International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 11 | Nov 2022 www.irjet.net p-ISSN: 2395-0072

DDoS Attack Detection and Botnet Prevention using Machine Learning

Neeraj Patil[1]

[1]*Department of Electronics Engineering, Vivekanand Education Society's Institute of Technology*

Abstract - *Distributed Denial of Service (DDoS) attacks are one of the major threats in the world of cyber security and networking. With advances in computer and communication technology, the losses caused by DDoS attacks are becoming more and more severe. Many large companies face great economic and reputational loss due to DoS and DDoS attacks. With this in mind, this paper proposes a machine learningbased DDoS attack detection method. We are currently using the NSL KDD Dataset to build our machine learning model. Machine learning algorithms like Logistic Regression Classifier, Support Vector Machine, K Nearest Neighbor, Decision Tree Classifier, ADABoost Classifier are used to train our model. The accuracy obtained is 90.4%, 90.3%, 89.1%, 82.28%. We also plan to add some additional features, such as how to prevent such types of attacks. And we also plan to add a feature like BOTNET detection, which will be very useful for individual device owners and users to prevent their device from becoming a botnet.*

Key Words: DDoS , Machine Learning , Botnet

1. INTRODUCTION

A Denial-of-Service (DoS) attack is an attack that aims to shut down a computer or network and make it inaccessible to the intended users. DoS attacks achieve this by flooding target servers with Internet traffic, sending constant requests to the server.

A Distributed Denial-of-Service (DDoS) attack is a malicious attempt to disrupt the normal operation of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DDoS attacks achieve their effectiveness by using various malware-infected computer systems and connected devices as sources of attack traffic. Machines used can include PCs, laptops and other network resources such as IoT devices.

When a botnet targets a victim's server or network, each bot sends requests to the target's IP address, which can cause the server or network to become overwhelmed, resulting in a denial of service. Because of this, legitimate users will not be able to use the services because the target servers are already overwhelmed with attack traffic. Since each bot is a legitimate Internet device, it can be difficult to separate attack traffic from normal traffic.

A botnet is an army of multiple malware-infected computers that work together to complete repetitive tasks. Botnets are under the control of a single attacking party, known as the "bot-master". The goal of creating a botnet is to infect as many connected devices as the attackers use this vast computing power to flood the servers of target organizations with large amounts of Internet traffic.

A DDoS (Distributed Denial of Service) attack results in the unavailability of services for users. A proposed solution to overcome this kind of attack is to monitor the network that is being attacked. To overcome the above problem, we try to build a hybrid heterogeneous multi-classifier ensemble learning to get stronger generalization and more complementarity. We design a heterogeneous detection system model and also construct model component classifiers based on Bagging, Random Forest, ANN and NN (-Nearest Neighbor) algorithms. In addition, we are working on the design of a detection algorithm based on Singular Value Decomposition (SVD) in a heterogeneous classification ensemble model. It is excellent and very stable in TNR (True Negative Rate), accuracy and precision for detection performance for DDoS attacks.

Our project only focuses on big organizations and services which are vulnerable to DDOS attacks in future, and can only be operated by Cyber security and IT departments of the organizations. We are planning to add some more features like Botnet prevention, which aims to reduce the creation of Botnet, and will further reduce the intensity of DDoS attacks in future. Botnet prevention can be handy for naive and legitimate users. This feature could scan URLs and check for malware, if any, and prevent the systems from being a part of the botnet.

2.LITERATURE REVIEW

This paper by Jin Kim et al. (2017) [1] projects the idea of using deep neural networks (DNN) to investigate and test an artificial intelligence (AI) intrusion detection system with the KDD Cup 99 dataset. The intrusion detection system using deep neural networks is done through data preprocessing and a deep neural network model. The

accuracy rate is 99.01%. The drawback is that time series data analysis will be needed using the recurrent neural network (RNN) model and the long short-term memory (LSTM) model for the battle against distributed denial of service (DDoS) attacks.

Machine Learning techniques have been adopted for DDoS Attack detection, in this [2] they have used a semisupervised ML approach for DDoS detection based on network Entropy estimation, Co-clustering, Information Gain Ratio and Extra-Trees algorithm. The unsupervised part of the approach allows to reduce the irrelevant normal traffic data for DDoS detection which allows to reduce false positive rates and increase accuracy. Whereas, the supervised part allows to reduce the false positive rates of the unsupervised part and to accurately classify the DDoS traffic. Various experiments were performed to evaluate the proposed approach using three public datasets namely NSL-KDD, UNB ISCX 12 and UNSW-NB15. An accuracy of 98.23%, 99.88% and 93.71% is achieved for respectively NSL-KDD, UNB ISCX 12 and UNSW-NB15 datasets, with false positive rates 0.33%, 0.35% and 0.46%.

The work in the [3] paper Pei et al. (2019) mainly focuses on DDoS attack modes and the variable size of traffic attack and aims to detect DDoS attack based on machine learning. This method includes feature extraction and model detection techniques. The characteristics of the model detection phase are trained in the training model on Random forest algorithm and test model is validated by DDoS attack and SVM is used to detect accuracy.

With great development in Science and Technology, the privacy and security of various organizations are prone to attacks. This paper [4] Kaur et al. (2019) mainly focuses on DDoS Attack Detection using Machine learning techniques such as KNN, SVM and ANN. The KDDCUP99 Datasets are used to perform the experiments and algorithms are implemented on the same. This paper specifies the limitations of KNN algorithm and the advantage of using hybrid approach as it gives higher accuracy (95.2-97.4 %) rate with the lower precision value.

In the paper [5]. Sahingoz et. al have proposed phishing URL detection using machine learning. Dataset is designed by them by using 37,175 phishing urls and 36,400 legitimate urls and these urls are fetched from PhishTank and Yandex Search API respectively. The Random Forest algorithm is used, and it identifies phishing URLs with a 97.98 percent accuracy rate.

The paper[6] Okuchaba et al. solved a major problem which is detection of phishing websites/urls using SVM and Deep neural networks. The urlset dataset was used, which included 48,009 authentic website Urls and 48,009 phishing Urls for a total of 98,019 website Urls. It was a pre-processed dataset from which they identified two features, with 0 indicating a legitimate website Url and 1 indicating a phishing website. After training, the support vector classifier provided them with 97.08% accuracy and the deep learning algorithm gave 98.33%.

3. DATASET FOR THE PROJECT

3.1 DDoS Attack Detection System

We have used NSL KDD dataset [] pre-separated (splitted) into Train and Test dataset [9].

Train dataset consists of 1,25,973 rows and 42 columns Test dataset consists of 22544 rows and 42 columns The algorithm's performance is evaluated using the NSL KDD dataset from the Kaggle dataset repository. Each instance in the NSL- KDD dataset is assigned to a network data class. Each class in NSL- KDD dataset are grouped into five main classes: (a) Normal, (b) Denial of Services (DoS), (c) Probing (Probe), (d) User to Root (U2R) (e) Remote to User (R2L).

Because of the large number of redundant instances, the NSLKDD 99 dataset is a reliable dataset for testing DoS and DDoS detection.

3.1.1 Data Preprocessing

Data preprocessing is carried out to make it suitable for building and training the machine learning model. All null values are dropped from the data.

One-Hot-Encoding is used to convert all categorical properties to binary properties.

In our project, we have used Machine Learning Algorithms like Logistic Regression Classifier and Support vector machine (SVM) for the detection of DDoS attacks. We have used K Nearest Neighbor, Random Forest Classifier, and Decision Tree Classifier as classification models. We have found that the Logistic Regression Classifier provides better accuracy than the rest, and we chose the same for model selection purposes.

3.1.2 Feature Selection

Feature selection is an important part of the model as it targets the important features/variables used for prediction. For bringing out the best features from the given dataset, the Scikit-learn API provides SelectKBest class. SelectKBest selects the best features according to the K highest score. Here, we can apply the method for both classification and regression data by changing the 'score_func' parameter. It is an important process when we are preparing a large dataset for training we are selecting the best features. This feature helps us to eliminate redundant parts of the data and also reduces training time.

3.2 Botnet Prevention System

The Botnet Prevention feature is basically a malicious URL scanner, which will scan for phishing / malicious web links and URLs. "Phishing site URL" dataset is used for the proposed feature. The dataset contains 5,49,361 rows containing link samples and 2 columns.

Dataset contains 1,45,180 bad urls and 4,04,181 good urls.

3.2.1 Data Preprocessing

A] Text Tokenizer : The system contains string input, so a text tokenizer is used to split the entire input into smaller units called tokens and form an array of tokens.

After tokenization, the text gets splitted into words and an array of tokens/words are formed.

Eg: https://www.youtube.com/

After Tokenization : ["https", "www", "youtube", "com"]

B] Text Vectorizer: Text vectorizer is used to convert text data into numerical vectors. CountVectorizer is used to transform a given text into a vector on the basis of the frequency(count) of each word that occurs in the entire text..

The experiments were carried out on a laptop running

Windows 10 64-bits OS, powered by 2.2 GHz octa-core AMD Ryzen 3 CPU paired with 8GB of RAM with storage configuration of 1TB hard drive.

4. PROPOSED SYSTEM

4.1 Steps Involved

Steps in our project are as follows:

1. Firstly, the user will get a local host ID, he has to copy paste it in any of his desired Search Engines (such as Google Firefox, etc). 2. Then the user has to enter all the Inputs shown on its screen.

3. Once the user fills all the inputs correctly,

4. Our model then will analyze all the given inputs and accordingly classifications of attacks will take place.

5. There are many kinds of DDOS Attacks happening worldwide hence we must train our model to detect all types of DDOS Attacks with much Accuracy and precision.

6. Therefore, Most popularly used Machine Learning Algorithms have been used such as SUPPORT VECTOR MACHINE (SVM) and Logistic Regression Algorithm which provided us the desired Accuracy.

7. After the classification is done our model will identify Is there a DDOS Attack happened or not? This process is termed as Detection of DDOS Attack

8. If the output came as a negative, then it will notify the user as "NORMAL" which means there is no DDOS Attack took place and hence our system is safe from the attack

9. If the output came as positive, then it will notify the user as "DDOS ATTACK" which means there is a DDOS Attack happening on your system. 10. Then accordingly the user will have to take the necessary actions.

4.1.1 Proposed Systems

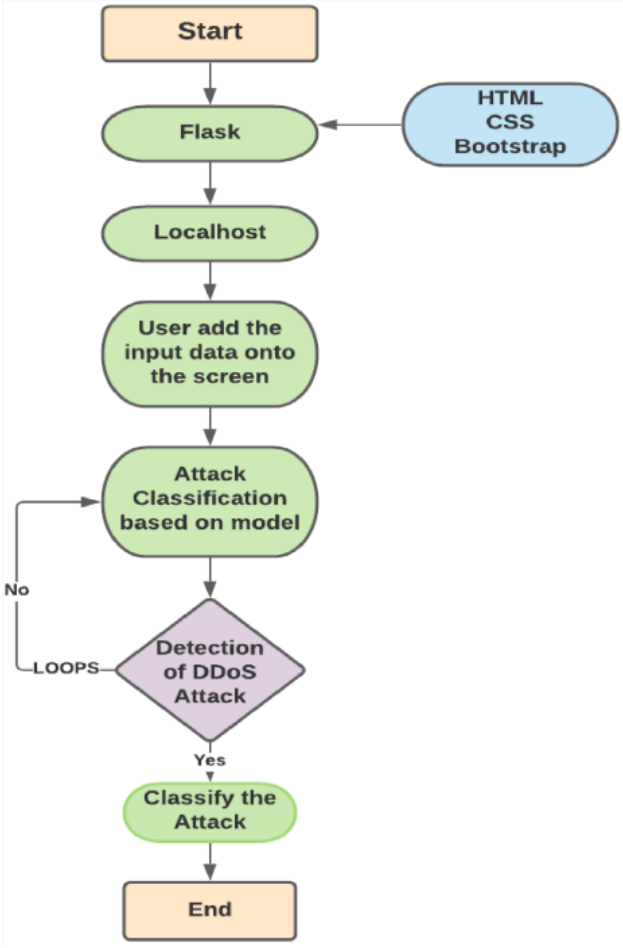

Fig -1: Flowchart of the DDoS Detection System

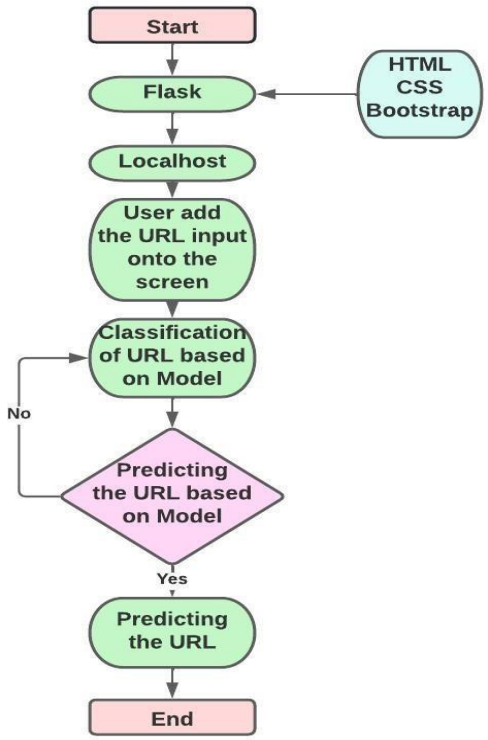

Fig -2: Flowchart of the Botnet Prevention System

4.2 PARAMETER EVALUATION

The accuracy of the models can be calculated using a confusion matrix. A confusion matrix is a table used to describe the performance of a classification model on a set of test data for which true values are known.

4.2.1 DDoS Attack Detection System

We have trained our dataset using various Machine learning algorithms. Mainly classification algorithms are used and accuracy of the models are evaluated.

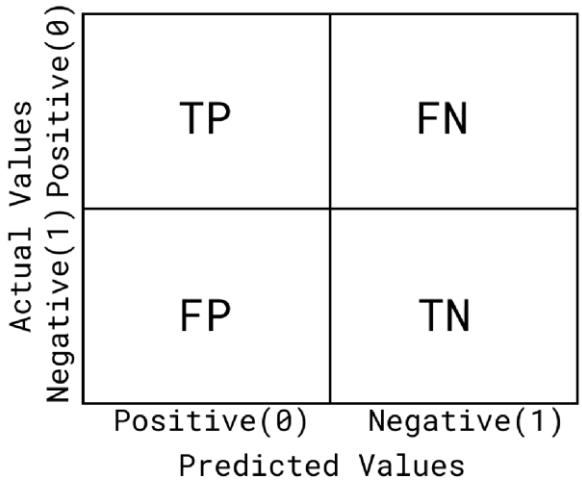

Fig-3: Confusion Matrix

True Positives (TP): In this case we predicted YES (The attack is DDOS) and actually the DDOS attack occurred.

True Negatives (TN): In this case we predicted NO, and in actuality the attack is not DDOS.

False Positives (FP): In this case we predicted YES, but in actuality there was no DDOS attack

False Negatives (FN): In this case we predicted NO, but in actuality there was a DDOS attack.

1. Accuracy

   Accuracy is the rate at which an attack is classified as an actual attack or a normal attack i.e. no attack.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

2. Detection rate

   The detection rate is the rate at which genuine attacks are detected even if they are efficient or not.

$$\text{Detection Rate} = \frac{TP}{TP+FN}$$

3. False alarm rate

   False alarm rate is the rate at which an event is wrongly identified as an attack.

$$\text{Detection Rate} = \frac{FP}{FP+TN}$$

4.2.1.1 Classification Models and their accuracy:

4.2.1 a. Logistic Regression:

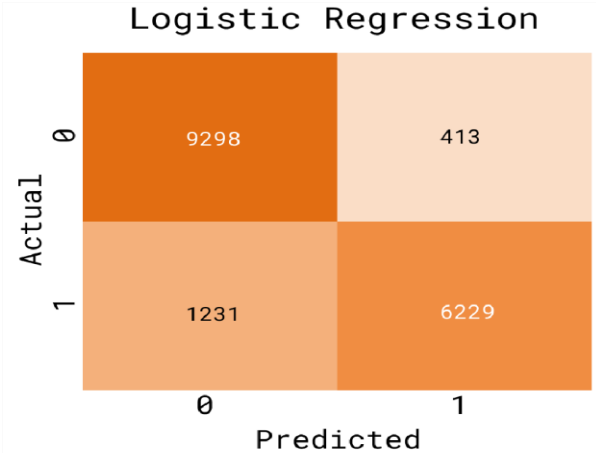

Fig-4: Confusion Matrix of Logistic Regression

TP = 9298, TN= 6229, FP= 1231, FN= 413

Accuracy= (9298+6229)/(9298+6229+1231+413)= 0.904

= 0.904*100= **90.4%**

4.2.1 b. Support Vector Machine:

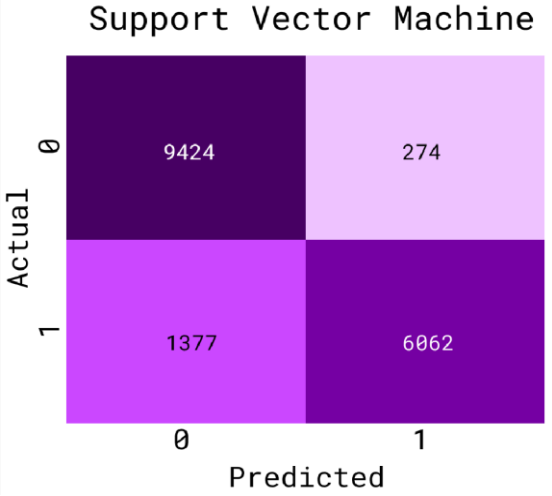

Fig-5: Confusion Matrix of Support Vector Machine

TP = 9424, TN= 6062, FP= 1377, FN= 274

Accuracy= (9424+6062)/(9424+6062+1377+274)= 0.9036

= 0.9036*100= **90.36%**

4.2.1.c K Nearest Neighbors Classifier:

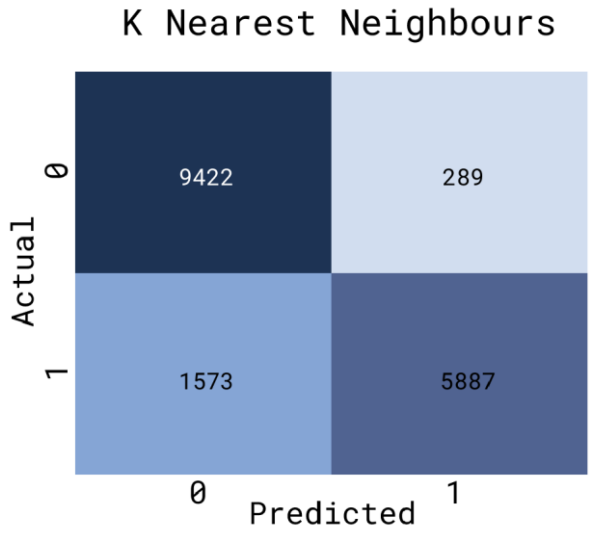

Fig-6 : Confusion Matrix of K Nearest Neighbors

Classifier TP = 9422, TN= 5887, FP= 1573, FN= 289

Accuracy= (9422+5887)/(9422+5887+1573+289)= 0.8915

= 0.8915*100= **89.15%**

4.2.1.d. ADA Boost:

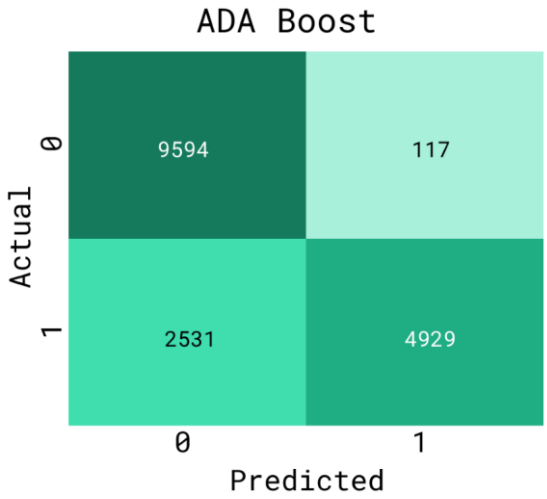

Fig-7: Confusion Matrix of ADABoost

TP = 9594, TN= 4929, FP= 2531, FN= 117

Accuracy= (9594+4929)/(9594+4929+2531+117)= 0.8457

= 0.8457*100= **84.57%**

4.2.1.e. Decision Tree Classifier:

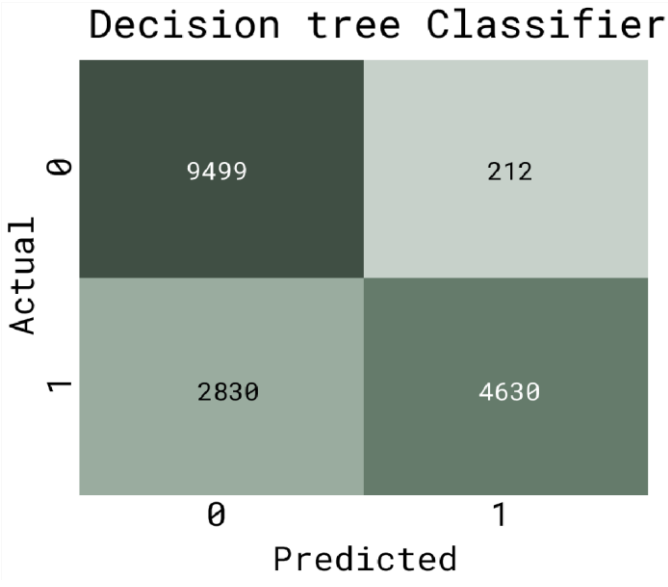

Fig-8: Confusion Matrix of Decision Tree Classifier

TP = 9499, TN= 4630, FP= 2830, FN= 212

Accuracy= (9499+4630)/(9499+4630+2830+212)= 0.8228

= 0.8228*100= **82.28%**

So, the Logistic regression classifier provides accuracy of 90.4% to the model.

For feature selection purposes, we have sklearn.feature_selection.SelectKBest method which reduces the number of input variables and targets only required ones.

4.2.2 Botnet Prevention System:

Logistic Regression algorithm is used to train the model which scans for legitimate or malicious URLs. Accuracy given by the model is 96.35%.

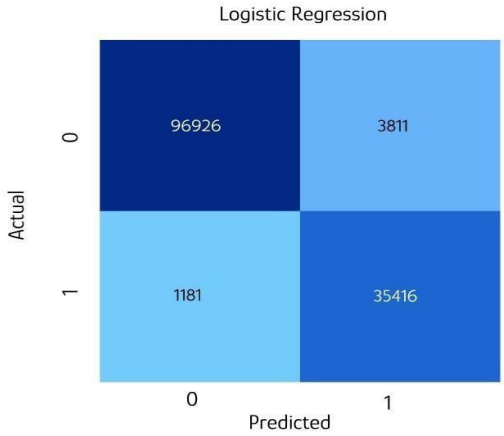

Fig-9: Confusion Matrix of Logistic Regression

TP = 96926, TN= 35416 , FP= 3811 , FN= 1181

Accuracy=

(96926+35416)/(96926+35416+3811+1181)= 0.9635

= 0.9635*100= **96.35%**

Summary of the results :

Algorithm	Accuracy	Detection rate	False Alarm
LR	90.4%	0.957	0.165
SVM	90.36%	0.973	0.182
KNN	89.15%	0.970	0.210
Decision Tree	82.28%	0.978	0.342

Table 1: Summary of Results

5. RESULTS

5.1 DDoS Attack Detection System

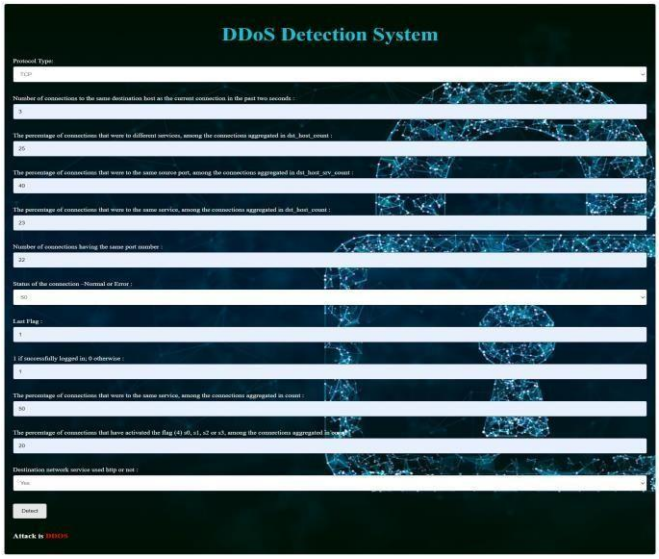

Fig-10: DDoS Attack Detection System **5.2**

Botnet Prevention System

Fig-11: Botnet Prevention System **6.**

CONCLUSIONS

Cyber security threats are changing, becoming much more elusive and complicated. Detecting malicious security risks and attacks is becoming a significant challenge in cyberspace. Machine learning is a powerful tool to overcome these challenges.

This work proposes the use of a linear regression model for the detection of DDoS attacks. By extracting the three protocol attack packets of the DDOS attack tool, feature extraction and format conversion are performed to extract DDoS attack traffic. Then, the extracted features are used as input features of machine learning and logistic regression algorithm is used to train and obtain a DDoS attack detection model. For the botnet prevention function, the URL is tokenized, and each token is classified into a legitimate and a malicious token, and a logistic regression algorithm is used to train the model overall.

7. REFERENCES

[1] Jin Kim, Nara Shin, S. Y. Jo and Sang Hyun Kim, "Method of intrusion detection using deep neural network," 2017 IEEE International Conference on Big Data and Smart Computing (BigComp), 2017, pp. 313316, doi: 10.1109/BIGCOMP.2017.7881684.

[2] Idhammad M, Afdel K, Belouch M. "Semi-supervised machine learning approach for DDoS detection." Applied Intelligence. 2018 Oct;48(10):3193-208.

[3] Pei J, Chen Y, Ji W. "A DDoS Attack Detection Method Based on Machine Learning." InJournal of Physics: Conference Series 2019 Jun 1 (Vol. 1237, No. 3, p. 032040). IOP

[4] Kaur G, Gupta P. "Hybrid approach for detecting ddos attacks in software defined networks."In2019 Twelfth International Conference on Contemporary Computing (IC3) 2019 Aug 8 (pp. 1-6). IEEE.

[5] Sahingoz, O.K., Buber, E., Demir, O. and Diri, B., 2019. Machine learning based phishing detection from URLs. Expert Systems with Applications, 117, pp.345-357.

[6] Zekri, M., El Kafhali, S., Aboutabit, N. and Saadi, Y., 2017, October. DDoS attack detection using machine learning techniques in cloud computing environments. In 2017 3rd international conference of cloud computing technologies and applications (CloudTech) (pp. 1-7). IEEE.

[7] Pervez, M.S. and Farid, D.M., 2014, December. Feature selection and intrusion classification in NSL-KDD cup 99 dataset employing SVMs. In The 8th International Conference on Software, Knowledge, Information Management and Applications (SKIMA 2014) (pp. 1-6). IEEE.