EAST POINT COLLEGE OF ENGINEERING & TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

ANALYSIS & DETECTION OF DDOS ATTACK USING MACHINE LEARNING TECHNIQUES

Abstract

Distributed Denial of Service attacks fall under the category of critical attacks that compromise the supply of the network.

DDos attacks continue to grow rapidly so to detect and mitigate these attacks became a challenging task. This work is carried out on a portal built on local server and a brand-new dataset will be generated with Intrusion Detection System.

Tor Hammer tool was used as an attacking mechanism.

The work incorporates various machine learning algorithms: Support Vector Machine, Decision Tree, KNN and Logistic Regression for classification.

Problem Statement

The main aim of our project is to process newly generated dataset for DDOS detection and to increase the accuracy of the detection rate in DDOS attack.

Our other main objectives are to, identify whether the traffic data is suspicious or normal, To reduce false negative rate in distributed denial of service (DDOS) and to get good detection rate.

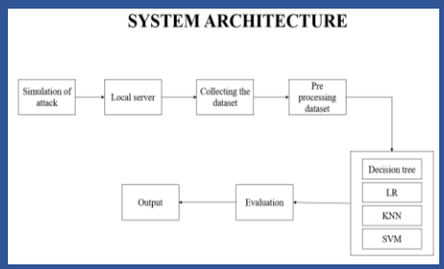
Objectives

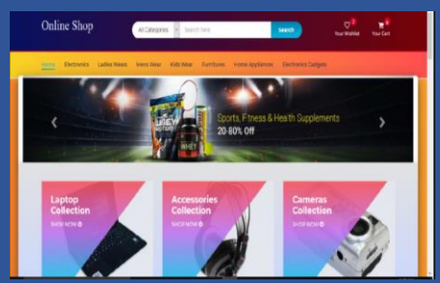
To identify whether the traffic data is suspicious or normal.

Classification algorithms are very important category of supervised machine learning algorithms.

Algorithms Support Vector Machine, Decision Tree, KNN and Logistic Regression for classification.

System Design & Implementation





Tools Used

1. Tor Hammer Tool
2. Intrusion Detection System SNORT
3. WEKA Tool
4. Jupyter Notebook
5. Linux Operating System

Result & Analysis

	Algorithm	Jaccard-score	F1-score
0	Decision Tree	0.045780	0.920277
1	SVM	0.144144	0.929593
2	Logistic Regression	0.011662	0.916172
3	KNN	0.128463	0.927074

Module No	Module Name	Input	Expected Outcome	Actual Result
1	Data Preprocessing	Unprocessed dataset	All the missing value in the entries must be assigned to null	All missing values are assigned to null
2	Decision Tree	Training and testing data	95-100%	92.02%
3	Logistic Regression	Training and testing data	95-100%	91.61%
4	KNN	Training and testing data	95-100%	92.70%
5	SVM	Training and testing data	95-100%	92.95%

Conclusion & Applications

Machine learning classification algorithms were applied to the data set namely Support Vector Machine, Decision tree, KNN and Logistic Regression. After considering all the algorithms and implementing them in the model SVM algorithm showed greater results compared to other algorithms. The SVM model's high performance and It's wide variety of classification problems includes high dimensional and not linearly separable problems. Our experimental results show that applying one-class SVM anomaly detection methods on our browsing behaviour instances can discriminate between normal behaviour instances and the attack behaviour instances. Our main application is to mitigate DDoS attack on the cloud platform.

TEAM MEMBERS:

1. DHIVAKAR A K (1EP17CS019)
2. PRUTHVI S (1EP17CS063)
3. SANTHOSH E (1EP17CS076)
4. SHREYA M (1EP17CS082)

UNDER THE GUIDANCE OF:
DR. EMILIN SHYNI C
PROFESSOR, DEPT OF CSE