International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
Volume 34 العدد
Part 2 المجلد
July 2024 يوليو
المجلة الدولية للعلوم والتقنية
ISTJ
تم استلام الورقة بتاريخ: 30/ 6/2024م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

# Training Machine Learning Algorithms to Detect Distributed Denial of Service Attacks

www.doi.org/10.62341/msai2687

**Mohamed Sasi Manita[1], Ahmed Ibrahim Suleiman[2].**
[1]College of Computer Technology, Zawia, Libya
[2]University of Zawia, Zawia, Libya

Email Address: m.manita@zu.edu.ly[1], a.suleiman@zu.edu.ly[2].

## Abstract

Cyber-attacks are becoming more and more sophisticated, posing a serious threat to our technologically dependent society. Such an attack is the Distributed Denial of Service (DDoS) attack, which is becoming a serious threat to businesses that have integrated their technology with public networks since they enable numerous attackers to obtain data or provide services to major corporations or nations. When a company's servers are overloaded with fraudulent requests while legitimate users' requests are denied, Distributed Denial of Service (DDoS) attacks disrupt Web service availability for an arbitrary amount of time. This results in financial losses since services are rendered unavailable. This paper provides a comparative analysis of popular ML algorithms, including Logistic Regression, Random Forest, and Neural Network, in terms of their effectiveness in DDoS attack detection. Along with a comprehensive evaluation of its performance. The study incorporates numerical data analysis and relevant diagrams to offer insights into the comparative efficacy of different ML techniques for DDoS attack detection.

**Keywords**: DDoS attacks, machine learning, random forest, Logistic Regression, Neural Network.

International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
العدد Volume 34
المجلد Part 2
يوليو July 2024
المجلة الدولية للعلوم والتقنية
ISTJ
تم استلام الورقة بتاريخ: 30/ 6/2024م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

# تدريب خوارزميات التعلم الآلي للكشف عن هجمات رفض الخدمة الموزعة

**محمد ساسي مانيطة[1]و أحمد ابراهيم سليمان[2]**
كلية تقنية الحاسوب بالزاوية[1]
جامعة الزاوية[2]

**الملخص**

في وقتنا الحالي أصبحت الهجمات السيبرانية (الهجمات الضارة على الانترنت) أكثر تعقيدًا مما يشكل تهديدًا خطيرًا على العديد من المؤسسات والأفراد في مجتمعنا والتي تعتمد في أعمالها بشكل أساسي على تقديم خدماتها عبر الانترنت. من أمثلة هذه الهجمات هو هجوم رفض الخدمة الموزعة اختصارا (DDoS) حيث يعتبر هذا النوع من الهجمات تهديدًا خطيرًا لهذه الشركات والمؤسسات .وذلك لتمكن الاشخاص الذين يوجهوا هذا النوع من الهجمات من الوصول الي مراكز بيانات هذه المؤسسات واختراق أنظمتها وتعطيلها. فعند تعرض خوادم هذه الشركات الى هجمات متمثلة بتوجيه كمية كبيرة من طلبات الخدمة الاحتيالية الامر الذي يجعلها غير قادرة على تقديم الخدمة للمستخدمين الشرعيين، كما أن من أضرارهذا النوع الهجمات والمتعارف عليه اصطلاحا (هجمات رفض الخدمة الموزعة (DDoS) ) أنه يسبب في عدم توفر خدمة الويب (عدم القدرة على الوصول لمركز الخدمة على الانترنت) لفترة زمنية غير متوقعة. مما يسبب في انهيار سمعة هذه الشركات وايضا خسائر مالية كبيرة لها. مما سبق ذكره وللمساعدة في التقليل من خطر هذا النوع من الهجمات تقدم هذه الورقة تحليلاً مقارنًا لخوارزمياتتعلم الآلة(ML)الشائعة، بما في ذلك (*Logistic Regression*) و(*Random Forest*) و(*Neural Network*)،حيث سيتم استخدام بيانات حقيقية لأحد الهجمات وتعليمها لهذه الخوارزميات ليتم تصنيفها ومعرفة الطلبات الحقيقية من الهجمات وبالتالي استخدامها في المستقبل لاكتشاف هذه الهجمات في وقت مبكرا ليتم التعامل معها. أخيرا تتضمن هذه الدراسة تحليلا للبيانات الرقمية والرسوم البيانية ذات الصلة لتقديم رؤى حول فعالية تقنيات تعلم الآلة المختلفة للكشف عن هجمات DDoS.

تم استلام الورقة بتاريخ: 30/ 6/2024م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

## Introduction

Cyberattacks are the newest type of attacks that have a significant impact on the planet. Cyberattacks are any illegal online actions intended to breach a national cyber asset's security policy and cause harm, interruption, or disruption of the asset's services or information access(Li and Liu 2021). Denial of Service (DoS) attack one the attacks that involves sending tens of thousands or even hundreds ofthousands of requests per second to a server from various IP addresses or locations. One type of DoS attack is a subclass known as Distributed Denial of Service (DDoS) attacks. DDoS attacks, also referred to as botnet attacks, use a large number of networked online devices to attack certain websites by creating fake traffic. DDoS attacks, in contrast to other forms of cyberattacks, do not try to breach your boundary. Rather, the intention is to obstruct authorized users from reaching the website and its servers(2024). DDoS can also be used as a justification for a number of malevolent actions, turning off security measures, and breaking through the target's boundary. Examples of such attacks include SYN Flood and Smurf attacks, which are attacks that require a lot of bandwidth, memory usage, and target processing that typically, cannot be handled by a server, leading to a service collapse.

In addition, DDoS attack is considered as one of the major types of cyber-attacks that can make an individual and Institutions to face serious issues. As an example: In November 2021, Microsoft mitigated a DDoS attack with a throughput of 3.47 Tbps and a packet rate of 340 million packets per second (pps), targeting an Azure customer in Asia which is believed to be the largest DDoS attack ever recorded(Nicholson 2022).Recently, And According to the IT Department of Central Bank Of Libya The “Foreign Currency Reservation Platform for Individuals” (FCMS.CBL.GOV.LY) was subjected to a Distributed Denial of Service (DDoS) cyber-attack on Monday (April 1, 2024), which affected access to the system and caused the platform to stop providing its services permanently for a period of an entire day until the IT team was able to address this attack. What increases the fear of these attacks is that they are

تم استلام الورقة بتاريخ: 30/ 6/2024م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

constantly increasing according to research from NETSCOUT's ATLAS Security Engineering & Response Team (ASERT), threat actors launched approximately 2.9 million DDoS attacks in the first quarter of 2021, a 31% increase from the same time in 2020 (Hildebrand 2021). As per this source, there were 6,019,888 global DDoS attacks in 1st half of 2022 and globally, DDoS attacks are predicted to number over 15.4 million in 2023 – almost double that of 2018 (Sloot 2023).For this reason, new strategies and methods must be developed and prototypes are required to prevent service outages and financial losses as well as to identify fraudulent attacks on concurrent requests in an effective and efficient manner. In order to tackle this issue and devise more effective mitigation tactics, scientists have created machine learning algorithms that more accuratelyclassify DDoS attacks, these algorithms can be trained to discriminate between malicious and benign traffic, which are two subtypes of DDoS attacks, by examining network traffic data.

Data can be automatically categorized into specified classes or categories using a class of machine learning techniques called classification algorithmson labeled datasets, where each data point is given a target class label, these models are trainedto be able to distinguish and classify this data into two parts the actual data and thesuspicious data. After it has been trained, these algorithms will be verified to be ready to use to test the incoming unknown data in real time, which help to anticipate malicious attacks.
In this paper, an empirical study of DDoS attacks classification by Machine learning: Random Forest, Logistic Regression and Neural Network. A big dataset (66238 documents) used to study, compare and evaluate these models. Then selecting the best model to use for classifying real-world DDoS attacks.

The structure of this paper as follows: Section 2 presents related works about DDoS attacks classification and Machine learning. The experiment presented in Section 3. Model Comparison and Discussion of these experiments are presented in Section 4. Finally, conclusions and future work take place in Section 5.

تم استلام الورقة بتاريخ: 30/ 6/2024م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

## Related Work

To anticipate DDoS attacks, machine-learning models can be used, for example, to train a neural network to identify patterns in network traffic. After that, the model can be utilized to spot anomalous traffic patterns that might point to a DDoS attack. The model's ability to identify patterns and spot abnormalities improves with the amount of data available to train it.

Machine learning algorithms can assist in early DDoS attack detection and help stop them from causing major harm by real-time log data analysis. In this section of this paper, we will briefly explain some of the related model and the closest rival to our proposed study.

(Zargar, Joshi, and Tipper 2013) Provided a thorough examination of defense strategies against denial-of-service (DDoS) assaults. The article covers a number of methods, such as traffic engineering, packet filtering, rate limitation, and trace-back. It assesses how well various techniques mitigate DDoS attacks and offers information on their advantages and disadvantages. The research also emphasizes how crucialit is to use machine-learning techniques in order to create defense mechanisms thatare more resilient and flexible in the face of changing DDoS attacks.

(Abu Rajab et al. 2006) the study analyzes the botnet phenomenon—, which is often, linked to DDoS attacks—using a multifaceted methodology. The study looks into the traits and actions of botnets, as well as their propagation strategies, command and control systems, and communication protocols. The study clarifies the scope and effects of botnet-driven DDoS attacks through the analysis of real-world data, highlighting the necessity for advanced detection and mitigation techniques that make use of machine learning algorithms.

(Karatas, Demir, and Sahingoz 2020) has presented a machine learning method for the classification of attacks. Using several machine-learning algorithms, he discovered that, in comparison to other studies, the KNN model performs the best for classification.

In (Martins et al. 2020) also machine learning techniques for intrusion detection were suggested by Nuno Martins et al. They used

تم استلام الورقة بتاريخ: 30/ 6/2024م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

the KDD dataset, which is available on the UCI repository. They tried with different supervised models to find the best performing classification algorithm. Using several categorization algorithms, comparison research was proposed in this work, and the results showed promise.

(D'hooge et al. 2019) proposed a systematic review for malware detection using machine learning models. They compared different malware datasets from online resources as well as approaches for the dataset, they discovered that machine learning-supervised models are highly efficient in detecting malware, allowing for faster and better decision-making.

(Aamir et al. 2021)proposed AI calculations were developed and evaluated on the most recent distributed benchmark dataset (CICIDS2017) to determine the ideal performance calculations using data that contains the latest port checks and DDoS attack routes. The permutation findings demonstrate that all combinations of support vector machines (SVM) and isolation checks can yield excellent test accuracy, for instance, above 90%. Nine calculations from a series of AI tests obtained the most notable score (highest), according to the abstract scoring standards stated in this article, since they provided more than 85% representation (test) accuracy in 22 absolute calculations.

The k-fold cross approval, the area under the curve (AUC) check of the receiver operating characteristic (ROC) curve, and the use of principal component analysis (PCA) for size reduction in preparation for AI execution model were also noted in this related investigation. It was discovered that numerous checks on various AI computations of the CICIDS2017 datasets were insufficient for port checks and DDoS attacks when considering such late attacks.

A scientific classification method was put out by (Ahmad et al. 2021) and is predicated on the well-known ML and DL processes that are a part of the network-based intrusion detection system (NIDS) design architecture. The quality and certain constraints of the suggested arrangements were evaluated, and a thorough analysis of the new NIDS-based clauses was carried out. By then, the current trends and advancements of NIDS based on ML and DL are

تم استلام الورقة بتاريخ: 30/ 6/2024م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

provided, together with information on the suggested technology, assessment measurement, and dataset selection. In this study, they exploit the shortcomings of the suggested technology by posing several exploration problems and offering recommendations.

(Cheng et al. 2021)suggested a novel in-depth binding review (OFDPI) approach with Open Flow function in SDN using AI computing. OFDPI supports a thorough bundling inspection of the two decoded packages. The process for managing traffic and scrambled traffic, respectively, involves setting up two dual classifiers. Furthermore, suspect packages can be tested by OFDPI through bundling windows that rely on immediate expectations. they assess OFDPI's demonstrations on the Ryu SDN regulator and Mininet stage using real-world datasets. For both encoding and decoding communications, OFDPI achieves a pretty good recognition accuracy when there is enough overhead.

Table 1 summarizes the previous papers that used machine-learning algorithms to detect distributed denial of service attacks.

**TABLE 1. SUMMARIZES THE PREVIOUS PAPERS THAT USED MACHINE LEARNING ALGORITHMS**

| Work | Main findings | Limitations |
|---|---|---|
| S. Zargar et al. [6] | -DDoS attacks are often launched using botnets of compromised computers.<br>-Comprehensive DDoS defense mechanisms are needed that can respond before, during, and after an attack. | -The lack of widespread deployment of DDoS defense mechanisms and the lack of collaboration among distributed defense mechanisms.<br>-The challenges in accurately detecting DDoS attacks at the intermediate networks or sources due to lack of evidence. |
| M. Abu Rajab et al. [7] | - Botnets represent a major contributor to unwanted internet traffic, accounting for 27% of all malicious connection attempts observed.<br>-Evidence of botnet infections was found in 11% | - The full scope and specifics of botnet behavior and activities are still not well understood, despite the increase in botnet activity.<br>- The data collection infrastructure, while multifaceted, still faces |

تم استلام الورقة بتاريخ: 30/ 6/2024م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

| | | |
|---|---|---|
| | of 800,000 DNS domains examined, indicating a high diversity among botnet victims. | uncertainty in fully capturing the botnet phenomenon. |
| G. Karatas et al. [8] | - The use of sampled data provided the best accuracy rates for minority attack classes, with an average 72.35% increase in accuracy compared to the original dataset.<br>- The proposed system using the Random Forest algorithm and sampled data achieved a 99.34% accuracy rate, which is a considerable improvement over a recent comparable study. | - The original dataset had imbalanced data, which was addressed by generating synthetic data for the minority classes |
| N. Martins et al. [9] | - Adversarial attacks were proven effective against malware and intrusion detection classifiers, with a wide variety of attack techniques tested.<br>- Adversarial defense techniques are still not thoroughly explored, with few studies testing their application. | - Further testing of a wider variety of adversarial defense techniques is needed, as only a few were explored in the studies reviewed.<br>- The main dataset used for intrusion detection, NSL-KDD, is outdated, and newer and more standardized datasets, potentially from IoT environments, should be used for future research. |
| L. D'hooge et al [10] | - The tree-based methods were more robust to feature reduction for certain attack classes with clear network footprints, like DoS and DDoS, but other attack classes like infiltration and web attacks were more heavily impacted by feature reduction. | - The authors plan to further test the generalization of the models, indicating that this was not fully addressed in the current study.<br>- The imbalance in the CICIDS2017 dataset, with far fewer positive samples for some attack classes, may have limited the performance of some classifiers. |
| M. Aamir et al. [11] | - All variants of discriminant analysis and Support Vector Machine (SVM) provide | - The analysis is limited to the CICIDS2017 dataset, which |

تم استلام الورقة بتاريخ: 30/ 6/2024م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

| | | |
|---|---|---|
| | good testing accuracy of over 90% in classifying port scanning and DDoS attacks.<br>- The Fine Gaussian variant of SVM achieved the best performance with 99% testing and training accuracy.<br>- Tree-based models, KNN, and most ensemble classifiers exhibited relatively poor performance in the range of 49-69% testing accuracy. | may not generalize to other datasets or attack types.<br>- The authors suggest considering more machine learning models, including neural networks, and performing more detailed feature engineering in future work.<br>- The authors also suggest analyzing additional dimensionality reduction techniques to improve performance. |
| Z. Ahmad et al. [12] | - The paper provides a broad overview of recent trends and advancements in ML- and DL-based NIDS solutions.<br>- The paper reviews recent journal articles on ML-and DL-based NIDS published in the last 3 years and discusses their proposed methodologies, strengths, weaknesses, evaluation metrics, and datasets used.<br>- The paper highlights the recent trends in the use of DL-based algorithms for NIDS, with AE and DNN being the most frequently used DL techniques. | - Inefficiency in detecting zero-day attacks and reducing false alarm rates.<br>- Challenges in detecting malicious intrusions efficiently due to the massive increase in network traffic.<br>- The research on using DL methods for NIDS is still in its early stage, with a lot of room for exploration. |
| Q. Cheng et al. [13] | - OFDPI achieves high detection accuracy for both unencrypted (98.86%) and encrypted (99.15%) packets using machine learning classifiers.<br>- OFDPI introduces an adaptive packet sampling mechanism based on linear prediction to balance detection accuracy and | - The dataset used has an imbalance between malicious and benign samples, and the paper suggests using techniques like focal loss and stratification to address this. It also collected an additional real-world dataset to validate the model and avoid overfitting. |

تم استلام الورقة بتاريخ: 30/ 6/2024م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

| | | |
|---|---|---|
| | performance overhead on the SDN controller.<br>- OFDPI extracts notable features from encrypted traffic to identify malicious packets without decrypting the traffic, preserving user privacy. | -The overhead on the SDN controller in OFDPI is higher than in prior work that used service function chaining to offload traffic to DPI modules, though the prior work did not report the detection accuracy of the DPI modules. |

## Experiment

This section presents an empirical study of DDoS attacks classification by Machine learning: Random Forest, Logistic Regression and Neural Network. A big data corpse (66238 documents) used to study, compare and evaluate these models. Once preprocess and data analysis are conducted, three machine learning algorithms will be used. The results are established on the basis of the statistical formulas such as precision, recall, F-measure, Accuracy, Confusion matrix. then will comparing the performance of the three models using the ROC curve and select the best model to use for classifying real-world DDoS attacks. The architecture and data flow diagram of the proposedsystem is shownin figure 1

## Dataset

The dataset was collected by (Hu et al. 2014) and was produced using network activity monitoring for a specified period of time. The capturing period began on Monday, July 3rd at 9:00 and continued nonstop for five days, concluding on Friday, July 7th at 17:00. Subsequent attackswere carried out throughout this time. Table 2 illustrates that Monday is a typical day with only light traffic. The types of attacks that are being carried out are Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet, and DDoS. They are carried out on Tuesday, Wednesday, Thursday, and Friday in the morning and afternoon, respectively.

تم استلام الورقة بتاريخ: 30/ 2024/6م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

**TABLE 2. DAILY LABEL OF DATASET**

| Days | Labels |
|---|---|
| Monday | Benign |
| Tuesday | BForce,SFTP and SSH |
| Wednesday | DoS and Hearbleed Attacks slowloris, Slowhttptest, Hulk and GoldenEye |
| Thursday | Web and Infiltration Attacks Web BForce, XSS and Sql Inject. Infiltration Dropbox Download and Cool disk |
| Friday | DDoS LOIT, Botnet ARES, PortScans (sS,sT,sF,sX,sN,sP,sV,sU,sO,sA,sW,sR, sL and B) |

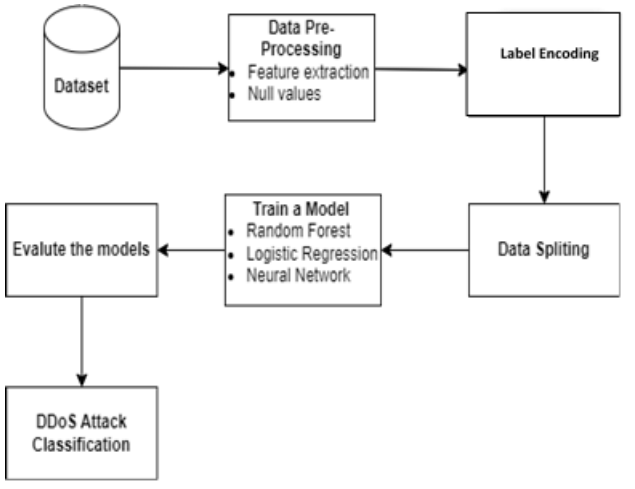



Figure 1. Data flow Chart for the Proposed System

## Pre-processing

This phase of the data analysis process is both important and time-consuming. In this case, the data will be sifted to eliminate irrelevant information and converted into high-quality data. Statistical techniques will be employed in this step to substitute values that are not relevant to the experimental analysis and to clean up the data.For the first phase of the examination, this is a requirement for all data analyses. After that, the data can be transformed into a reliable

تم استلام الورقة بتاريخ: 30/ 6/2024م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

format. Thus, the following tasks are being carried out in this experiment as text pre-processing of the dataset under study:

- Remove the spaces before the column names.
- Identifying the columns with null values. The figure 2 shows the columns with Null Values.
- Replacing the null values with the N character
- Remove of the null values from a dataset. The figure 3 shows the Total number of Missing values in each feature.
-

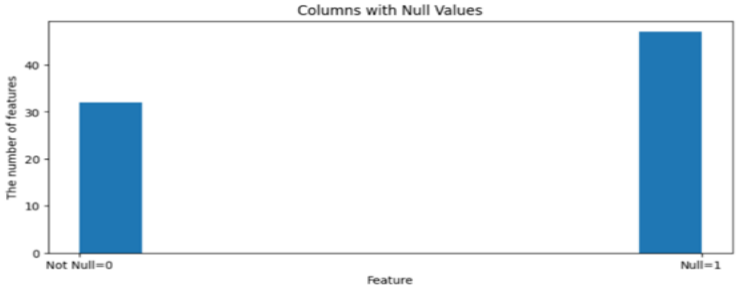



Figure 2. Columns with Null Values

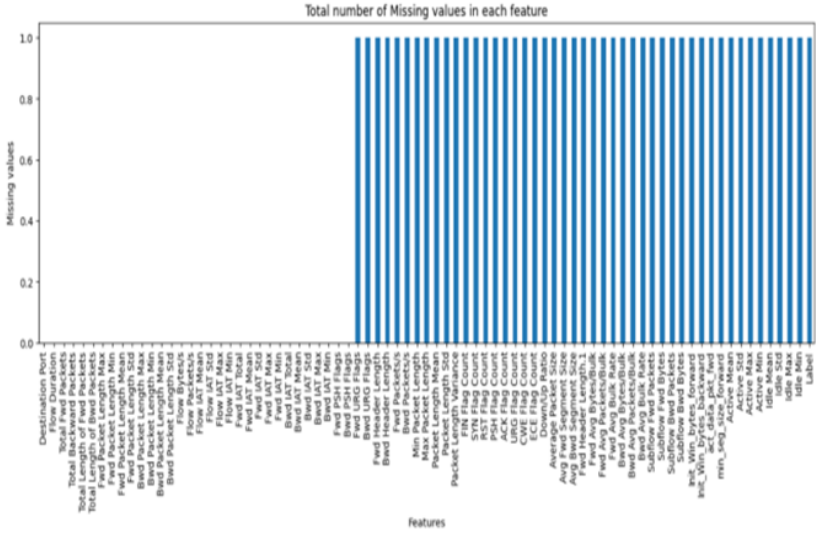



Figure 3. Total number of Missing values in each feature

تم استلام الورقة بتاريخ: 30/ 6/2024م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

## Label Encoding

Computers cannot process letter data because their understanding is sporadic. Additionally, in this instance, our computer algorithms are unable to comprehend our information in letter form. In order for our suggested model to comprehend this data, it is crucial that it be converted into digital format. We can change the tag encoder into the desired form because it is a machine learning process. The whole presentation of our dataset, which has been transformed to numerical form, is shown in the figure 4.

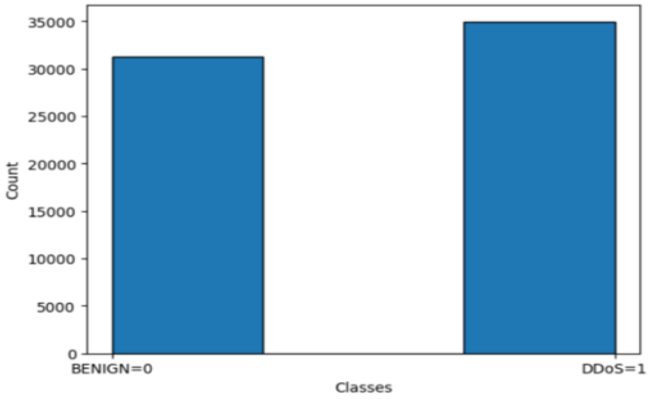



Figure 4. Label Encoding

## Data Splitting

The dataset is separated into two classes: independent (i) and dependent (ii). Another name for the dependent class is the target class. Classes that are independent of one another are known as independent classes. In order to accommodate our suggested model, the dataset has been divided into 70% for training and 30 % for testing. The sk-learn model selection library can be used to separate data to train and test the dataset for assessment.

## Performance metrics

After the method has been selected and built, the classifier's performance needs to be evaluated to check if the classification model can correctly categorize unseen data into the relevant classes. Many methods have been used to evaluate the performance of the

تم استلام الورقة بتاريخ: 30/ 6/2024م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

classification algorithm, such as the definitions of f1-score, accuracy, precision, and recall given below:

$$Recall = \frac{TP}{TP+FN} \quad (1)$$

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

$$F1 = \frac{2 * (\text{precision} * \text{recall})}{(\text{precision} + \text{recall})} \quad (4)$$

Where True Positive, True Negative, False Positive, and False Negative are denoted by the letters TP, TN, FP, and FN, respectively. The above metrics are combined with the micro-average measures in the multilabel categorization.

**Supervised Models**

Artificial intelligence (AI) is the application of logic and reasoning in computers to allow structures to understand and evolve from reality without the need for explicit customization. The main goal of artificial intelligence is to create computer systems that are better at gathering data and using it to learn new things. In order to describe and anticipate all of the information indicators of the task, supervision is a series of calculations that makes use of past experiences, knowledge, and data (Zakarya 2013). The suggested model and the outcomes in the next section.

1. **Random Forest Classifier**

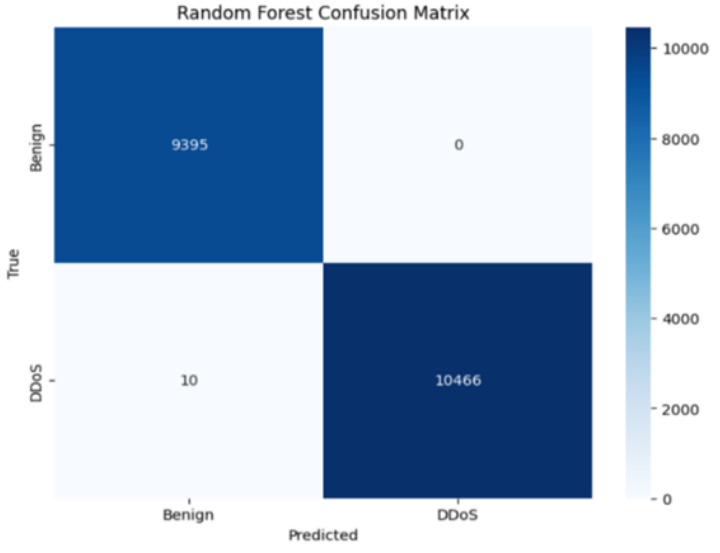
A decision tree combined with a random forest algorithm. As compared to other classifiers, it is incredibly quick. Following feature scaling, the machine learning classification model comes next. In our proposed investigation, we used a random forest classification technique. The proposed model uses random forest, one of the most popular and efficient machine learning classification techniques, to make multiple selections.

- **Random Forest Confusion Matrix**

The AI group execution blueprint makes use of this technique. We may better understand the sorts of errors caused by the representation model and its correctness by calculating the

تم استلام الورقة بتاريخ: 30/ 2024/6م وتم نشرها على الموقع بتاريخ: 30/ 2024/7م

confusion matrix. In the same way as true and prophetic markings are arranged, it is utilized to determine the representation's accuracy. They present the classifier and its representation graphically. Our model's confusion matrix is displayed in Figure 5.




Figur 5. Random Forest Confusion Matrix

For a given algorithm, the confusion matrix indicates the total number of real and predicted labels. Comparably, the absolute quantity of existing marks and the anticipated names for organization are dealt with by the disordered dot matrix. True positives, true negatives, false positives, and false negatives are all mixed together in these real and expected names. We will assess the precision of our model configurations and expectations using these attributes.

- The genuine negative is resolved by TN, which is all the benefits of accurately anticipating a negative instance.
- False positives are eliminated by FP, which counts the total number of positive deviations from the baseline.

تم استلام الورقة بتاريخ: 30/ 2024/6م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

- False negatives are resolved by FN, which states that a negative result is the total of all deviations from the fundamental expectations.
- True-Positive is solved by TP, which is the total of the precise expectations that an event will be positive.

Subsequently, we distinguished the suggested model exhibition using the confusion matrix described above. We assess the correctness of the suggested model using this confusion matrix, which also helps us assess the accuracy of order reports and projected outcomes.

- **Random Forest Result**

According to the representation in Table 3, the recall (RE) factor is 99% accurate and the precision (PR) factor is 100% in classification. However, the model's average accuracy (AC) of 99% is considered remarkable and outstanding in the given setup. It is worth noting that the F1 score is also 99% as indicated by the average accuracy factor.

**TABLE 3. RANDOM FOREST PERFORMANCE MEASURE**

| Accuracy | F1 Score | Precision | Recall |
|---|---|---|---|
| 99% | 99% | 100% | 99% |

## 2. Logistic Regression Classifier

Logistic Regression In classification are the most common and popular method for machine learning tasks. In this method, a set of training examples is given with which each example is marked belonging into one of two categories. Then, by using the Logistic Regression algorithm, a model that can predict whether a new example falls into one category or other is built.

- **Logistic Regression Confusion Matrix**

Figure 6, as given below, illustrates the confusion matrix of Logistic Regression.

تم استلام الورقة بتاريخ: 30/ 2024/6م وتم نشرها على الموقع بتاريخ: 30/ 2024/7م

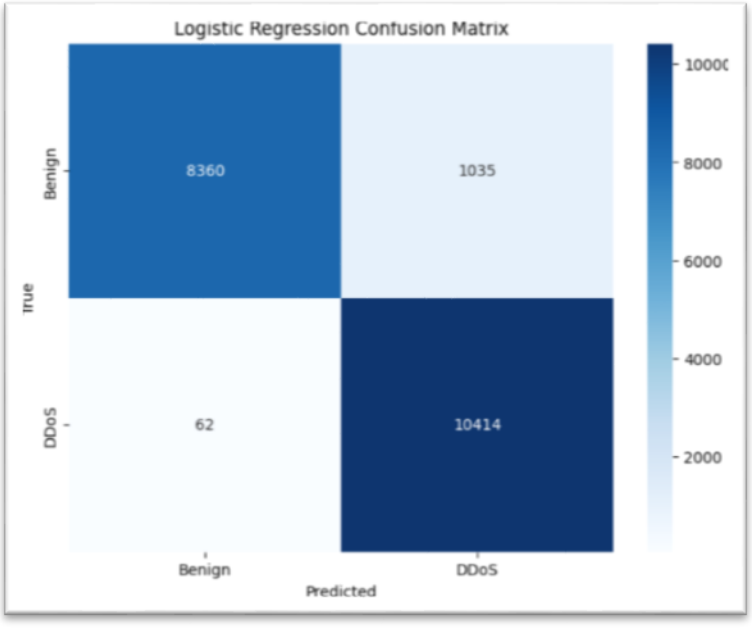



Figure.6. Logistic Regression Confusion Matrix

- **Logistic Regression Result**

The following outcomes show how well the algorithms performed. Table 4, which is shown below, shows all of the classification results. The gathered data revealed that the classification's recall (RE) is 99% accurate and its precision (PR) factor is about 90%. In addition, the average Accuracy (AC) of our proposed method is an astounding 94%. It is important to remember that the average accuracy indicates a 95% F1 score.

**TABLE 4. LOGISTIC REGRESSION PERFORMANCE MEASURE**

| Accuracy | F1 Score | Precision | Recall |
|---|---|---|---|
| 94% | 95% | 90% | 99% |

تم استلام الورقة بتاريخ: 30/ 2024/6م وتم نشرها على الموقع بتاريخ: 30/ 2024/7م

### 3. Neural Network Classifier

A neural network classifier is a type of algorithm used in machine learning for categorizing data and its a powerful tool in the machine learning toolbox, offering high accuracy and flexibility for various classification tasks.

- **Neural Network Confusion Matrix**

Figure 7, as seen below, shows the neural network's confusion matrix.

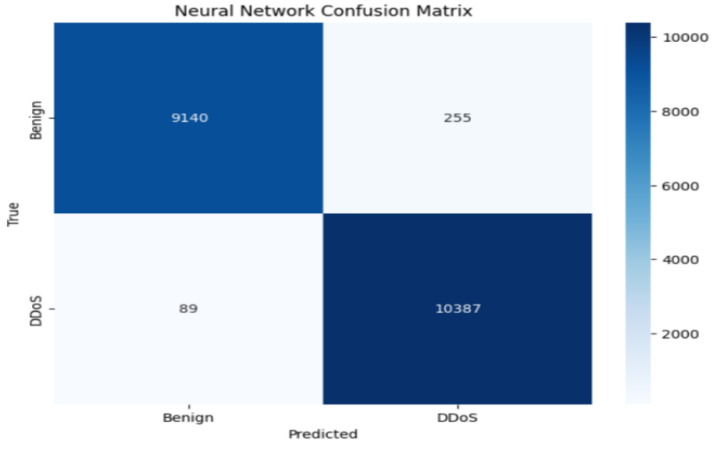



Figure 7. Neural Network Confusion Matrix

- **Neural Network Result**

The performance of the algorithms is demonstrated by the following results. All of the classification findings are displayed in Table 5, which is viewed below. The gathered data revealed that the classification's recall (RE) is 99% accurate and its precision (PR) factor is about 97%. In addition, the average Accuracy (AC) of our proposed method is an astounding 98%. It's critical to keep in mind that an F1 score of 98% is indicated by average accuracy.

**TABLE 5. NEURAL NETWORK PERFORMANCE MEASURE**

| Accuracy | F1 Score | Precision | Recall |
|---|---|---|---|
| 98% | 98% | 97% | 99% |

تم استلام الورقة بتاريخ: 30/ 2024/6م وتم نشرها على الموقع بتاريخ: 30/ 2024/7م

## Model Comparison and Discussion

On the CIC-IDS2017 datasets, we employed supervised learning techniques, such as neural networks and random forest logistic regression (Hu et al. 2014). Very good accuracy was reported, ranging from 94% to 99%. Table 6 displays the comparative analysis of the suggested algorithms on the dataset. We observed that the Random Forest model is more appropriate for identifying DDoS attacks based on our observations and findings.

By getting the Receiver Operating Characteristic (ROC), which is displayed in Figure 7, Area Under Curve (AUC) analyses are used to further validate the fitness of classification models. **Performance Evaluation of Three Machine Learning Algorithms (RF,LR.NN)**

| Evaluation Metrics | Random Forest | Logistic Regression | Neural Network |
|---|---|---|---|
| Accuracy | 0.99 | 0.94 | 0.98 |
| F1 Score | 0.99 | 0.95 | 0.98 |
| Recall | 0.99 | 0.99 | 0.99 |
| Precision | 1.00 | 0.90 | 0.97 |

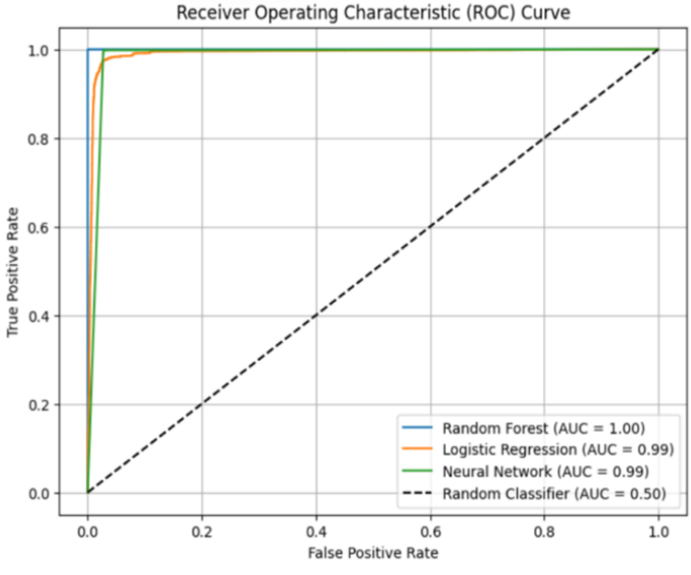



Figure 8. Receiver Operating Characteristic (ROC) Curve.

تم استلام الورقة بتاريخ: 30/ 6/2024م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

The true positive and false positive rates are plotted on the graph. When true positive and false positive rates change, the Area Under Curve (AUC) statistic shows how accurate a model is in classifying data. Figure 8 illustrates how well the LR, NN, and RF models have learned from the data; as a result, the area under the curve values under ideal performance are comparable to the computed accuracy values derived from Python confusion matrices. Compared to LR and NN, the RF model classifies the data more accurately.

## Conclusion and future work

We presented a thorough, methodical strategy for DDOS attack detection in this study. Initially, we chose the CIC-IDS2017 dataset, which includes DDoS attack data(Hu et al. 2014). Next, data wrangling was done using Python and a Jupyter notebook. Second, the dataset underwent preprocessing steps before being split into two classes: the dependent class and the independent class. We used the suggested supervised machine learning methodology. The supervised method produced predictions and classification results that were produced by the model. We employed classification algorithms from Random Forest, Logistic Regression, and Neural Networks.

In the first classification, we discovered that the Random Forest Precision (PR) and Recall (RE) are both 99% correct. Furthermore, we noticed that the average Accuracy (AC) of the proposed model was 100%, which is absolutely amazing and adequate. Take note that the F1 score is displayed as 99% by the average Accuracy. We observed that the Logistic Regression Precision (PR) and Recall (RE) for the second classification are 90% and 99%, respectively. We observed that the recommended model's average accuracy (AC) was 94%. The F1 score's average accuracy was 95%. We observed that the F1 score and Neural Network Accuracy (AC) in the third classification are both 98% accurate. For the recommended model, we observed 97% average Precision (PR), which is fantastic and incredibly intelligent. The Recall (RE) in the capacity of 99%.

تم استلام الورقة بتاريخ: 30/ 6/2024م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

By comparing the proposal models, we observed that the Random Forest model is more appropriate for identifying DDoS attacks based on our observations and findings.

For both labeled and unlabeled datasets, the idea can be extended to work on unsupervised learning toward supervised learning. Additionally, we will look into the impact that non-supervised learning algorithms will have on the detection of DDoS attacks; in particular, we will consider non-labeled datasets.

**References**

Aamir, Muhammad, Syed Sajjad Hussain Rizvi, Manzoor Ahmed Hashmani, Muhammad Zubair, and Jawwad Ahmed . Usman. 2021. "Machine Learning Classification of Port Scanning and DDoS Attacks: A Comparative Analysis." *Mehran University Research Journal of Engineering and Technology* 40 (1): 215–29. https://doi.org/10.22581/muet1982.2101.19.

Abu Rajab, Moheeb, Jay Zarfoss, Fabian Monrose, and Andreas Terzis. 2006. "A Multifaceted Approach to Understanding the Botnet Phenomenon." In *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*, 41–52. Rio de Janeriro Brazil: ACM. https://doi.org/10.1145/1177080.1177086.

Ahmad, Zeeshan, Adnan Shahid Khan, Cheah Wai Shiang, Johari Abdullah, and Farhan Ahmad. 2021. "Network Intrusion Detection System: A Systematic Study of Machine Learning and Deep Learning Approaches." *Transactions on Emerging Telecommunications Technologies* 32 (1): e4150. https://doi.org/10.1002/ett.4150.

Arctic. 2024. "A Brief History of Cybercrime." *Arctic Wolf* (blog). April 19, 2024. https://arcticwolf.com/resources/blog/decade-of-cybercrime/.

Cheng, Qiumei, Chunming WU, Haifeng Zhou, Dezhang Kong, Dong Zhang, Junchi Xing, and Wei Ruan. 2021. "Machine Learning Based Malicious Payload Identification in Software-Defined Networking." arXiv. http://arxiv.org/abs/2101.00847.

تم استلام الورقة بتاريخ: 30/ 6/2024م وتم نشرها على الموقع بتاريخ: 30/ 7/2024م

D'hooge, Laurens, Tim Wauters, Bruno Volckaert, and Filip De Turck. 2019. "Classification Hardness for Supervised Learners on 20 Years of Intrusion Detection Data." *IEEE Access* 7:167455–69. https://doi.org/10.1109/ACCESS.2019.2953451.

Hildebrand, Carol. 2021. "The Beat Goes On." *Netscout* (blog). May 17, 2021. https://www.netscout.com/blog/asert/beat-goes.

Hu, Han, Yonggang Wen, Tat-Seng Chua, and Xuelong Li. 2014. "Toward Scalable Systems for Big Data Analytics: A Technology Tutorial." *IEEE Access* 2:652–87. https://doi.org/10.1109/ACCESS.2014.2332453.

Karatas, Gozde, Onder Demir, and Ozgur Koray Sahingoz. 2020. "Increasing the Performance of Machine Learning-Based IDSs on an Imbalanced and Up-to-Date Dataset." *IEEE Access* 8:32150–62. https://doi.org/10.1109/ACCESS.2020.2973219.

Li, Yuchong, and Qinghui Liu. 2021. "A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments." *Energy Reports* 7 (November):8176–86. https://doi.org/10.1016/j.egyr.2021.08.126.

Martins, Nuno, Jose Magalhaes Cruz, Tiago Cruz, and Pedro Henriques Abreu. 2020. "Adversarial Machine Learning Applied to Intrusion and Malware Scenarios: A Systematic Review." *IEEE Access* 8:35403–19. https://doi.org/10.1109/ACCESS.2020.2974752.

Nicholson, Paul. 2022. "Five Most Famous DDoS Attacks and Then Some." *A10 Networks* (blog). May 4, 2022. https://www.a10networks.com/blog/5-most-famous-ddos-attacks/.

Sloot, Bart. 2023. "Cybersecurity Trends 2023." *Leaseweb Network* (blog). January 3, 2023. https://blog.leaseweb.com/2023/01/03/cybersecurity-trends-2023/.

تم استلام الورقة بتاريخ: 30/ 6/ 2024م وتم نشرها على الموقع بتاريخ: 30/ 7/ 2024م

Zakarya, Muhammad. 2013. "DDoS Verification and Attack Packet Dropping Algorithm in Cloud Computing."

Zargar, Saman Taghavi, James Joshi, and David Tipper. 2013. "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks." *IEEE Communications Surveys & Tutorials* 15 (4): 2046–69. https://doi.org/10.1109/SURV.2013.031413.00127.