International Journal of Innovative Research in Engineering
*Volume 3, Issue 6 (November-December 2022), PP: 176-179.*
*www.theijire.com*
***ISSN No: 2582-8746***

# DDoS Attack Detection Using Machine Learning

**Jayashree C. Pasalakar[1], Rutuja Ilag[2]**
*[1,2] Information Technology, AISSMS IOIT, Pune, India.*

**How to cite this paper:**
Jaya shree C. Pasalakar[1], Rutuja Ilag[2], "DDoS Attack Detection Using Machine Learning", IJIRE-V3I06-176-179.



***Abstract:*** *DDoS network attacks are referred to as Distributed Denial of Service attacks. When the DDoS Attack occurs on a particular server it makes the server slow down and even crashes sometimes. The attacker uses the HTTP requests to overwhelm the server which is consistent with its process. Because of DDoS, the user's site shows the service will not be provided and is denied. In the existing research study, the authors worked on Machine Learning Algorithm which had very low accuracy. It is necessary to work with the latest dataset and algorithms with greater accuracy to identify the current state of DDoS attacks. We used a machine learning approach for DDoS attacks which is Classification and Prediction. For this purpose, we used the Supervised Machine Learning Algorithms which are SVM and Naïve Bayes. For the proposed study, UNSWnb15 and CCIDS2017 dataset was used. Additionally, we generated a confusion matrix for the identification of the model performance. The Machine Learning approach is used to predict a DDoS in a network with a maximum accuracy of 99.68%, if the recommended combination of feature selection and classification algorithm is chosen.*

***Keywords:*** *Ransom ware, DDoS, SDN, Machine Learning, Malware, Vulnerable*

## I. INTRODUCTION

Distributed network attacks are referred to, usually, as Distributed Denial of Service (DDoS) attacks. These attacks take advantage of specific limitations that apply to any arrangement asset, such as the framework of the authorized organization's website. A DDoS attack sends different requests (with IP spoofing) to the target web assets to exceed the site's ability to handle various requests, at a given time, and make the site unable to operate effectively and efficiently – even for the legitimate users of the network. Typically, the target of various DDoS attacks are web applications and business websites; and the attacker may have different goals.


Artificial intelligence (AI) is a small tool that transforms information into data. In the past 50 years (approximately), information has had an impact on users' privacy and security. Except for the possibility of researching it and finding the examples hidden in it, the amount of information is negligible. We used the Machine Learning (ML) technique in this paper, so a short brief about machine learning was introduced in the next paragraph. ML is one form of artificial intelligence (AI) that give the systems the ability to learn automatically from the data itself without any programming or involvement from the human. The learning process starts with information or data in our case data was network traffic to search for any patterns in the collected data to make the right decision in future data.

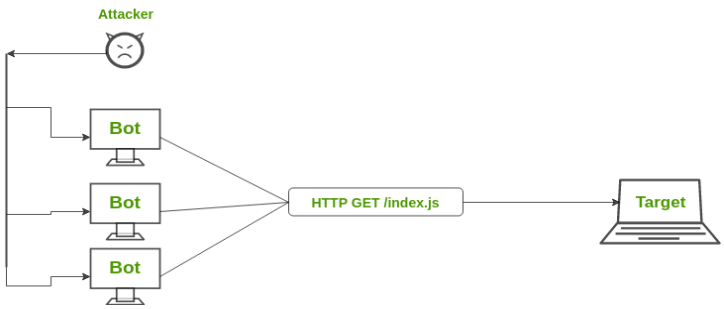


*Figure 1. Process of DDoS Attack*

Therefore, the developed model from learning acts as the human brain. ML can be categorized into 3 main techniques according to Learning from data book as follow:

The Unsupervised Learning is the model builds itself by learning relationships between the data using only the input data as the training data i.e. no output data were used in learning. This type of learning is used in clustering mechanisms. Supervised Learning: This type of learning used in 2 main categories: In Regression: you have to own input data and corresponding output data. . In Classification**:** you have to own the input data and valid output labels. Bayes Classifier is used classification relied on Bayes theorem application. SVM is used to carry out linear and nonlinear classification effectively. One networking paradigm that enables software-based programming of networking devices is SDN (Software-Defined Networking). It recognizes malicious traffic and links issues fast. Despite having numerous functions, they are also susceptible to DDoS attacks. To stop this malware attack, research is ongoing and has already begun. Some of the current research develops methods to anticipate DDoS attack flow using machine learning approaches. A key factor in the field of security is the quick development of artificial intelligence using artificial neural networks (ANN), machine learning (ML), and natural language processing (NLP). With the use of feature selection algorithms, classifiers, and machine learning, it is possible to create intelligent IDS that can recognize unidentified attacks. This DDoS attack, which was detected by a hybrid IDS, also targeted the most advanced area of information technology, the Internet of Things. This technique has tremendous importance since DDoS assaults can cause major problems and are difficult to identify and neutralize. The elapsed time during any form of real-time detection of DDoS attacks is also a challenge. The current methods for detecting DDoS attacks, however, have significant shortcomings, including high processing costs during detection and an inability to handle heavy network traffic heading toward the server. To distinguish DDoS from regular packets, classification algorithms classify the packets.

## II.MATERIAL AND METHODS

The SYN Flood is called a three-way handshake. The UDP flood is a denial-of-service attack in which User Datagram Protocol packets are forwarded to a targeted server to exhaust that server's capability to execute and reply to the requests. The HTTP flood is an attack in which the attacker exploits an HTTP GET or POST request to attack a web server. The HTTP flood attack frequently uses a botnet. A Death Ping controls IP conventions and sends malicious pings to the framework. The Smurf attacked Smurf to abuse the Internet Protocol and Internet Control Message Protocol. It will imitate the IP address and use ICMP to ping the IP address of the specified organization. A fragile attack is a type of attack which uses a large amount of UDP traffic to transmit to the transmission organization of the switch.

A DDOS attack is an attempt to interrupt a targeted server's normal traffic by overwhelming the target with a flood of Internet traffic. Dataset is divided into Training and Testing data. The data set uses 85% in training the algorithm and 15% of the remaining dataset is used for testing. The SVM classification algorithm gives an accuracy of 99.68%.

The following Methods are used for Data Ana
1. Feature Selection
2. Data Pre-processing
3. Feature Selection

**Machine Learning Algorithm Used**

Machine learning is divided into two forms: supervised learning and unsupervised learning. Supervised learning includes both the inputs and the desired outputs. After appropriate training, the program can provide expectations for new data. The algorithm will also give its output with the expected output correctly, and find errors to adjust the pattern. While unsupervised learning takes a set of data containing inputs and finds structure in the data.

**Machine learning techniques used:**

**Logistic Regression**– A classification algorithm used in Machine Learning and widely used in the cyber security domain to classify cases that is malicious or benign. It tries to determine whether a new sample best fits into a category.

**Support Vector Classifier**- A classification as well as regression algorithm in Machine Learning which visualizes a decision boundary among various data points from a class of data points. This algorithm is mostly used to detect malware, intrusions, and spam filtering.

**K-Nearest Neighbor** – It is an unsupervised machine learning algorithm that works on the principle of similar things working together. This algorithm stores the available data and classifies the data based on similar cases. This was used to identify the program's behavior as benign or malicious.

**Random Forest** – A supervised machine learning algorithm that performs both classifications as well as regression. It considers a group of decision trees and considers the majority classes in the case of classification and the average in the case of regression. It uses bagging (reducing variance using noisy data) and features randomness to create a forest of trees that shows decent accuracy than that of an individual tree.

**Ensemble Classifier**- It is a method used to provide better and more accurate than the rest of the models. It combines all the basic models to generate a new model, that provides more accuracy than the accuracy provided in individuals. Bagging,

Stacking, Boosting, etc. are some methods considered ensemble classifiers.

**Artificial Neural Network** – A derived biological neural network model which develops the structure of the human brain. These neural network mimics the human brain and helps to take decisions like humans. This network consists of three layers namely a) the Input layer b) the Hidden layer c) the Output layer where the input layer takes the input and provides an output from the output layer where the hidden layers act as weighted nodes to the input layer to give out the output.

**Hybrid Machine Learning Model**– It is the combination of one or more machine learning algorithms that helps to reduce the disadvantage of one another to provide better results. No single ML approach is suitable for all problems, just as no single cap fits all heads.

**Multi-Layer Perceptron-** It is one neural network that consists of three layers namely the input layer, hidden layer, and output layer among which the hidden layer plays a major role in computational operations and forward the data from the input to the output layer. These were majorly used in pattern classification, recognition, prediction, and approximation.

**Multiple Linear Regression** - An extension of linear regression which in turn gives out the result by a response variable from several explanatory variables. This model helps to establish a linear relationship between independent and dependent variables.

**Naive Bayes Algorithm:** Naive Bayes is a conditional probability model that demonstrates

$$P(A|B) = P(B|A)\, P(A)$$
$$P(B)$$

Here A and B are two events. P (A|B)
P (A) and P (B)
P (B|A)

**Support Vector Machine (SVM):**

In this algorithm, with an estimation of a particular coordinate, the system plots every data item as a point in n-dimensional space. Support vector machine is the supervised algorithm for machine learning that can be used both for regression and classification. After that classification, the hyper-plane that separates the two classes is found. Exceptionally fine. Support Vectors are essentially the coordinates of individual observation. Support vectors are essentially the best segregate the two classes. SVM is a standout amongst other realized methods in pattern classification and image classification.
This evaluation and observation say that this prediction, as compared to actual data it gives 90 % accuracy.
We calculated the Prediction matrix as:

Precision: PR = TP / TP + FP
Recall: RE = TP / TP + FN
F1 Score: F1 = 2 * (PR * RE) / (PR + RE)
Accuracy: AC = TP+TN / (TP+TN+FP+FN)

## III.DISCUSSION

A DDoS Attack is a major security threat or attack which is designed to overwhelm the server with continuous HTTP requests. These requests are the combinations of the actual users and the attackers who intend to disturb the server. This type of attack causes the smoothly running server to crash. These attackers decide on the target first. Once the target is decided it makes the system to be unable to respond to the requests and this makes the Denial of Services at the user's site. Many times this happens that the server is under attack without the owner's awareness. Many Authors have contributed to the study of DDoS Attack detection which helps us to determine whether the system has gone under the attack or not:

Intrusion Detection/Network Traffic Classification:

XianweiGao proposed a comparative work for network traffic classification. They used machine learning classifiers for intrusion detection. The dataset taken is CICIDS and KDD from the UCI repository. They found support vector machine SVM one of the best algorithms as compared to others. **Tong tong Su** et al. proposed adaptive learning for intrusion detection. They used the KDD dataset from an online repository. These models are D tree, R-forest, and KNN classifiers. In this study, the authors found that D tree and ensemble models are good for classification results. The overall accuracy of the proposed work is 85 %.

Feature Selection Analysis in network:

Davidetal**.** used the entire sandbox analysis report as the feature and learned the report on a word level by deep belief network. Although dynamic analysis can monitor the behavior of malware, there are some disadvantages. Malware can easily detect security sand box environments, to evade the analysis. For example, the Wanna Cry ransom ware tries to connect to a server that does not exist. If the virtual environment can resolve the address, the malware will assume that this is a sandbox environment and stop running. Some malware probably needs a specific software environment to run. The malware will fail to

be detected if the sandbox environment does not match it. Static analysis can quickly extract opcodes, sections, APIs, and other important features with tools. Compared with dynamic feature representation, the static approach is simpler and faster, and it is more suitable for cloud tenants.

Binary Data Analysis:

In 2011, Nataraj et al. proposed a novel method by converting malware binaries into grayscale images and found that images of the same family appear similar in texture. Ni et al. used the Sim Hash algorithm to reconstruct the opcode sequences into fixed-length sequences and converted them to images by treating every 1-bit data as 1 pixel. Cui et al. applied bi-cubic interpolation to rescale malware images into a fixed size. Fu J Fu j et al. proposed an approach to visualize malware as RGB-colored images and extract global features from the images. But converting malware into images may drop information significantly, and the detection accuracy of this model is not always satisfied.

## IV.CONCLUSION

The study of DDoS Attack detection is carried out this proposed work. The various Machine Learning algorithms are applied to get the perfect required outcomes through this study. Distributed Denial of Service (DDoS) is the attack that causes the server to crash through its malicious attacks. In the proposed work we applied the classification Techniques of Machine learning to detect these types of attacks. As for this study, we required a supervised Machine Learning algorithm. These algorithms are SVM (Support Vector Machine) and Naïve Bayes Algorithm. Among all Machine Learning Algorithms of Supervised and Unsupervised types these two have great accuracy. But through this study, we learned that SVM has more accuracy than that the Naïve Bayes. We used two datasets UNSWnb15 and CCIDS2017. We applied all the methods to these two datasets. For applying the algorithms, we divide the datasets into two reliable parts. The model generated the prediction for the required supervised algorithm. As for the Unsupervised algorithm, reliable data and algorithm are required.

## V. ABBREVIATIONS

**DDoS –** Distributed Denial of Service
**IP –** Internet Protocol
**SDN –** Software Defined Networking
**DoS –** Denial of Service
**NIST –** National Institute of Standards and Technology
**IDS –** Intrusion Detection System
**ANN** – Artificial Neural Network
**ML-** Machine Learning
**NLP-** Natural Language Processing
**SVC –** Support Vector Classifier
**RF-** Random Forest
**MLP –** Multi-Layer Perceptron
**XG-Boost** – Extreme Gradient Boosting
**ANOVA** – Analysis of Variance
**IoT** – Internet of Things

## References

*1] Net Losses: Estimating the global cost of cybercrime. Technical report, Intel Security Group, 2014.*
*2] Natara ,Fu j et al. Binary Data Analysis IEE 2011*
*3] David et al used various methods for detecting the malicious ransom ware 2015 IEEE*
*4] R. Miao, R. Potharaju, M. Yu, and N. Jain, Cloud Characterizing, ACM, 2015.*
*5] P. Singh and M. Khari, Black hole analysis Springer, 2021.*
*6] F.Y. Lee and S. Shieh, "Defending against spoofed DDoS attacks with path fingerprint." International Journal of Computers and Security, Elsevier, March 2005.*
*7] A. Yudhana, I. Riadi, F. J. I. J. O. A. C. S. Ridho, and APPLICATIONS, "DDoS Classification Using Neural Network and Naïve Bayes Methods for Network Forensics," 2018.*
*8] H. Wang, C. Jin, and K.G. Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering." IEEE/ACM Transactions on Networking, Feb. 2007.*
*9] M. Zakarya, "Ddos verification and attack packet dropping algorithm in cloud computing," World A*