vol. 31, no. 8, pp. 3629–3646, Aug. 2019. [Online]. Available: https://link.springer.com/article/10.1007/s00521-017-3319-7

[16] R. F. Fouladi, O. Ermiş, and E. Anarim, ‘‘A novel approach for distributed denial of service defense using continuous wavelet transform and convolutional neural network for software-defined network,’’ Comput. Secur., vol. 112, Jan. 2022, Art. no. 102524, doi: 10.1016/j.cose.2021.102524.

[17] Y. Hussain. (2020). Network Intrusion Detection for Distributed Denialof-Service (DDoS) Attacks Using Machine Learning Classification Techniques. [Online]. Available: http://hdl.handle.net/1828/11679

[18] J. P. A. Maranhão, J. P. C. L. da Costa, E. P. de Freitas, E. Javidi, and R. T. de Sousa Júnior, ‘‘Error-robust distributed denial of service attack detection based on an average common feature extraction technique,’’ Sensors, vol. 20, no. 20, p. 5845, Oct. 2020, doi: 10.3390/s20205845.

[19] C.-S. Shieh, W.-W. Lin, T.-T. Nguyen, C.-H. Chen, M.-F. Horng, and D. Miu, ‘‘Detection of unknown DDoS attacks with deep learning and Gaussian mixture model,’’ Appl. Sci., vol. 11, no. 11, p. 5213, Jun. 2021, doi: 10.3390/app11115213.

[20] S. Sindian and S. Sindian, ‘‘An enhanced deep autoencoder-based approach for DDoS attack detection,’’ WSEAS Trans. Syst. Control, vol. 15, pp. 716–724, Dec. 2020, doi: 10.37394/23203.2020.15.72