OPEN ACCESS 100

ISSN 2356-5462
http://socj.telkomuniversity.ac.id/ijoict/

Intl. Journal on ICT
Vol. 10, No. 1, Jun 2024. pp. 100-109
doi: doi.org/10.21108/ijoict.v10i1.964

Enhancing Cybersecurity Against DDOS Attacks Evaluating Supervised Machine Learning Techniques

P.Janaki[1*], E.Karthikeyan[2]

[1,2]*Department of Computer Science, Government Arts College*
Udumalpet, Tamilnadu, India.
**janaki95bca@gmail.com, [2]First-Third University*

Abstract

An individual or group launches a cyber attack when they intentionally try to get into another person's or group's computer system. Typically, the goal of an attacker is to gain an advantage by interfering with the victim's network. Now that COVID-19 has wreaked havoc on businesses throughout the world, it's cybercriminals' ideal storm. When it comes to cyber threats, Distributed Denial-Of-Service attacks (DDoS) are the most common and dangerous for corporate networks, apps, and services. Distributed denial of service attacks aim to flood a server, service, or network with malicious traffic in an effort to interrupt regular traffic. Financial losses, decreased productivity, damaged brands, worse credit and insurance ratings, damaged relationships with suppliers and customers, and IT budget overruns are all possible outcomes. Developing Network Intrusion Detection Systems (NIDSs) that can reliably foretell DDoS attacks is an urgent issue. This study used the CICDDoS2019 dataset to assess supervised Machine Learning (ML) methods. The machine learning algorithms that were assessed include AdaBoost, Naïve Bayes, MLP-ANN, Random Forest, and SVM. We use the assessment metrics: Area Under the Curve (AUC), Accuracy, F-measure, Precision, and Recall. This study demonstrates that of the algorithms tested, AdaBoost shows the highest promise in detecting DDoS attacks.

Keywords: Cyber attacks, Machine learning, Intrusion Detection System

I. INTRODUCTION

AN interruption sent from one computer to another, or even to servers in a network, is known as a cyber attack [1]. Malware, Phishing, Ransomware, Denial of Service, Crypto-jacking, SQL injection, Zero-day vulnerabilities, and Man-in-the-Middle attacks are just a few examples of data security concerns [2]. Over the course of the COVID epidemic, DDoS attacks increased in frequency, following Ransomware's lead [3]. The growth of DDoS is likely related to the global corona virus epidemic, according to experts at Kaspersky [4]. Criminals online often mistakenly believe that small businesses are easier targets than large corporations. Organizations should take precautions against more than just ransom ware when it comes to network attacks [5].

Online transactions are the only ones most people trust during COVID-19 environment. The internet is the hub of all company operations. Because of this pandemic most of people recommended to work from home by the majority of the organizations [6]. As a result of the corona virus epidemic, more and more individuals are turning to online platforms for their educational and training needs. People felt secure using contactless support via online services. As a result, online services are promising for all types of businesses [7]. All of the businesses processed billions of dollars

Received on 28 Jun 2024. Revised on 12 July 2024. Accepted and Published on 24 July 2024.

worth of transactions in a single day. There would be serious financial consequences for the customer and the company if the network problems caused even a single minute of delay [8].

Prior to the pandemic, DDoS attack volumes were already significant, with the regular reports of large-scale attacks targeting various sectors such as finance, e-commerce, and government institutions. Attackers continuously developed new techniques and exploited vulnerabilities to increase the scale and effectiveness of their attacks. The COVID-19 pandemic led to a surge in internet usage as more people shifted to remote work, online transactions and business. This will create the new opportunities for cyber criminals to launch DDoS attacks. As the world adapts to post-pandemic conditions, the volume of DDoS attacks may continue to fluctuate. Over the years, since 2018 DDoS has increased its volume to bring down legal services.

At this juncture, the criminal will launch DDoS attacks on the victim. DDoS attacks are a major headache for businesses and their clients [9-10]. The best way to identify DDoS attacks is via an Intrusion Detection System (IDS). IDS will keep a close eye on all of the data sent to and from a certain server, and it will respond swiftly to any signs of attack [11-12]. A mix of hardware and software applications makes up IDS. In such an attack scenario, intrusion detection systems will sound the alert and reject the attacker's nefarious actions [13-14]. In order to distinguish between typical and non-standard network traffic, a machine learning system is used [15].

In light of the enormous disruptions brought about by the COVID-19 pandemic, the urgent necessity to counter the growing danger of DDoS attacks is driving this study. Businesses are suffering major repercussions including financial losses, decreased productivity, and reputational harm as cybercriminals take advantage of this anarchy to attack them. It is impossible to successfully counter this danger without Network Intrusion Detection Systems (NIDSs. In order to reliably forecast DDoS attacks, this research examines supervised Machine Learning (ML) methods using the CICDDoS2019 dataset. The study shows that the AdaBoost algorithm is the most promising method for identifying DDoS attacks by comparing it to Naïve Bayes, MLP-ANN, Random Forest, and SVM using important metrics including AUC, Accuracy, F-measure, Precision, and Recall. In order to protect company networks, apps, and services from ever-changing cyber threats, this study is essential for improving cyber security safeguards.

DDoS attacks are considered as a most dangerous for several reasons, that are Disruption of services, financial loss, Reputation damage, Facilitation of other attacks, Accessibility to attack tools and difficulty in mitigation. This research has demonstrated the effectiveness of machine learning techniques in detecting and mitigating DDoS attacks within network infrastructures. In our paper, we have identify the best ML algorithm to deal with the identification of DDoS occurrence by utilizing the some attributes of flow entries.

The order of remaining paper is as following: In Section 2, the related existing works for defense mechanisms against DDoS using Machine Learning are discussed and analyzed. Section 3, proposed and discussed our approach, and discussed about various machine learning algorithms. The section 4, shows the implementation and evaluation of our proposed work, and finally section 5, end with the conclusion.

II. LITERATURE REVIEW

Alfatemi, A., et al. [2] researched about one of the most common dangers in today's linked cyber scene was distributed denial of service (DDoS) attacks. They have developed a stable and very accurate detection method by combining Deep ResNets with synthetic oversampling techniques. This was the main contribution of these authors study. The author solves the problem of classic detection algorithms' poor performance by taking use of the class imbalance that exists in many cyber-security datasets. The author successfully balanced the dataset using the Synthetic Minority Over-sampling Technique (SMOTE), which allowed the model to identify subtle attack patterns that were frequently missed by traditional approaches.

Aslam, N., et al. [4] proposed SDN's potential in the networking industry was enormous. Among the many pressing issues that need fixing was the lack of assurance around the safety of SDN. Users were worried about the growing number of distributed denial of service attacks. The frequency with which attackers attempt to bring the services' servers down increases annually. One of the biggest obstacles was dealing with DDoS attacks in a timely manner. In addition to finding and fixing the problem, it's critical to avoid increasing the server load and to fix it quickly so that users don't experience any significant downtime.

Bukhowah, R., et al. [6] presents an overview of ICN designs and their integration with the Internet of Things (IoT). With a focus on denial-of-service attacks, the article offers a thorough literature analysis that covers typical cyber security risks. These authors research shows that denial-of-service (DoS) attacks were a major problem for the Internet of Things (IoT) and the Internet of Connection (ICN). To help combat this, the author provide methods for identifying

and reducing the impact of these attacks using integrated ML technologies like Support Vector Machines (SVM), Random Forest (RF), and K-Nearest Neighbors (KNN).

Das, S., et al. [7] proposed DDoS attack detection and prevention methods. While the study was still in its early stages, machine learning-based detection systems have shown promise in identifying DDoS attacks. In order to identify distributed denial of service (DDoS) attacks, this study detailed a machine learning-based strategy that makes use of a novel ensemble method. This approach employs a chain reaction using five supervised classifiers and six Meta classifiers. Separately, six Meta classifiers were given the results of five distinct unsupervised classifiers.

Hekmati, A., and Krishnamachari, B. [9] proposed to identify distributed denial of service (DDoS) attacks in Internet of Things (IoT) settings, the author presented a GCN-based approach in this article. These authors research demonstrated that GCNs were flexible enough to handle partial data while still handling the complicated relational dynamics of Internet of Things (IoT) devices, which were thought of as nodes in a graph. In order to maintain detection integrity even when networks were down, the author presented a strong detection framework that uses GCNs' inherent capabilities to infer partial or absent relational data.

Saiyed, M. F., and Al-Anbagi, I. [11] presented a new, lightweight Genetic Algorithm for DDoS Attack Detection (GADAD) system that can identify attacks with high or low volume. Datasets including several types of application and transport layer high- and low-volume DDoS attacks were created using a real-life testbed known as HL-IoT. The GADAD system used a number of tree-based ML models on the HL-IoT and ToN-IoT datasets, in addition to GAStats, a suite of adaptive and intelligent feature selection algorithms.

Setia, H., et al. [13] introduces in the setting of Vehicular Ad Hoc Networks (VANET Cloud), a novel method for detecting distributed denial of service (DDoS) attacks. This study was unique among its kind as it investigates the use of ML-based approaches to identify DDoS attacks in VANET Cloud settings. The thorough statistical study of network traffic characteristics, including both normative network conditions and adversarial attack scenarios, was a significant addition of this project.

Yuvaraja, T., et al. [15] proposed a method with a 99.1 percent accuracy rate and a lower number of false alarms than traditional approaches, the proposed solution was shown beneficial in the CICDDoS2019 dataset evaluation. Through enabling quick reactions and effective mitigation of low-rate attacks, these authors technique helped overcome the challenges faced by these constantly evolving threats.

In light of the interruptions brought on by the COVID-19 epidemic, this study seeks to address the issue of the growing danger of Distributed Denial-of-Service (DDoS) attacks. Distributed denial of service (DDoS) attacks is an attempt by an attacker to flood a server, service, or network with malicious traffic in an effort to interrupt its regular operation. Financial losses, lost productivity, brand harm, and impaired customer relationships are some of the serious implications that might result from this threat to the availability of corporate networks, applications, and services. It is crucial to create reliable Network Intrusion Detection Systems (NIDSs) that can foresee and avert DDoS attacks in order to lessen the impact of these dangers

III. RESEARCH METHOD

The methodology employed in this research involves evaluating supervised Machine Learning (ML) techniques to detect Distributed Denial-of-Service (DDoS) attacks using the CICDDoS2019 dataset. The dataset provides a comprehensive collection of network traffic data, allowing for the training and testing of ML algorithms. Five ML algorithms—AdaBoost, Naïve Bayes, MLP-ANN, Random Forest, and SVM—are assessed based on various evaluation metrics such as AUC, Accuracy, F-measure, precision, and recall. These metrics provide insights into the performance of each algorithm in accurately identifying and predicting DDoS attacks, ultimately leading to the determination of the most effective ML approach for combating this cyber threat. Figure 1 shows the machine learning approach for detecting DDoS attack.

A. Intrusion Detection System

Unusual actions that compromise the security of the system are known as intrusions. When certain criteria are satisfied, the administrator will get a warning from intrusion detection, which involves testing and analysis of network data. Two primary components make up the intrusion detection system. Forensic Analysis and Alert Administrator are two of them. The data mining process's programming element is forensic analysis.

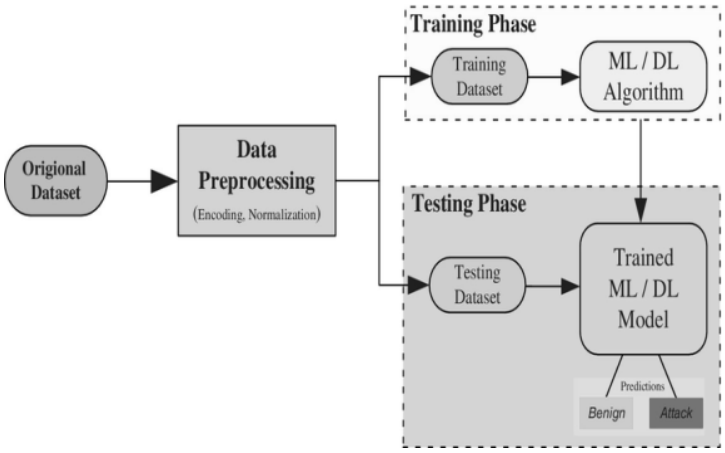

Figure 1: Machine Learning Approach for detecting DDoS Attack

The data mining process's programming element is forensic analysis. The hardware module known as "Alert Administrator" notifies the server administrator of any suspicious behavior detected by the intrusion detection system. Intruders' creation of anomalous network activity is known as intrusion. In this case, we employ data mining methods to discover the pattern of network traffic based on the flows of traffic that are currently there. It is possible to use that pattern to identify a new network that handles valid or malicious data.

A Distributed Denial of Service attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming it with a flood of internet traffic. Unlike traditional denial-of-service(DOS) attacks, which are launched from a single source. DDoS attacks employ multiple compromised computers and internet connected devices, often spread across different geographic locations, to amplify the volume of traffic and make it more difficult to mitigate. Figure 2 depicts the DDoS attack mechanism.

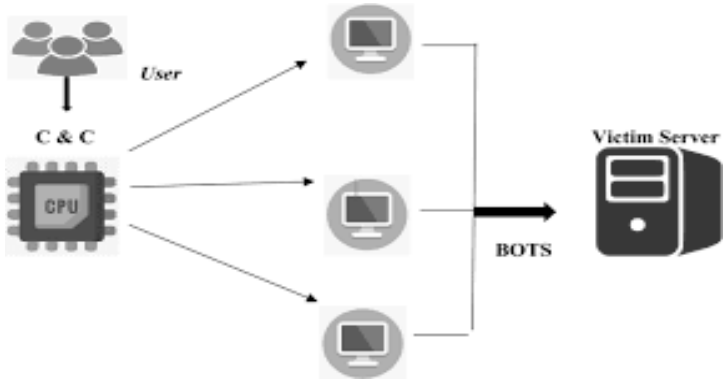

Figure 2: DDoS attack Mechanism

B. AdaBoost

The Adaptive Boosting algorithm, or AdaBoost for short, was developed by Yoav Freund and Robert Schapiro[7]. The AdaBoost method is based on a one-level decision tree model. In place of trees, AdaBoost is only wood land of stumps. To achieve its goals, AdaBoost prioritizes cases that are difficult to order categorize and downplays situations that are easily handled. Classification and regression issues are both addressed by the AdaBoost technique.

Thought behind AdaBoost:

1) Because stumps (a single node and two leaves) aren't very good at establishing precise classifications, they can only be described as poor classifiers or learners. The principle behind the AdaBoost algorithm is that a strong classifier may be created by combining several weak classifiers.
2) Not all stumps are equally executed or classified.
3) It is possible to commit consecutive stump by thinking about previous stump mistakes.

C. Naïve Bayes

The Naïve Bayes method is based on the Bayes theorem and is one of many probability-based classifiers. A vector of characteristics, each with an associated probability, makes up the probabilistic model. Assuming that qualities are not dependent on each other, the classifier estimates the class conditional probability[3]. Combining the probability-based model with the decision rule allows for the building of the classifier model.

$$p(C_k|x_1, \dots, x_n) = \frac{1}{Z}\, p\,(C_k) \prod_{i=1}^{n} p(x_i|C_k) \text{ ---------- (1)}$$

$$\hat{y} = arg \max_{k\in\{1,..,K\}} p\,(C_k) \prod_{i=1}^{n} p(x_i|C_k) \text{ ---------- (2)}$$

Because of the relationship between the class variable ('C') and the scaling element ('Z'), the conditional distribution is addressed by Equation (1). A Bayes classifier constructed with the probability model is addressed in Equation (2).

D. MLP-ANN

One kind of artificial neural network is the multilayer perception (MLP-ANN). The multi-layer perception (MLP) is a kind of feed-forward neural network. There are three levels to it, with a fourth layer that is concealed. A completely linked neural network is MLP. The three layers seen in Figure 3 are the input, hidden, and output layers. Figure 4 displays Multi Layer perceptron Model. MLP ANN are versatile and powerful models that can learn complex patterns from high dimensional data. However, they also have limitations, such as need for large amount of training data, the risk of over fitting, and the challenge of determining the optimal architecture for a given task. MLP-ANN is widely used in machine learning and pattern recognition tasks[3].

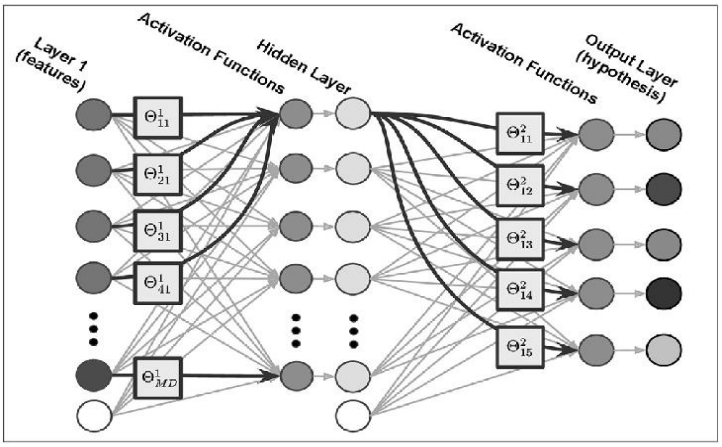

Figure 3: Multi Layer Perceptron Model

E. Support Vector Machine

An algorithm to use for pattern recognition, spam filtering, or intrusion detection, SVM is a popular choice. Classification, regression, and distribution estimation are three areas where SVM designs vary. The main goal of this algorithm is to assign each IP packet to one of the predefined classes. Because of this, decided to use c-support vector classification (C-SVC) on both training and test datasets [7].The training vectorsxi, where i range from -1 to l, and an indicator vector$y$, where yi falls between -1 and 1, are both members of Rl. Because we have organized three datasets with different feature counts, the measurement parameter n in the studies may take on values between three and five. Where -1 denotes the "Ordinary" for IP addresses in the victim pool and +1 denotes the "DDOS attack" for attacker pool, and use C-SVC to tackle the optimization challenge that goes along with it.

$$minimize_{\omega,b,\varepsilon} \quad \frac{1}{2}\omega^T\omega + C\sum_{i=1}^{l}\varepsilon_i \quad subject\ to \begin{matrix} y_i(\omega^T\emptyset(x_i) + b) \geq 1 - \varepsilon_i, \\ \varepsilon_i \geq 0, i = 1,2, \dots, l. \end{matrix} \text{ ------- (3)}$$

The regularization parameter, C, should be present but not dominating, and (xi) converts xi into a space with additional dimensions addressed in Equation [3].

IV. RESULTS AND DISCUSSION

A. Dataset Preparation

For this research work, CICDDOS2019 dataset was taken that was made available via the Kaggle repository [4]. Specifically, this dataset pertains to network traffic and includes 80 characteristics. Using the feature selection process, the 24 top features were chosen for this study. There are seven distinct category labels and two thousand records in it. There are several forms of distributed denial of service (DDOS) attacks, including benign, UDP, MSSQL, SYN-Flood, Port map, LDAP, and NETBIOS threats. Figure 4 presents architecture of DDoS detection using Machine Learning techniques.

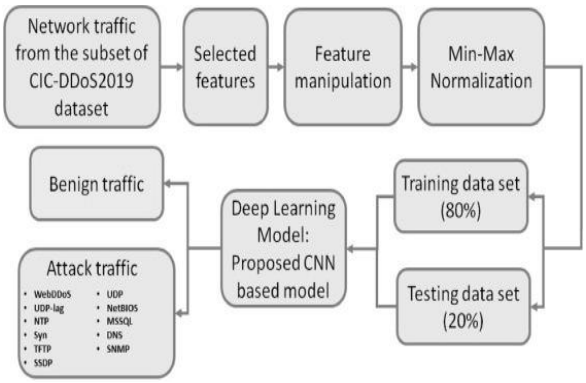

Figure 4: Machine Learning Techniques to detect a DDoS Attack

B. Improving performance of the classification algorithm

1) Hold-out: When it comes to cross-validation strategies, the Hold-out one is the simplest. There are two distinct groups of data: the training set and the testing set. When assessing the hold-out method, the data was partitioned so that 60% could be used for training and 40% for testing.

2) Cross-validation: To do cross-validation, also known as "k-fold cross-validation," the dataset is randomly divided into k groups. The remaining groups serve as training data, while one is used as a test data set. The training data set is used to train the model, and the test data set is used to score it. This process continues until all possible combinations of groups have been used as test data.

3) Bootstrap aggregating: The Bagging method is another name for Bootstrap aggregation. If the learning algorithm does anything wrong, the bagging algorithm is used to fix it. Figure 5 portrays various DDoS attack levels.

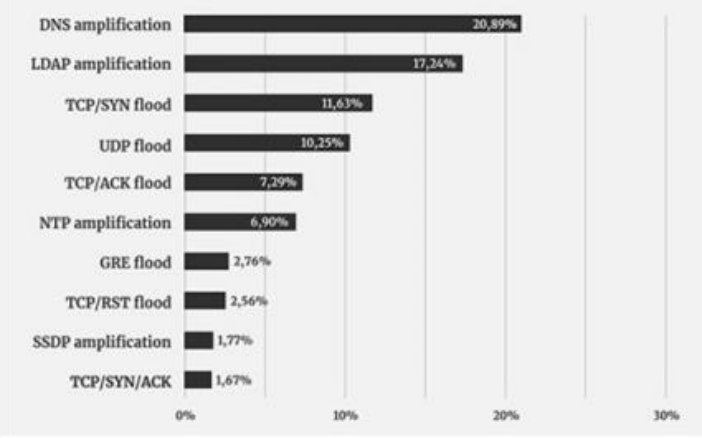

Figure 5: Various DDoS Attack levels

TABLE 1
THE EVALUATION RESULTS OF CLASSIFIERS USING HOLD-OUT VALIDATION

Model	AUC	CA	F1	Precision	Recall
Adaboost	0.992	0.987	0.987	0.987	0.987
Naïve Bayes	0.985	0.933	0.931	0.942	0.933
MLP_ANN	0.985	0.899	0.876	0.885	0.899
Random Forest	0.995	0.967	0.967	0.969	0.967
SVM	0.989	0.850	0.826	0.807	0.850

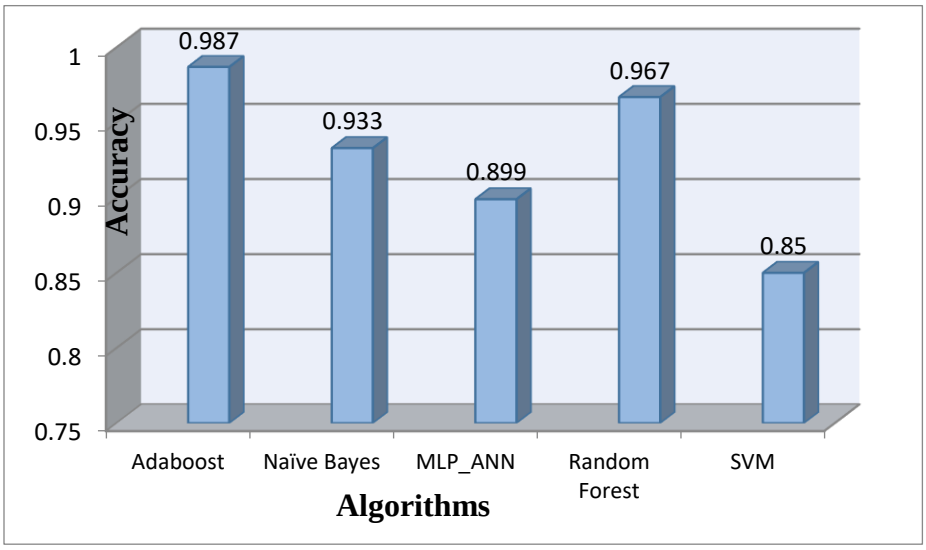

Figure 6: Comparison of Accuracy level for the different classifying algorithms with the Hold-out method

With this validation, Adaboost Algorithm achieves a remarkable 98.7 percent accuracy rate. According to Naïve Bayes, MLP-ANN, Random forest, and SVM, the accuracy of the other classifiers was 93.3%, 89.9%, 96.7%, and 85% respectively. If the Accuracy measure is inadequate, then a judgment may be impossible to make. Since the datasets used for training and testing could not always be relevant. Hence, other from Precision and Recall, think about additional performance metrics to find better categorization algorithms. Classifiers AUC, F1, Precision, and Recall scores are shown in Figure 6 and Table 1. The Adaboost algorithm produces the highest values for AUC, F1, Precision, and Recall in these performance measure studies, with respective values of 0.992, 0.987, 0.987, and 0.987.

TABLE 2
THE EVALUATION RESULTS OF CLASSIFIER USING CROSS-VALIDATION

Model	AUC	CA	F1	Precision	Recall
Adaboost	0.996	**0.993**	0.993	0.993	0.993
Naïve Bayes	0.988	0.934	0.933	0.941	0.934
MLP-ANN	0.992	0.918	0.898	0.934	0.918
Random Forest	0.996	0.978	0.977	0.978	0.978
SVM	0.992	0.858	0.833	0.816	0.858

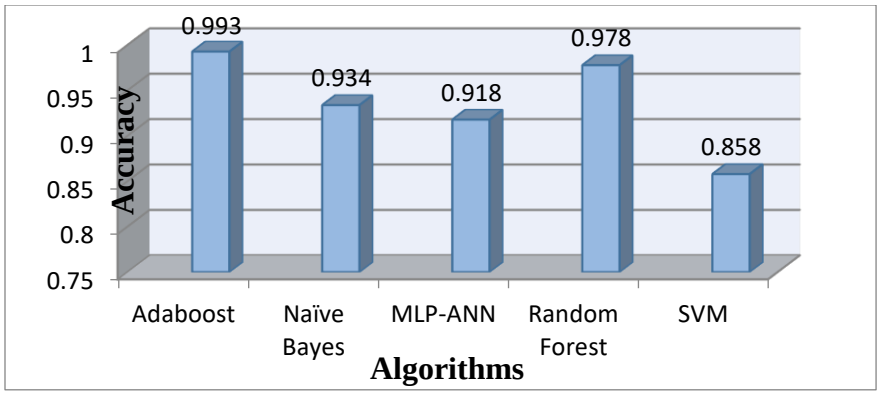

Figure 7: Comparison of Accuracy level for different classification algorithms with Cross validation method

An impressive 98.7 percent accuracy is achieved by Adaboost Algorithm in the Hold-out validation. Yet, that was insufficient. The Cross Validation approach was used to enhance the classifiers' performance. Once again, Adaboost Algorithm achieves a high accuracy of 99.3% in this validation. The accuracy of the other classifiers was as follows: 93.4% for Naïve Bayes, 91.8% for MLP-ANN, 97.8% for Random forest, and 85.8% for SVM. If the Accuracy measure is inadequate, then a judgment may be impossible to make. Since the datasets used for training and testing could not always be relevant. Hence, other from Precision and Recall, think about additional performance metrics to find better categorization algorithms. You can see the classifiers' AUC, F1, precision, and recall values in Table 2 and Figure 7. The Adaboost method only attains the superior AUC, F1, Precision, and Recall values of 0.996, 0.993, and 0.993, respectively, for these performance metric assessments.

TABLE 3
THE EVALUATION RESULTS OF CLASSIFIERS USING BOOTSTRAP VALIDATION

Model	AUC	CA	F1	Precision	Recall
Adaboost	0.997	**0.99**	0.99	0.996	0.996
Naïve Bayes	0.991	**0.95**	0.95	0.957	0.957
MLP-ANN	0.993	**0.93**	0.90	0.882	0.930
Random	0.998	**0.97**	0.97	0.971	0.970
SVM	0.991	**0.86**	0.83	0.814	0.860

The Adaboost Algorithms achieve a remarkable 98.7 percent and 99.3 percent accuracy in the Hold-out and cross-validation approaches, respectively. The Ensemble (Bootstrap) approach was used to improve the classifiers' performance. Once again, Adaboost Algorithm achieves a high accuracy of 99.6 percent in this validation. According

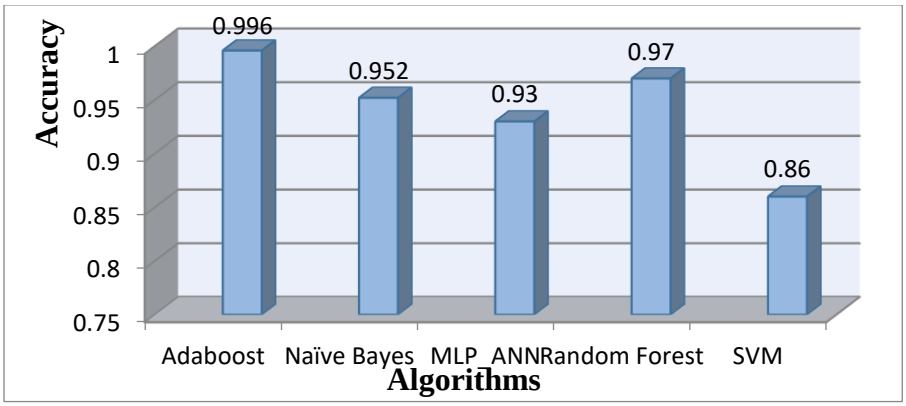

Figure 8: Comparison of Accuracy level for different classification algorithms with a Bootstrap method

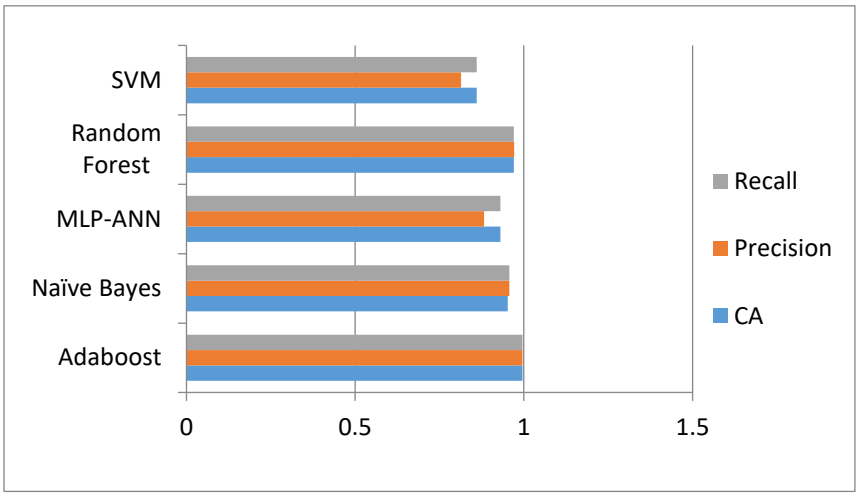

Figure 9: Comparison of Accuracy, Precision, and Recall for different classification algorithms with the Boot strap method.

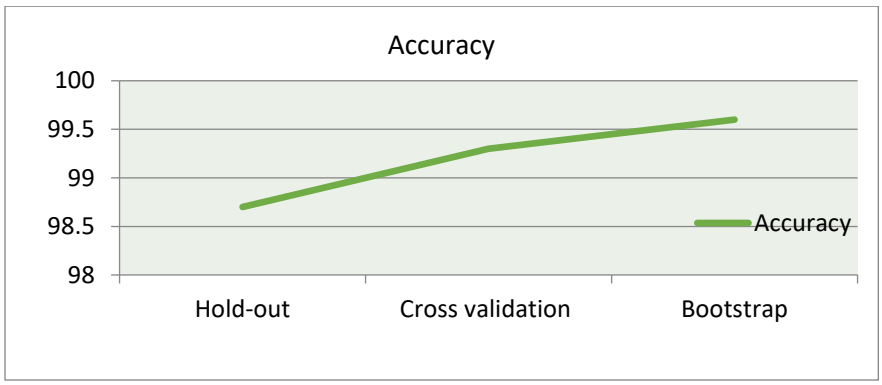

Figure 11: Improvement in Accuracy with the Bootstrap method

to the other classifiers, Naïve Bayes, MLP-ANN, Random forest, and SVM had accuracy rates of 95.2%, 93%, 97%, and 86% respectively. When looking for improved classification algorithms, it's important to include additional performance metrics like Precision and Recall. Classifiers' AUC, F1, Precision, and Recall scores are shown in Figure 8 and Table 3. It is worth noting that the Adaboost method only attained the highest AUC, F1, Precision, and Recall values of 0.997, 0.996, and 0.996 respectively, in these performance measure studies.

The data associated with the distribution of classifier executions may be seen. Using this number, the Adaboost algorithm yields results that are better than one hundred. When it comes to placement, the random woodland comes in second. The results show that the AdaBoost algorithm outperforms the competition when it comes to classification. The AdaBoost method will get excellent results in all three metrics: recall, precision, and classification accuracy.

V. CONCLUSION

The CICDDoS2019 dataset was subjected to a DDoS attack prediction using the "Enhancing Cyber security against DDoS Attacks Evaluating Supervised Machine Learning Techniques" research proposal. When it comes to data mining, classification is where network security really shines. The DDoS dataset employs AdaBoost, Naïve Bayes, MLP-ANN, Random forest, and SVM as its classification methods. This research provides the test results of these algorithms together with their performance rating. The Ensemble (Bootstrap) approach was used to improve the classifiers' performance. When compared to Cross-Validation and Hold-out validation, the AdaBoost algorithm's accuracy level will grow with Bootstrap. An impressive 99.6 percent accuracy was achieved by combining the Boosting and Bagging ensemble techniques. Consequently, the intrusion detection system's DDoS attack prediction results will be improved by this technique.

REFERENCES

[1] Abid, Y. A., Wu, J., Xu, G., Fu, S., & Waqas, M. (2024). Multi-Level Deep Neural Network for Distributed Denial-of-Service Attack Detection and Classification in Software-Defined Networking Supported Internet of Things Networks. *IEEE Internet of Things Journal*.

[2] Alfatemi, A., Rahouti, M., Amin, R., ALJamal, S., Xiong, K., & Xin, Y. (2024). Advancing DDoS Attack Detection: A Synergistic Approach Using Deep Residual Neural Networks and Synthetic Oversampling. arXiv preprint arXiv:2401.03116.

[3] Ali, M., Shahroz, M., Mushtaq, M. F., Alfarhood, S., Safran, M., & Ashraf, I. (2024). Hybrid Machine Learning Model for Efficient Botnet Attack Detection in IoT Environment. IEEE Access.

[4] Aslam, N., Srivastava, S., & Gore, M. M. (2024). A comprehensive analysis of machine learning-and deep learning-based solutions for DDoS attack detection in SDN. Arabian Journal for Science and Engineering, 49(3), 3533-3573.

[5] Benmohamed, E., Thaljaoui, A., Elkhediri, S., Aladhadh, S., & Alohali, M. (2024). E-SDNN: encoder-stacked deep neural networks for DDOS attack detection. Neural Computing and Applications, 1-13.

[6] Bukhowah, R., Aljughaiman, A., & Rahman, M. H. (2024). Detection of DoS Attacks for IoT in Information-Centric Networks Using Machine Learning: Opportunities, Challenges, and Future Research Directions. Electronics, 13(6), 1031.

[7] Das, S., Ashrafuzzaman, M., Sheldon, F. T., & Shiva, S. (2024). Ensembling Supervised and Unsupervised Machine Learning Algorithms for Detecting Distributed Denial of Service Attacks. Algorithms, 17(3), 99.

[8] Gadallah, W. G., Ibrahim, H. M., & Omar, N. M. (2024). A deep learning technique to detect distributed denial of service attacks in software-defined networks. Computers & Security, 137, 103588.

[9] Hekmati, A., & Krishnamachari, B. (2024). Graph-Based DDoS Attack Detection in IoT Systems with Lossy Network. arXiv preprint arXiv:2403.09118.

[10] Naqvi, S. S. A., Li, Y., & Uzair, M. (2024). DDoS attack detection in smart grid network using reconstructive machine learning models. PeerJ Computer Science, 10, e1784.

[11] Saiyed, M. F., & Al-Anbagi, I. (2024). A Genetic Algorithm-and t-Test-Based System for DDoS Attack Detection in IoT Networks. IEEE Access, 12, 25623-25641.

[12] Salama, A. M., Mohamed, M. A., & AbdElhalim, E. (2024). Enhancing Network Security in IoT Applications through DDoS Attack Detection Using ML. Mansoura Engineering Journal, 49(3), 10.

[13] Setia, H., Chhabra, A., Singh, S. K., Kumar, S., Sharma, S., Arya, V., ... & Wu, J. (2024). Securing the road ahead: Machine learning-driven DDoS attack detection in VANET cloud environments. Cyber Security and Applications, 2, 100037.

[14] Shaikh, J., Butt, Y. A., & Naqvi, H. F. (2024). Effective Intrusion Detection System Using Deep Learning for DDoS Attacks. The Asian Bulletin of Big Data Management, 4(1).

[15] Yuvaraja, T., Rajan Salem Jeyaseelan, W. G., Ashokkumar, S. R., & Premkumar, M. (2024). Detecting and Mitigating Low-Rate DoS and DDoS Attacks: Multimodal Fusion of Time-Frequency Analysis and Deep Learning model. Tehnički vjesnik, 31(2), 495-501.