# Intrusion-Detection-System

**INTRUSION DETECTION SYSTEM USING MACHINE LEARNING ALGORITHMS**

The aim of this system is to Detect Attack in a network using Machine Learning.

**ABOUT DATASET: -**

Dataset Source: The BoT-IoT Dataset

(https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/bot\_iot.php)

**DATASET USED: -**

10-best features (5% of BoT-IoT dataset)

https://cloudstor.aarnet.edu.au/plus/s/umT99TnxvbpkkoE?path=%2FCSV%2FTraning%20and%20Testing%20Tets%20(5%25%20of%20the%20entier%20dataset)%2F10-best%20features%2F10-best%20Training-Testing%20split

The BoT-IoT dataset was created by designing a realistic network environment in the Cyber Range Lab of The center of UNSW Canberra Cyber. The environment incorporates a combination of normal and botnet traffic. The dataset’s source files are provided in different formats, including the original pcap files, the generated argus files and csv files. The files were separated, based on attack category and subcategory, to better assist in labeling process.

We have used the 5% of the dataset to create our ML model. It contains 10 best features for training and testing dataset. This dataset has 19 columns with category and subcategory as the target columns and over 2.9 million rows.

**ML Models: -**

We have used 3 different models to the same dataset to check the performance of different models. The models which we have used are Logistic Regression Model, Support Vector Machines and XGBoost model. Preprocessing is similar on the all 3 models with category as the target value. Data is also encoded and scaled to fit in the model. After getting the base accuracy for the model, we tuned our model by HyperParameter Tuning and got better accuracy for each of the model.

**Results: -**

Logistic Regression: ~ 97%

SVM: ~ 99%

XGBoost: ~ 91%

SVM performed best here after parameter tuning.