DDoS Attack Detection & Mitigation

In propose work we are employing Machine & deep learning algorithms to detect IOT attacks. IOT are small devices which can be deployed anywhere to sense environment or its nearby data and then utilize internet connection to post sense data to centralized server for further processing or monitoring. Due to internet connectivity this small devices will be easily attack or hacked to inject false information or to steal data. To avoid such attacks heavy antivirus cannot be deployed as it consume heavy battery power and required heavy processing resources.

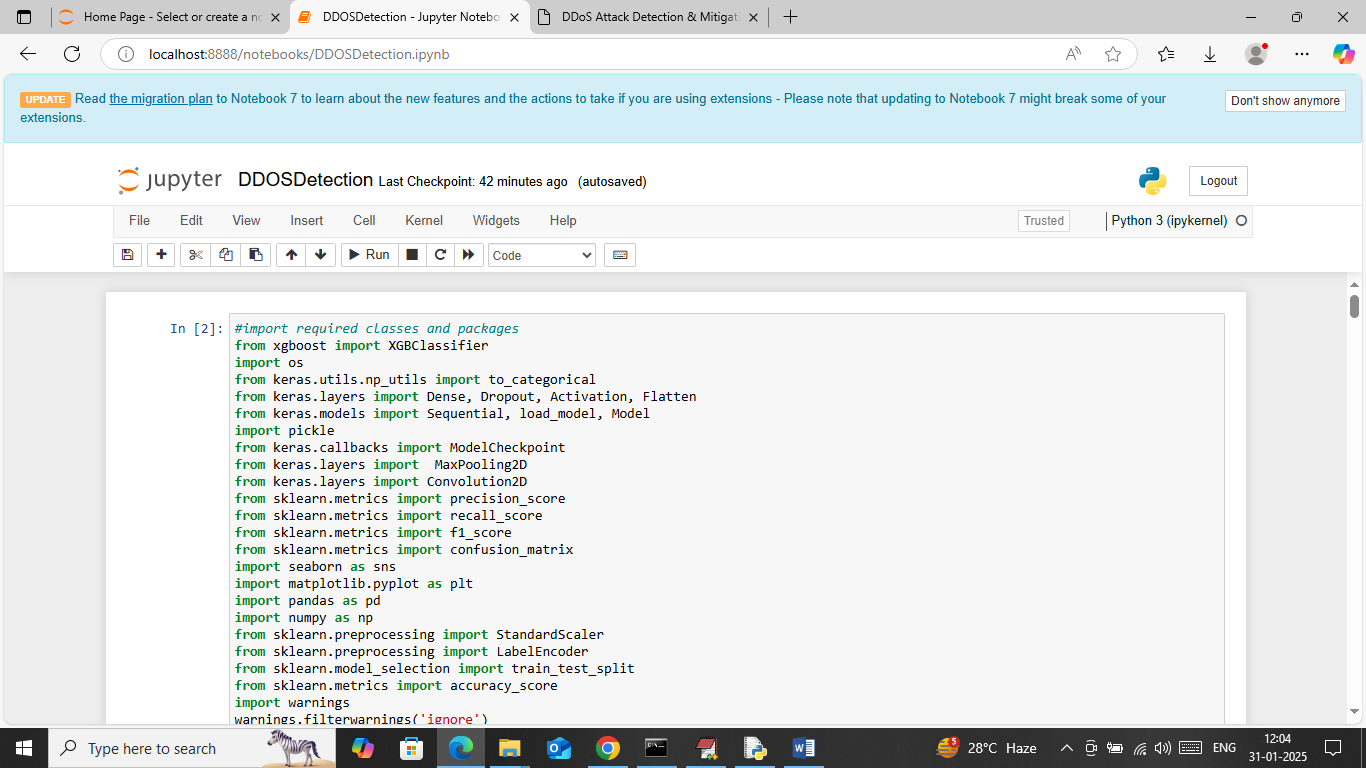
So rule based or ML based algorithms are cheap in processing but Rule based technique detection accuracy is very less so we are experimenting with ML and DL algorithms such as XGBOOST and CNN. This algorithms are able to detect attacks with an accuracy of more than 95%.

To train above algorithms we have utilize IOT23 DDOS attack dataset and then each algorithm performance is evaluated using different metrics like accuracy, precision, recall, Confusion Matrix and FCSORE.

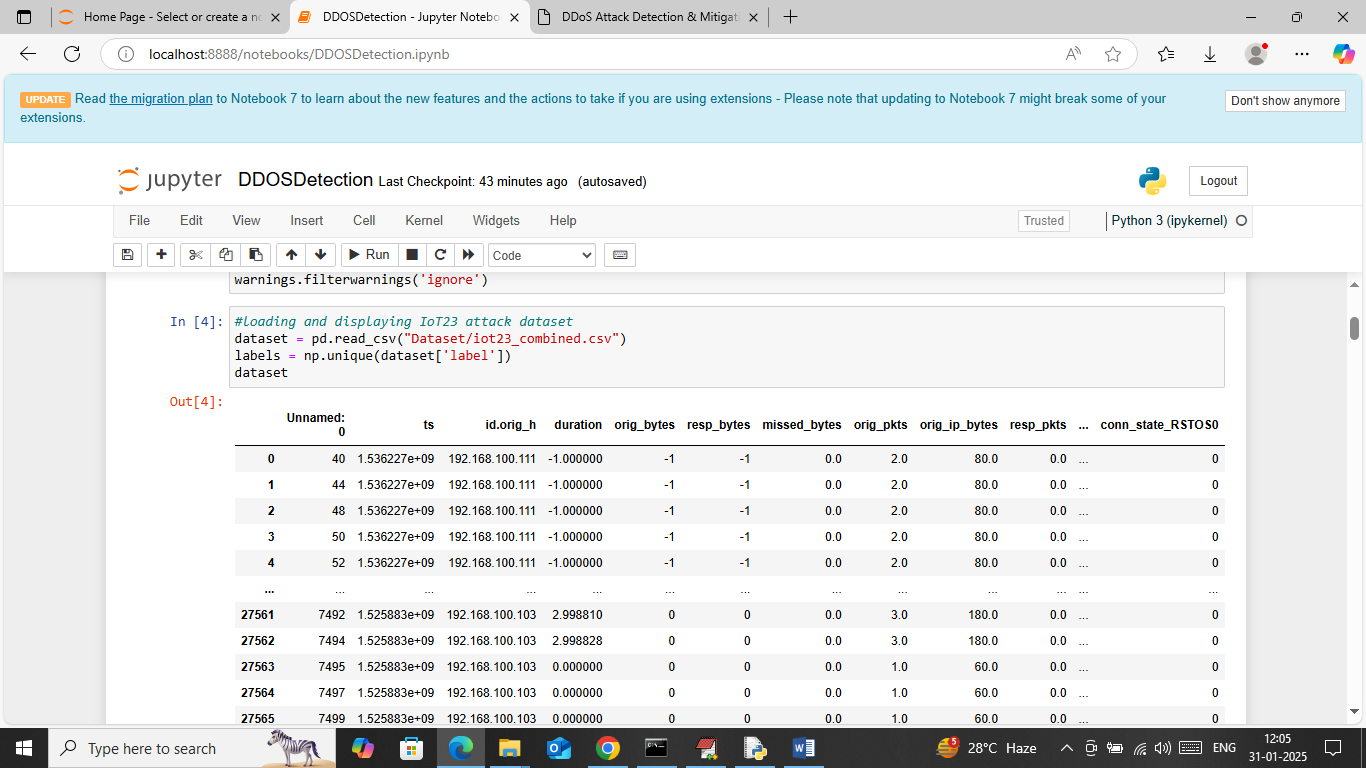
Upon attack detection this application will add IP address to firewall which will prevent that IP from future IOT access.

SCREEN SHOTS

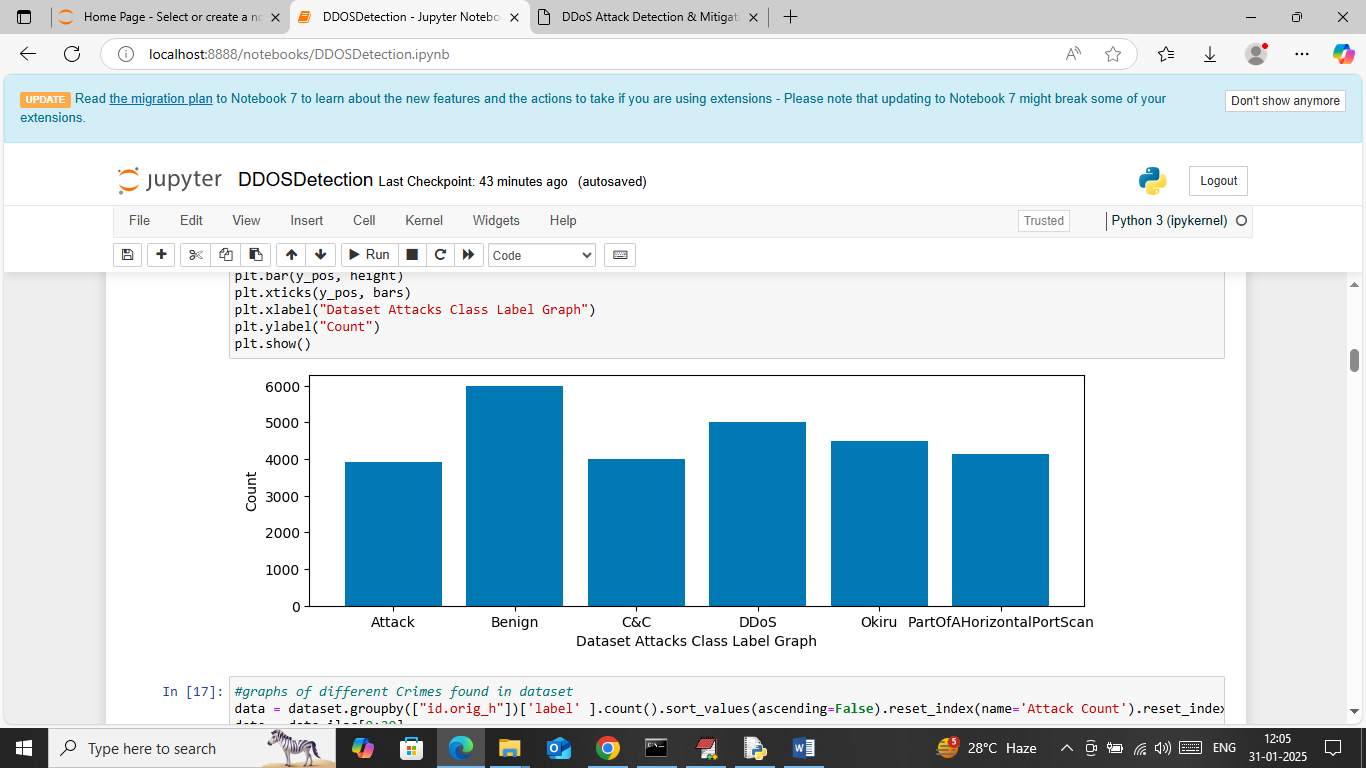
For training, testing, dataset processing we have utilize JUPYTER notebook and then employ web based flask framework to detect DDOD attack from test data. To run project double click on run.bat file to start JUPYTER notebook. Below are the code and output screen with blue colour comments



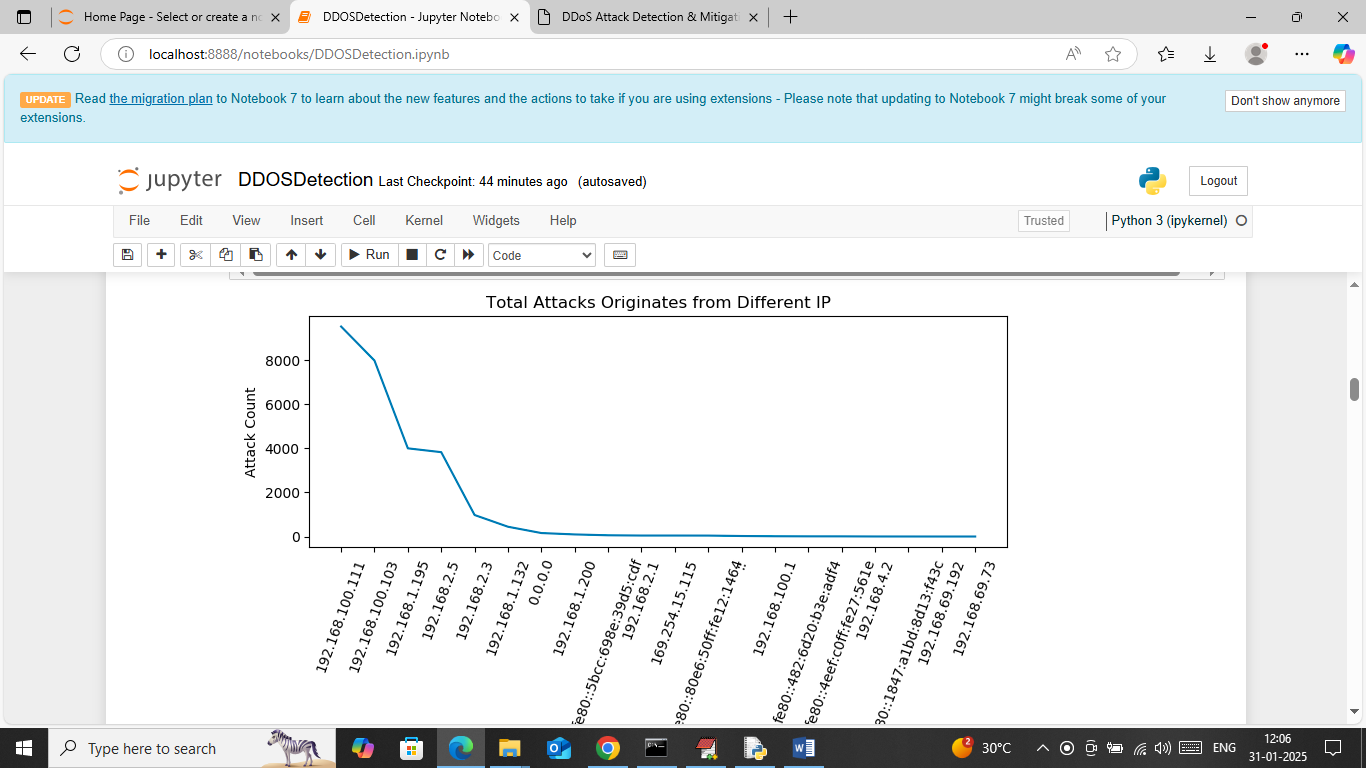
In above screen loading required python classes and packages



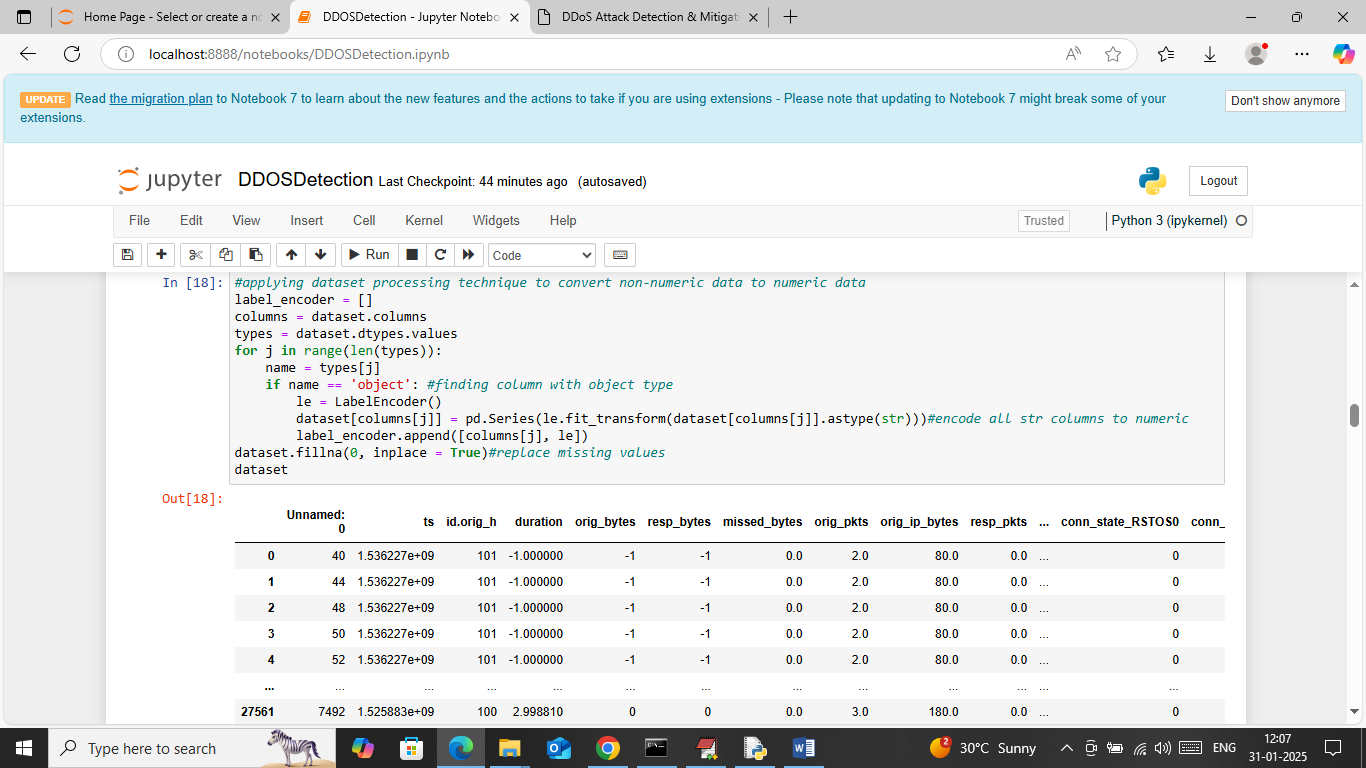
In above screen loading and displaying IOT23 dataset



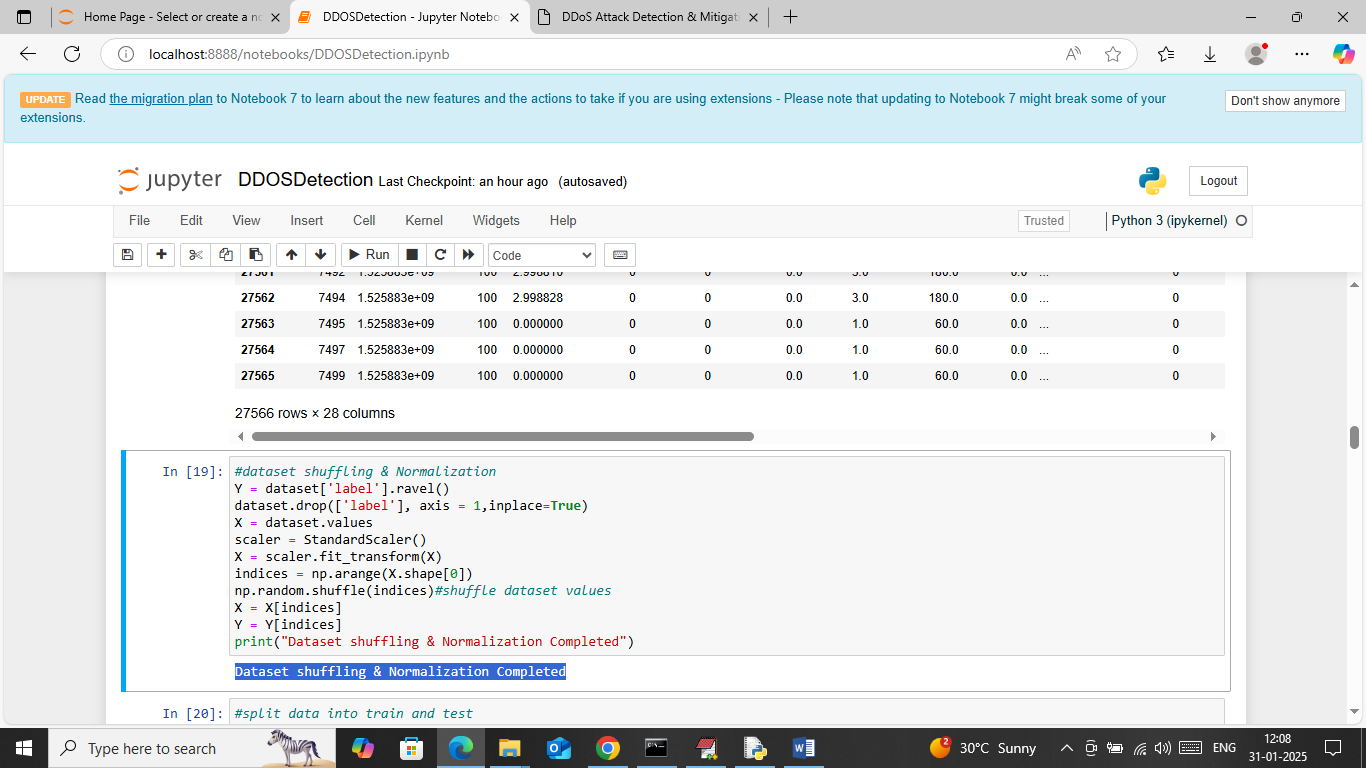
In above screen visualizing graph of different IOT attacks found in dataset where x-axis represents attack names and y-axis represents number of instances available in that attack category



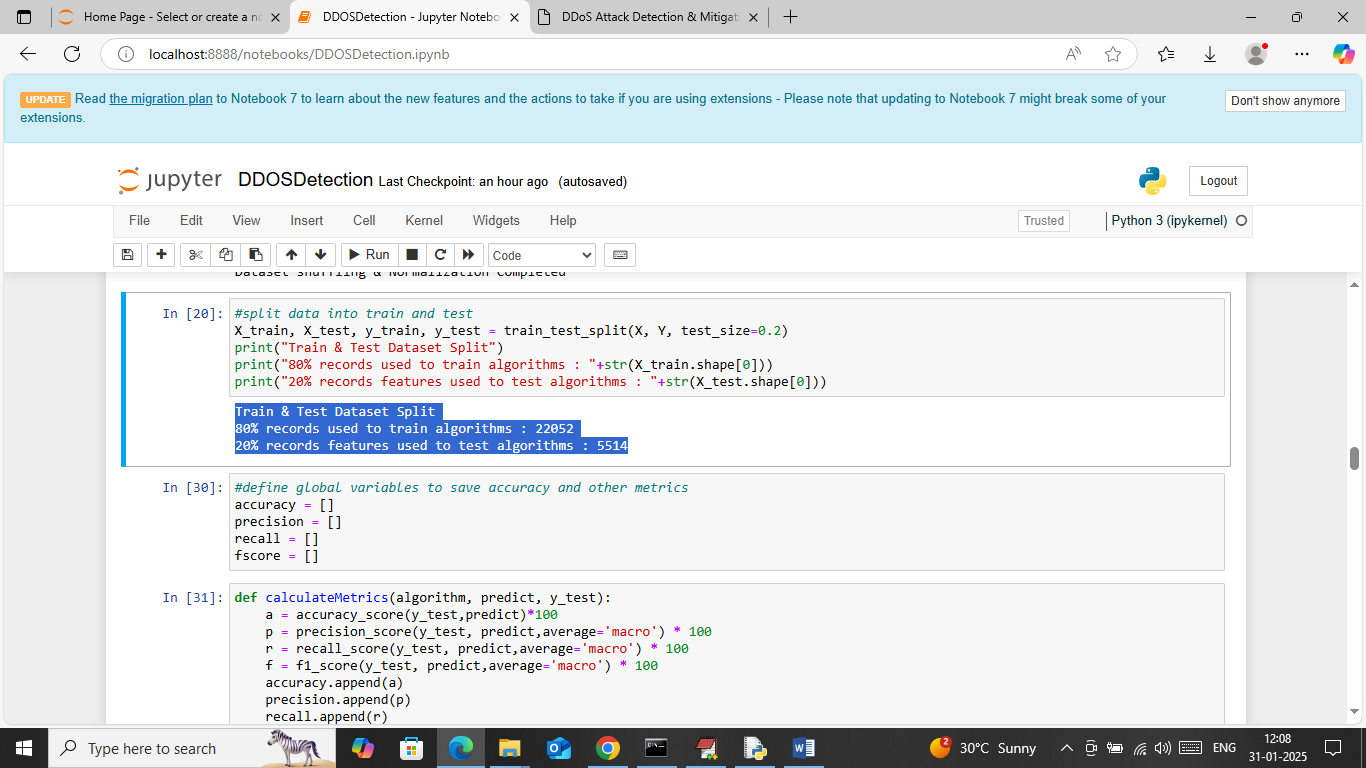
In above screen visualizing graph of most number of attacks originates from different IP. In above graph x-axis represents IP and y-axis represents number of attacks happen from that IP



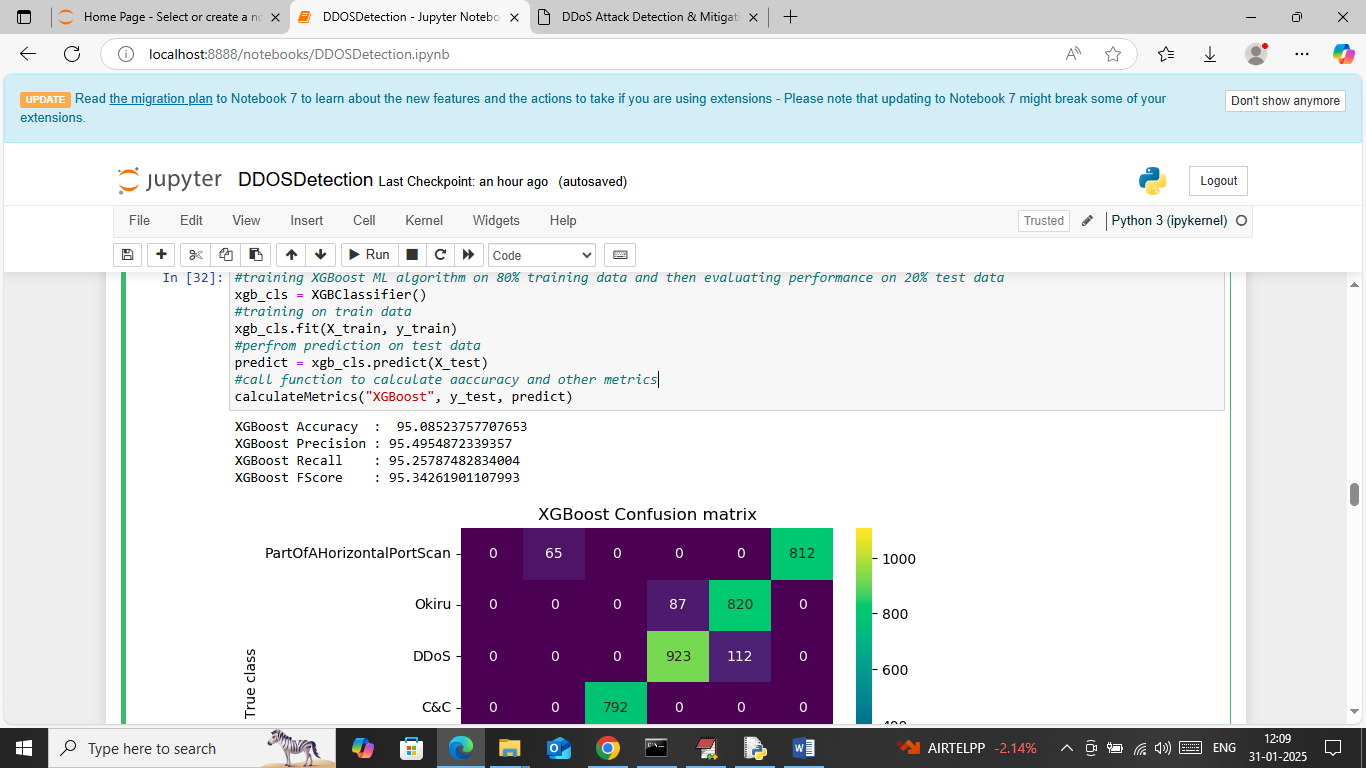
In above screen applying Label encoder class on dataset values to convert non-numeric data to numeric features and then replacing missing values with 0 and then can see cleaned dataset values



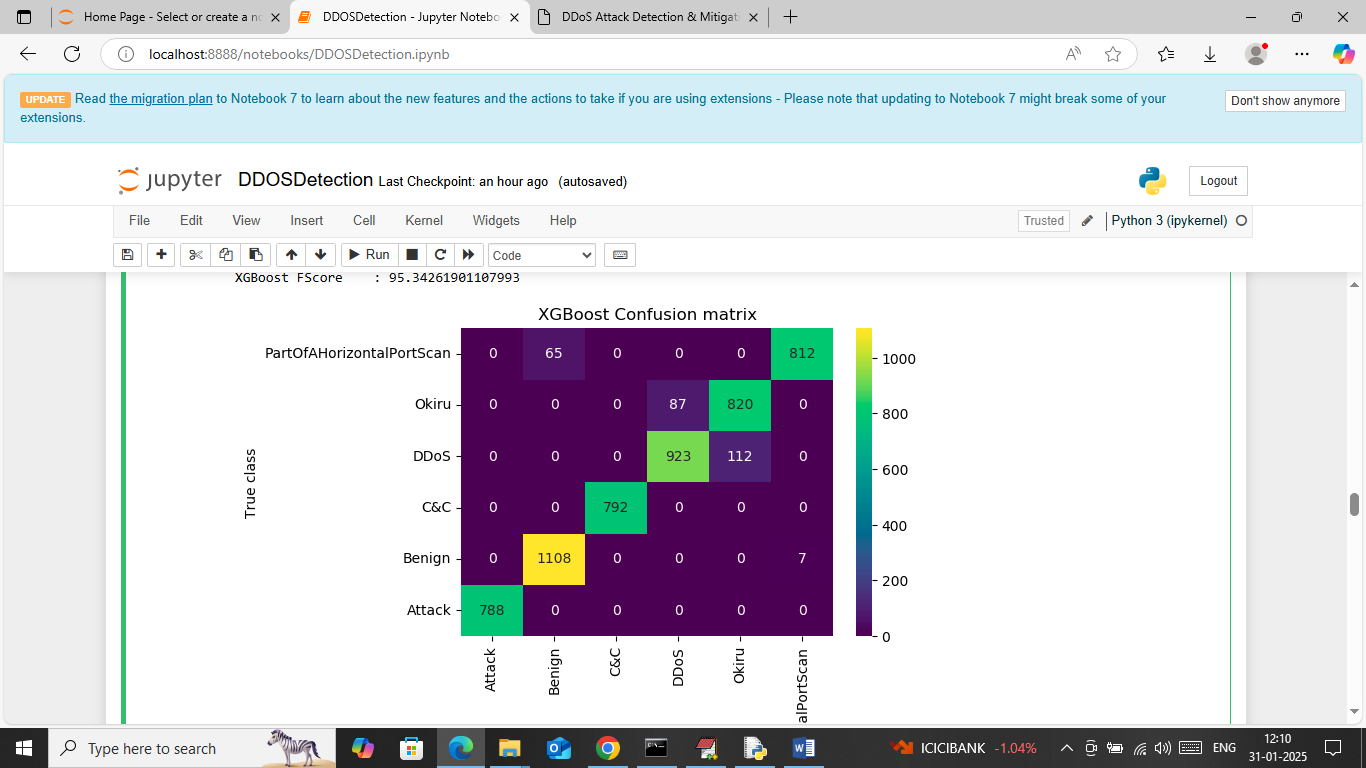
In above screen applying various dataset processing techniques such as shuffling and normalization



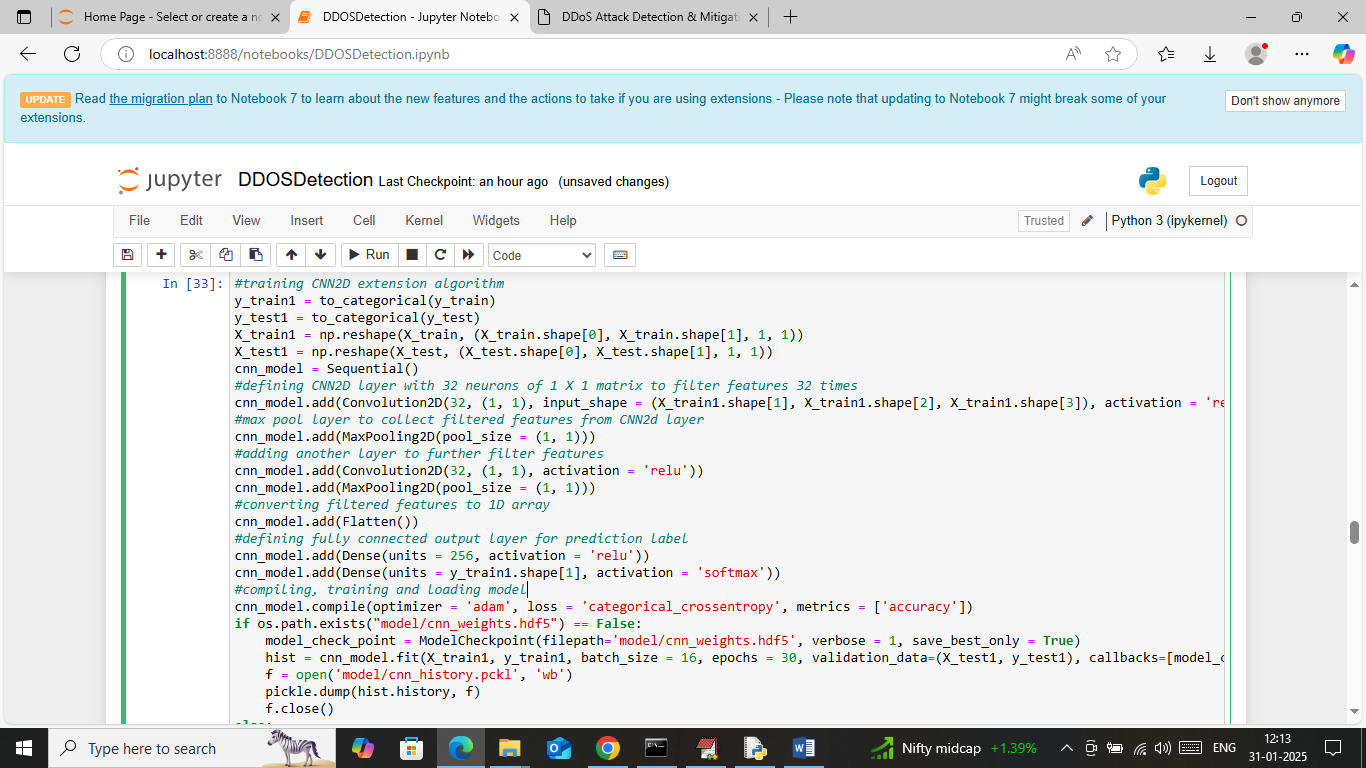
In above screen splitting dataset into train and test where application using 80% dataset for training and 20% for testing and then can see train and test size. In next blocks defining function to calculate accuracy and other metrics



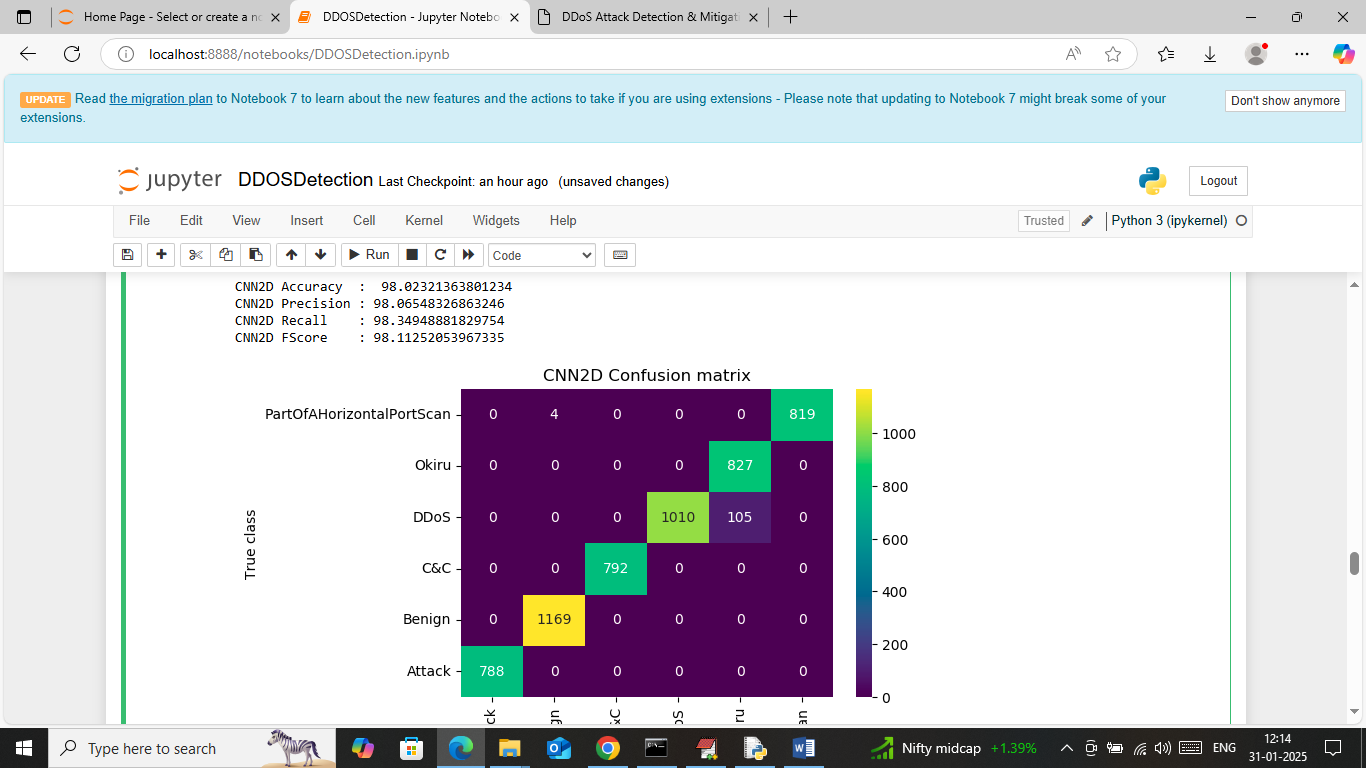
In above screen training XGBOOST algorithm on 80% training data and then performing prediction on 20% test data and then calculating prediction accuracy. In above screen XGBOOST got 95% accuracy on test and can see other metrics like precision, recall and FSCORE. Below is the confusion matrix classification graph



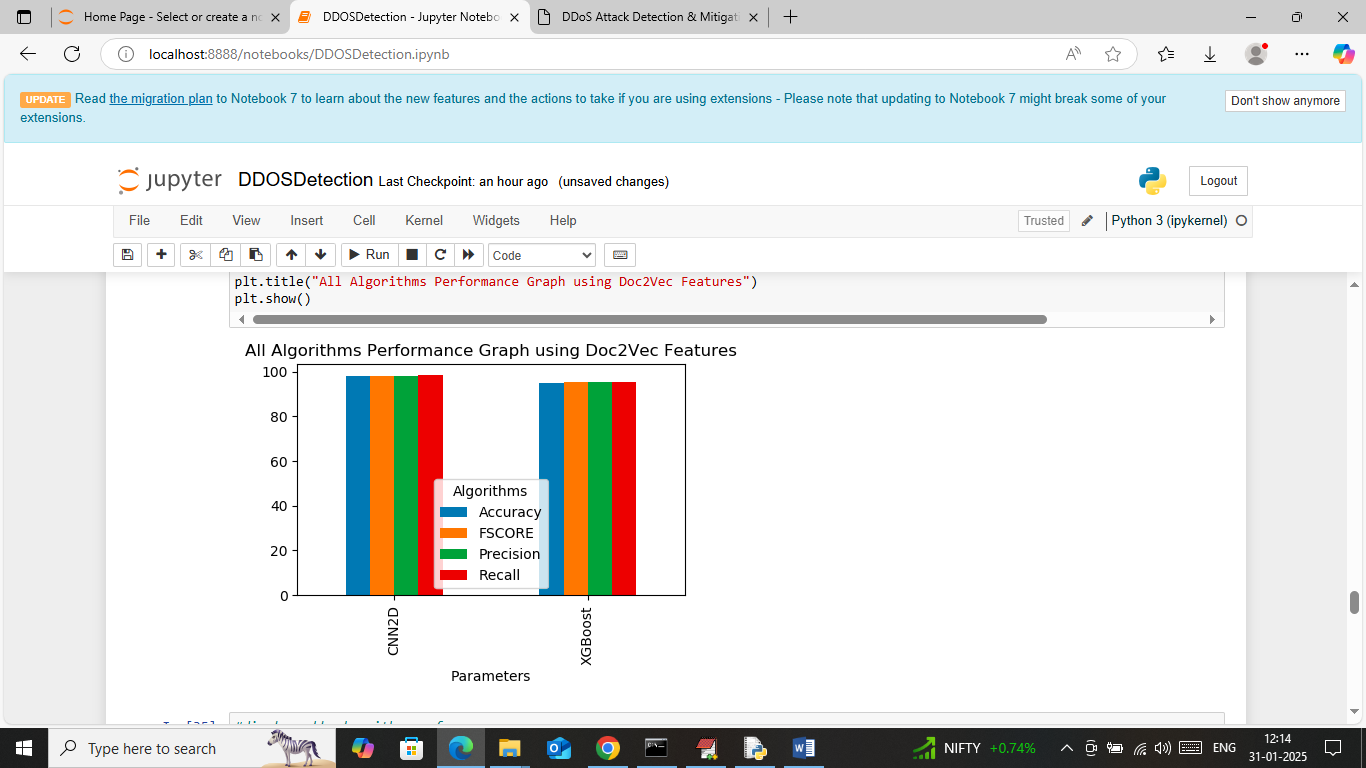
In above graph x-axis represents ‘Predicted Labels’ and y-axis represents True Labels and then all different colour boxes in diagonal represents correct prediction count and remaining blue boxes represents incorrect prediction count which are very few.



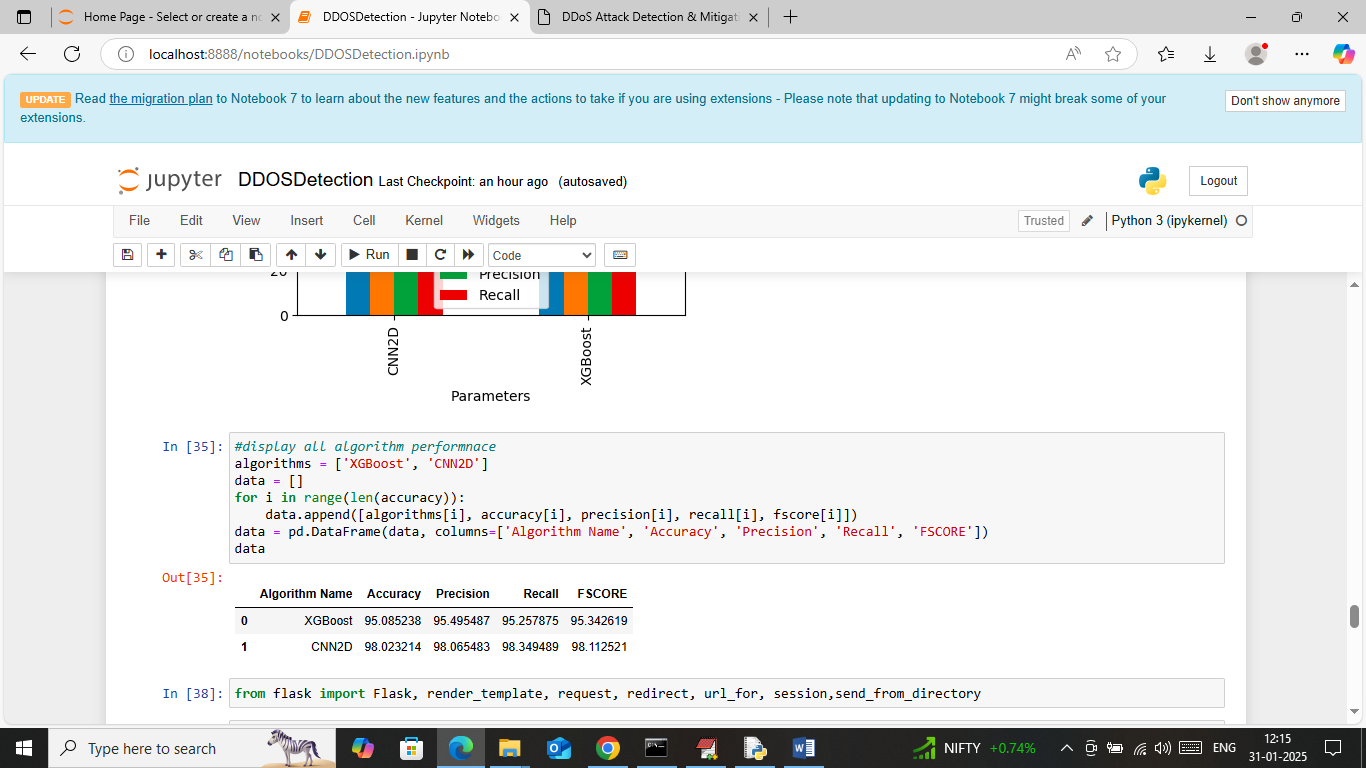
In above screen defining and training CNN2D algorithm and after executing this model will get below output



In above screen CNN got 98% accuracy and can see other metrics also

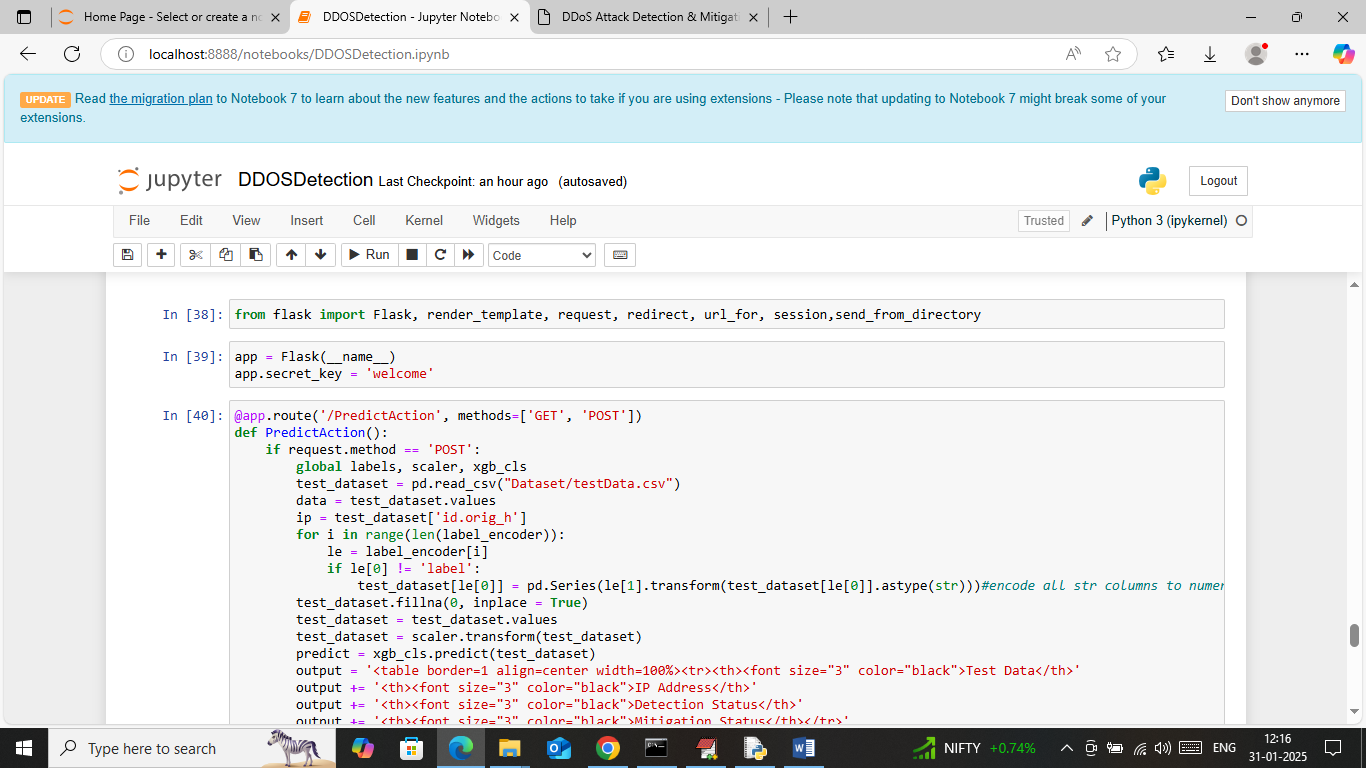


In above screen displaying comparison graph between both algorithms where x-axis represents algorithm names and y-axis represents accuracy and other metrics in different colour bars.

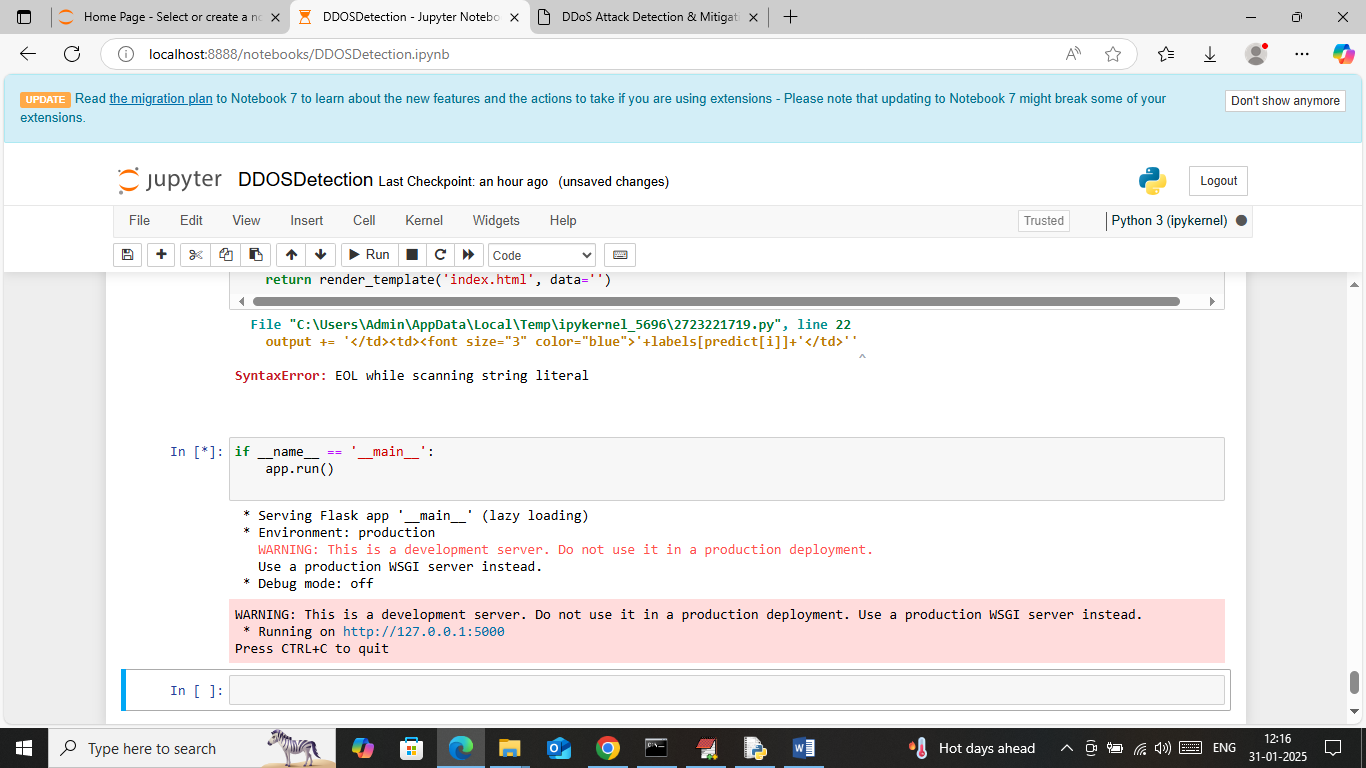


In above screen displaying both algorithm performance in tabular format. So in above screen we have done all data training and experiments execution.

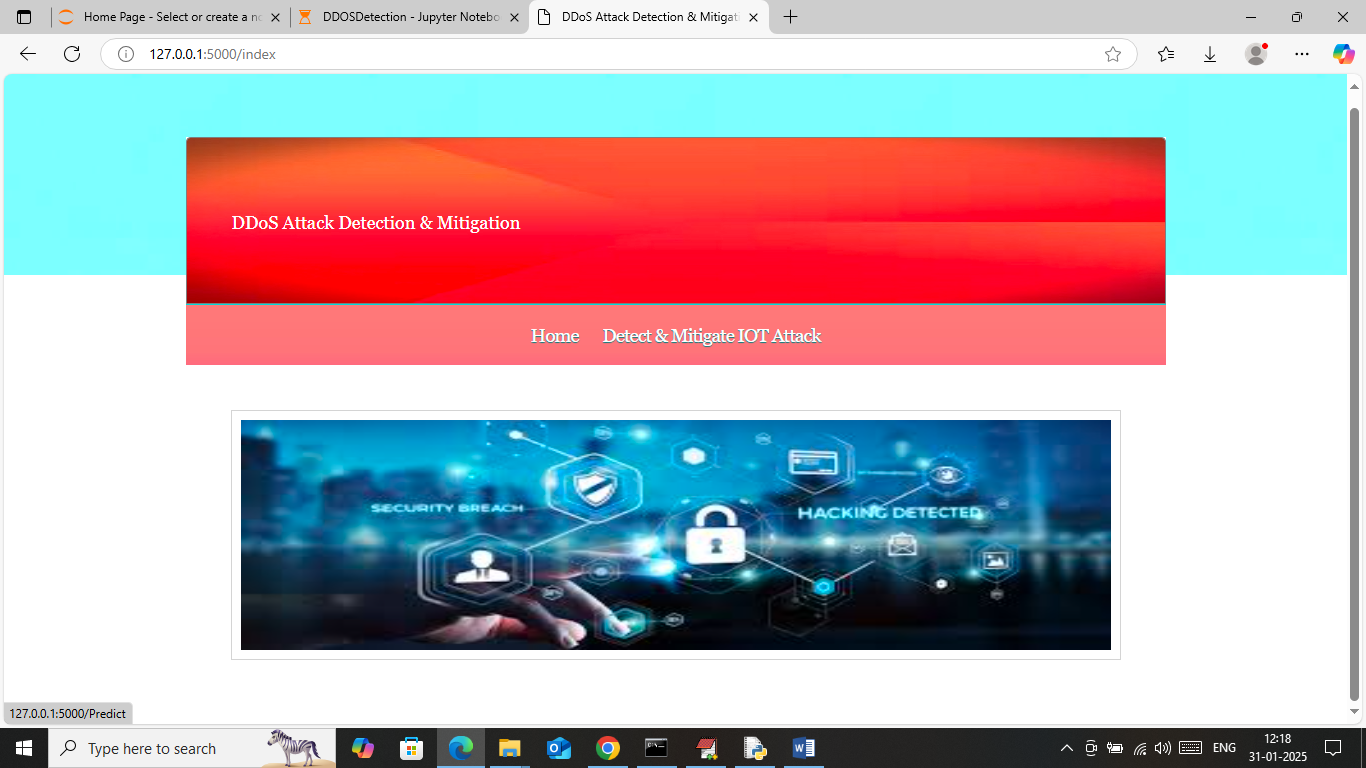
Now run all flask block code to mitigate attack from web page



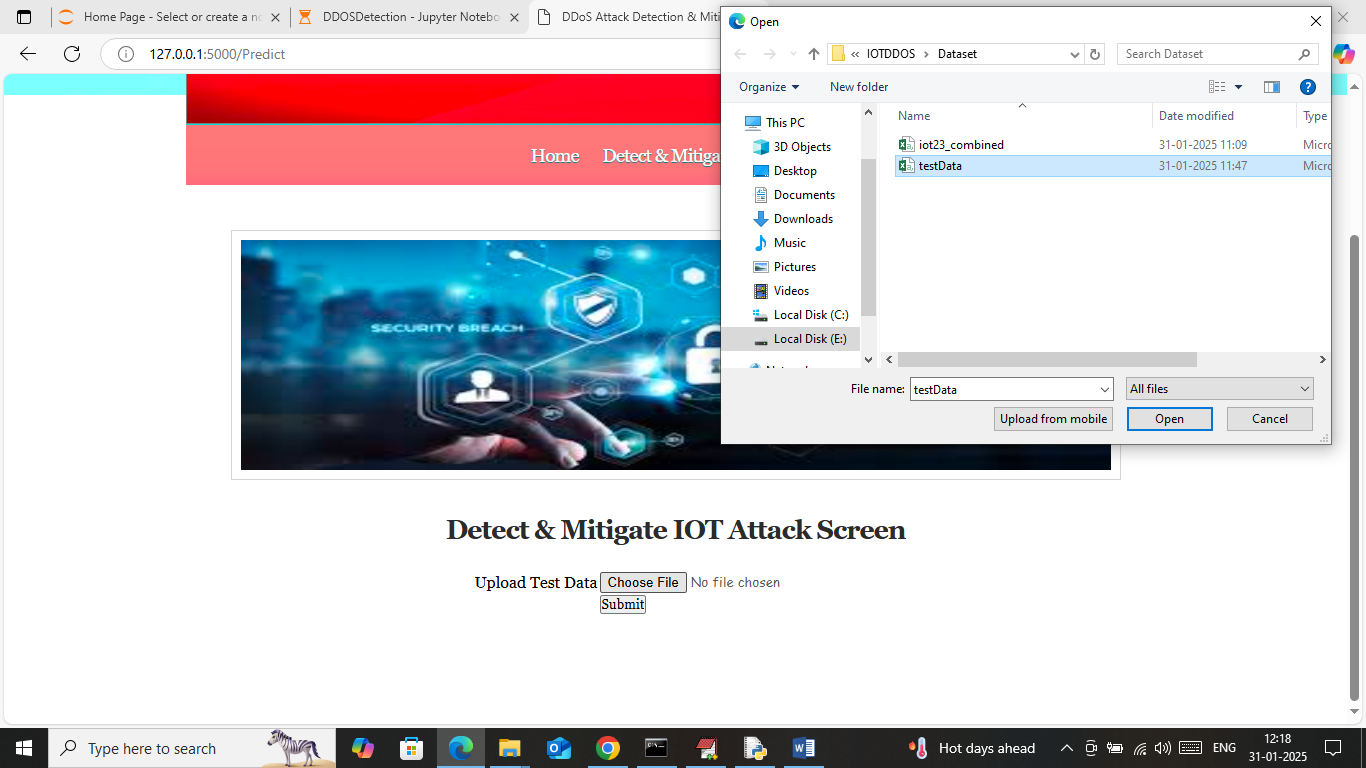
In above screen run all flask blocks to start flask server and then will get below page



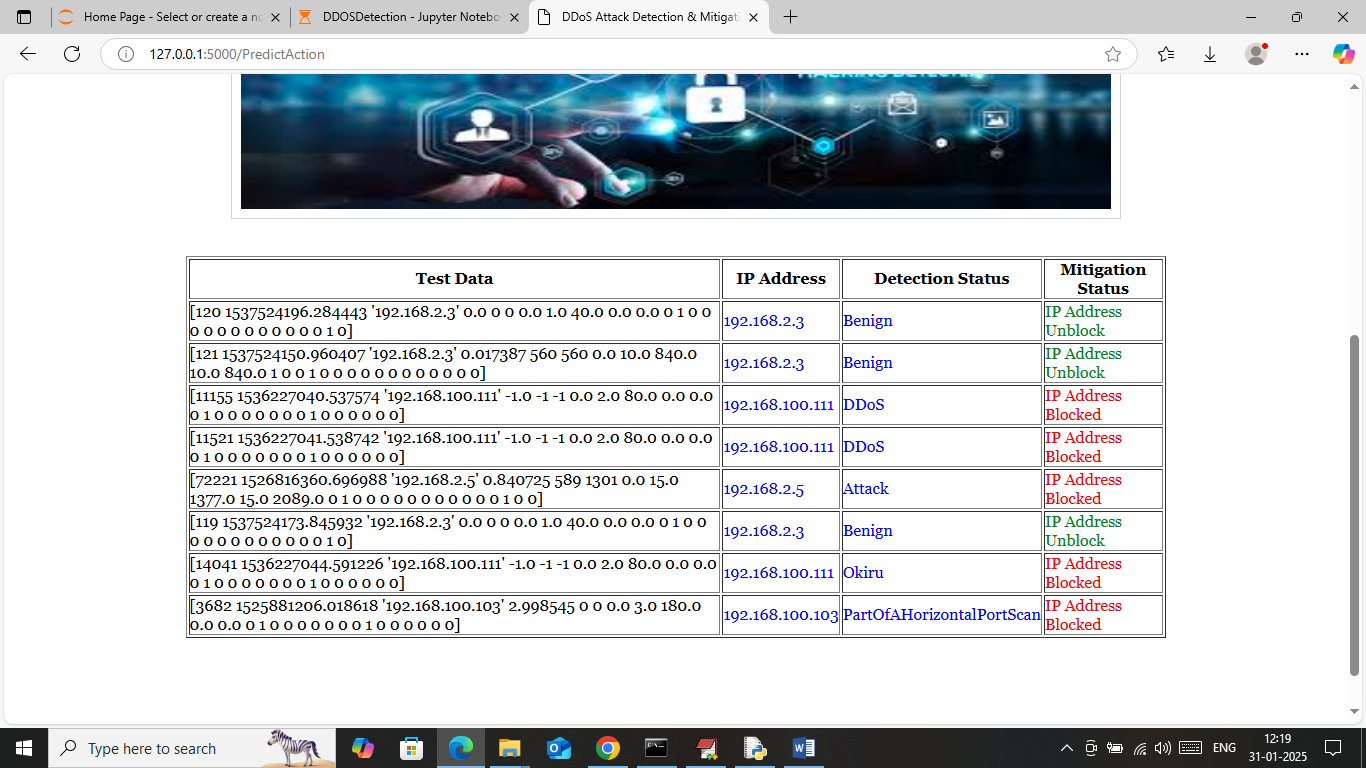
In above screen flask server started and now open browser and enter URL as <http://127.0.0.1:5000/index> and then press enter key to get below page



In above screen click on ‘Detect & Mitigate IOT Attack’ link to get below page



In above screen select and upload test data file which contains IOT network request data and then press button to get below page



In above screen in first column can see network request data and in second column can see SOURCE IP address which is sending request to IOT. In 3rd column can see predicted output as ‘Benign (normal) or attack’ and based on detected attack that IP will get blocked.

So by using above ML and DL algorithm you can detect and mitigate all possible IOT attacks.