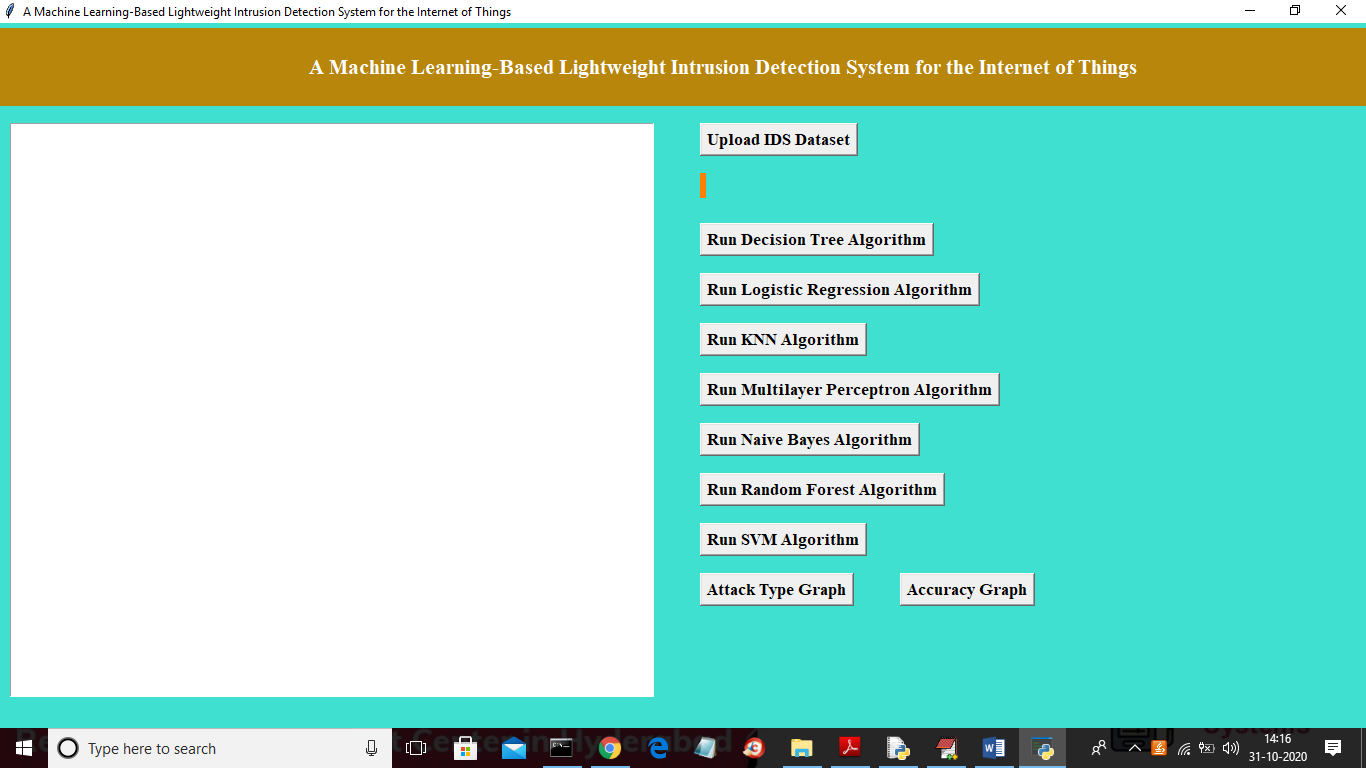
A Machine Learning-Based Lightweight Intrusion Detection System for the Internet of Things

In this paper author is building light weight intrusion detection system for IOT networks using machine learning algorithms. Author has evaluated performance of various machine learning algorithms such as SVM, Random Forest, Decision Tree, Naïve Bayes, Logistic Regression, KNN and Multilayer Perceptron and in all algorithms Decision Tree and KNN is giving better performance. To reduce training time author is using filter based features selection algorithm which will select important attributes from training dataset and the attributes whose correlation value is less than given threshold will be removed out.

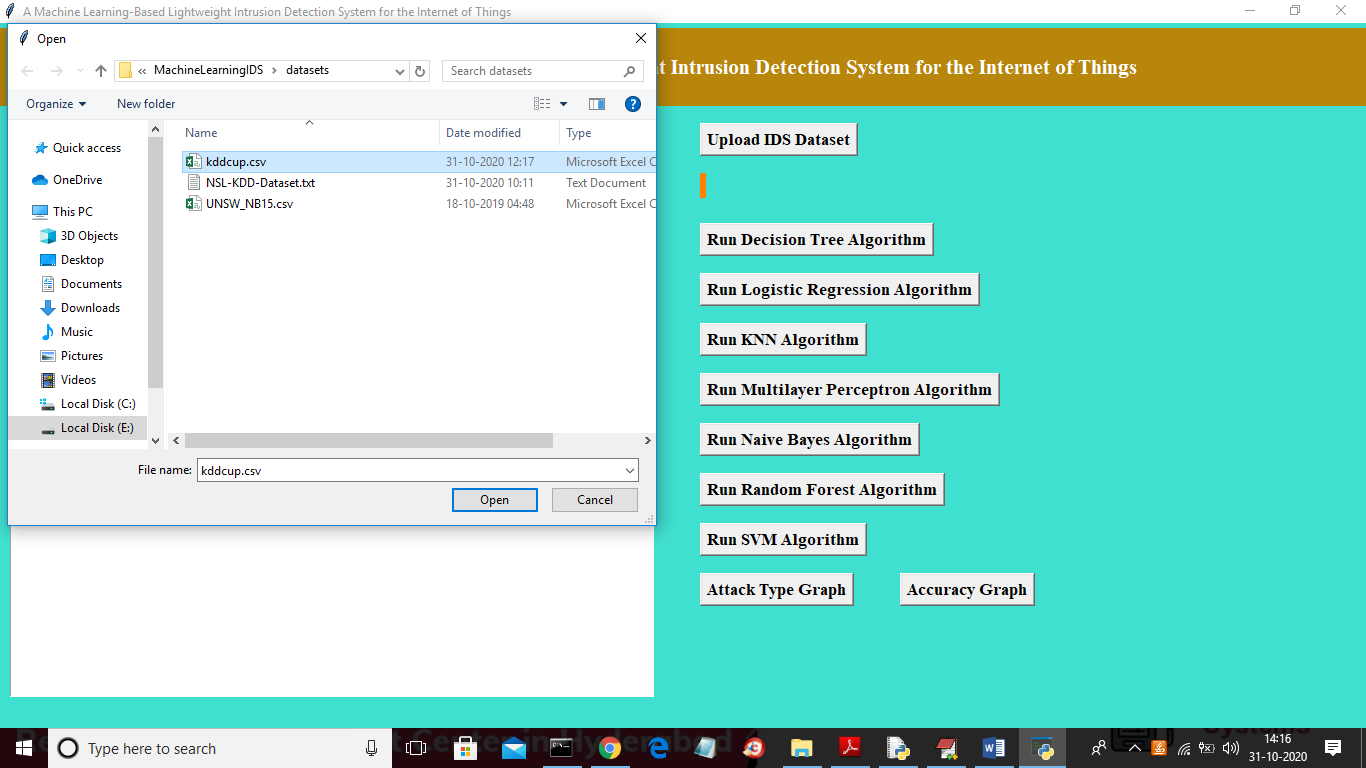
To implement this project author has used 3 datasets such as KDDCUP, NSLKDD and UNSW\_NB15 and this dataset contains various attacks as Denial of Service, R2L, U2R, Probe and many more. Other details can be read from paper.

Screen shots

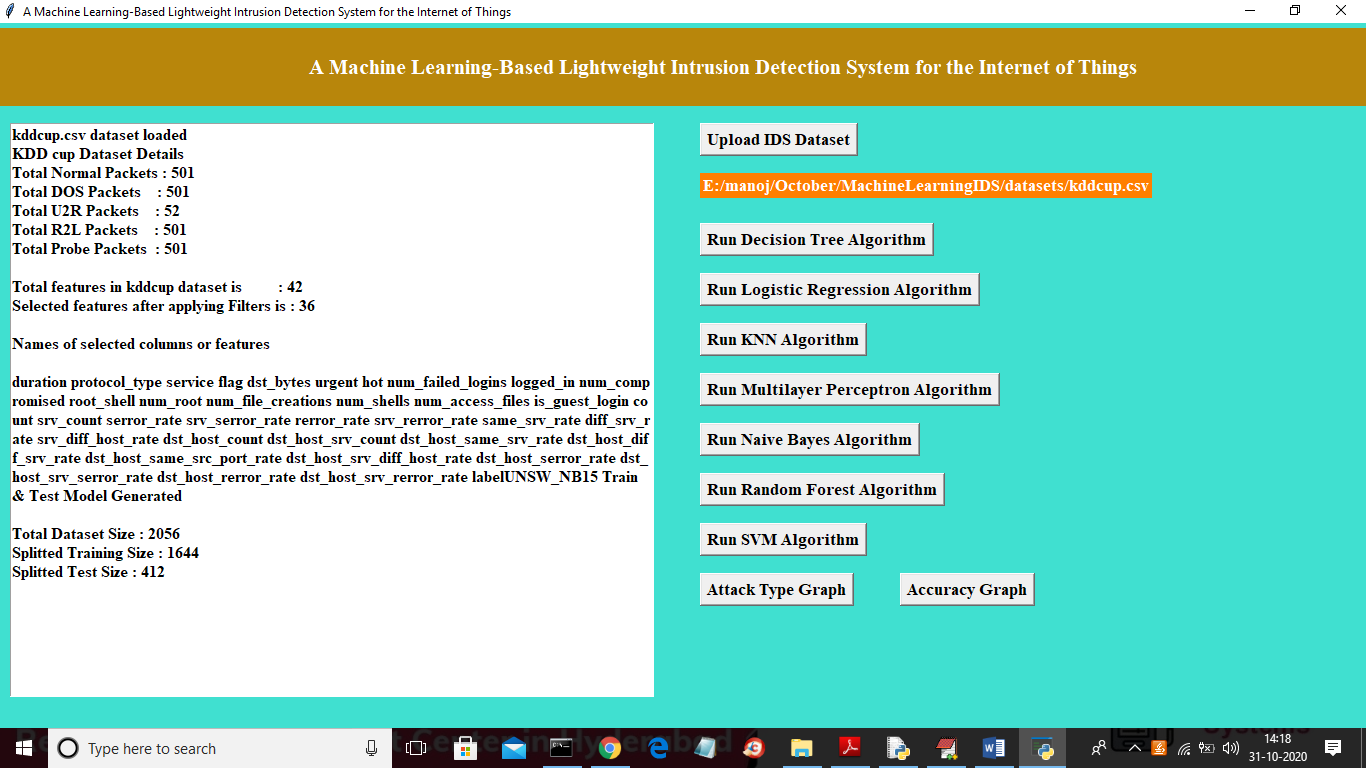
To run project double click on ‘run.bat’ file to get below screen



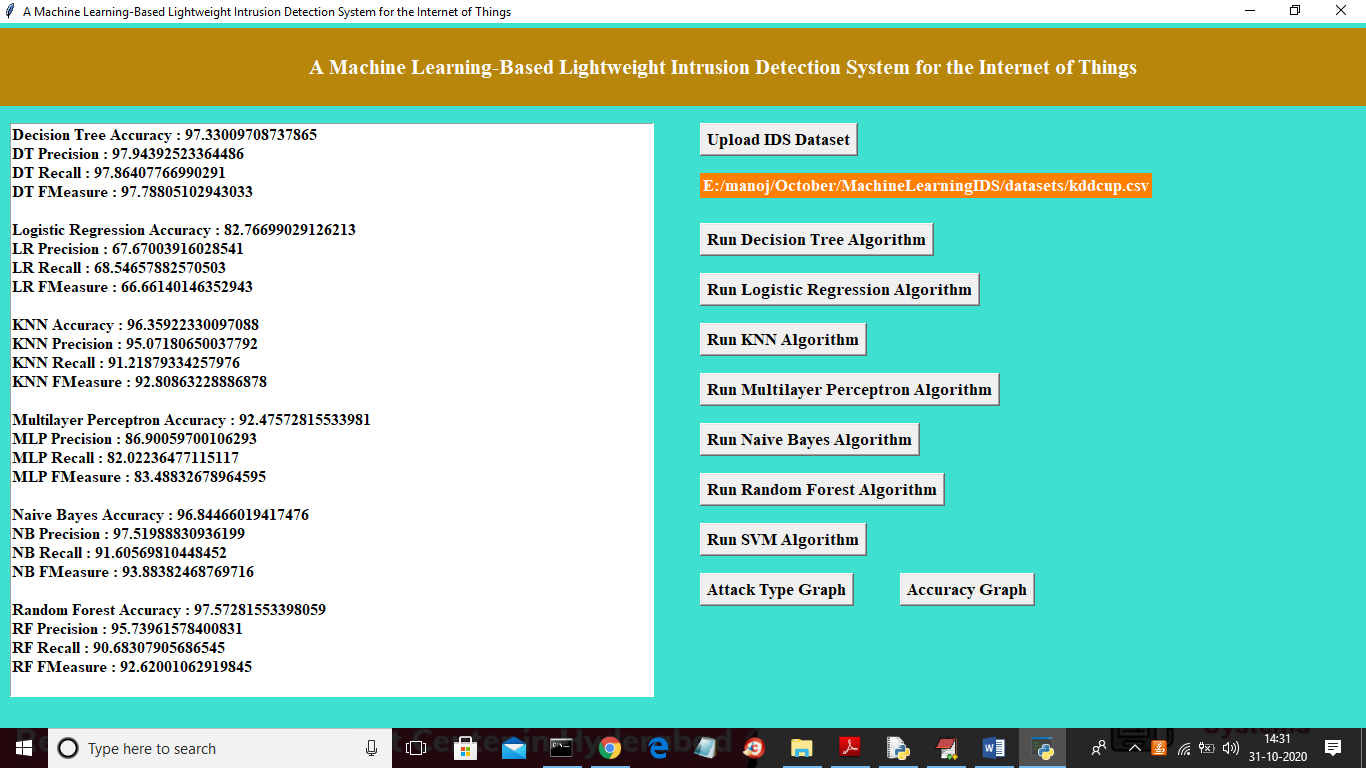
In above screen click on ‘Upload IDS Dataset’ button and upload any one dataset



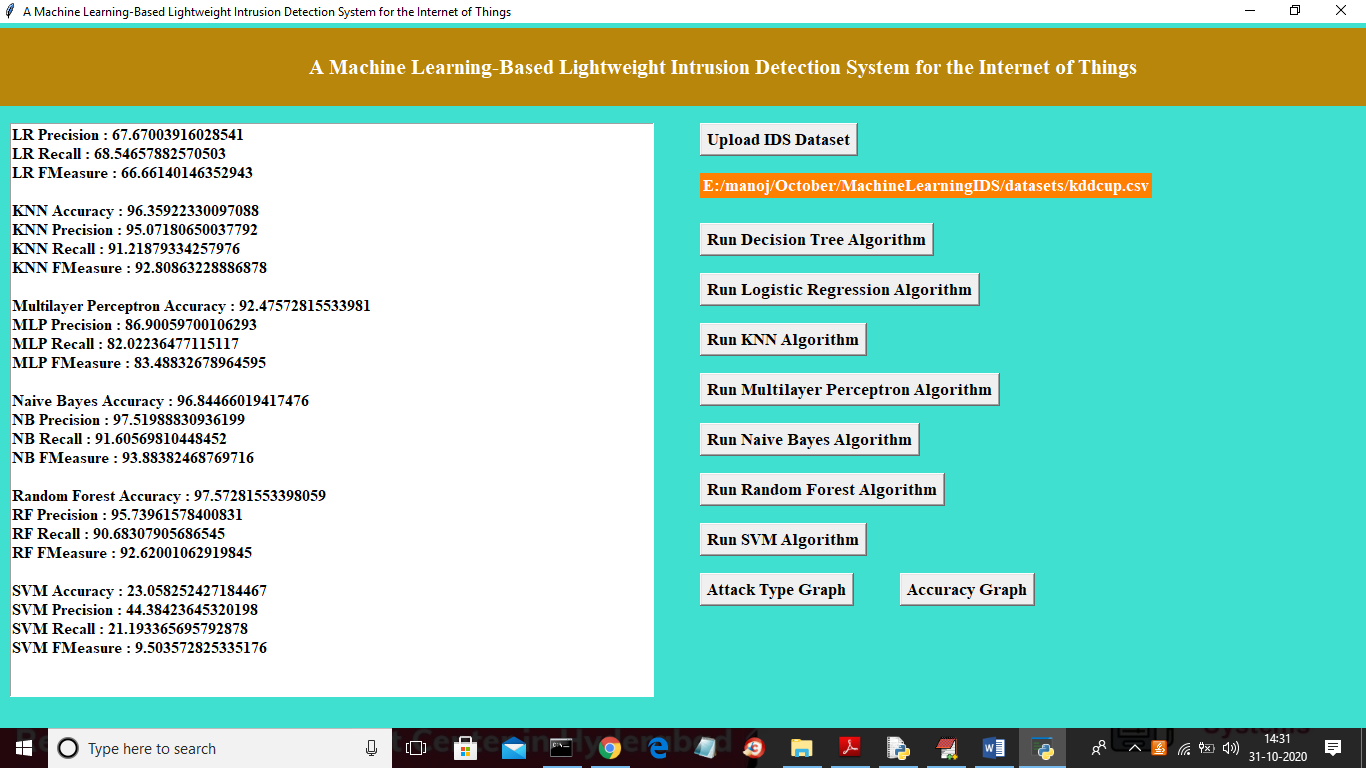
In above screen selecting and uploading ‘kddcup.csv’ dataset and click on ‘Open’ button to load dataset and then application will perform dataset preprocesing and then apply feature selection algorithm and then split dataset into train and test part.



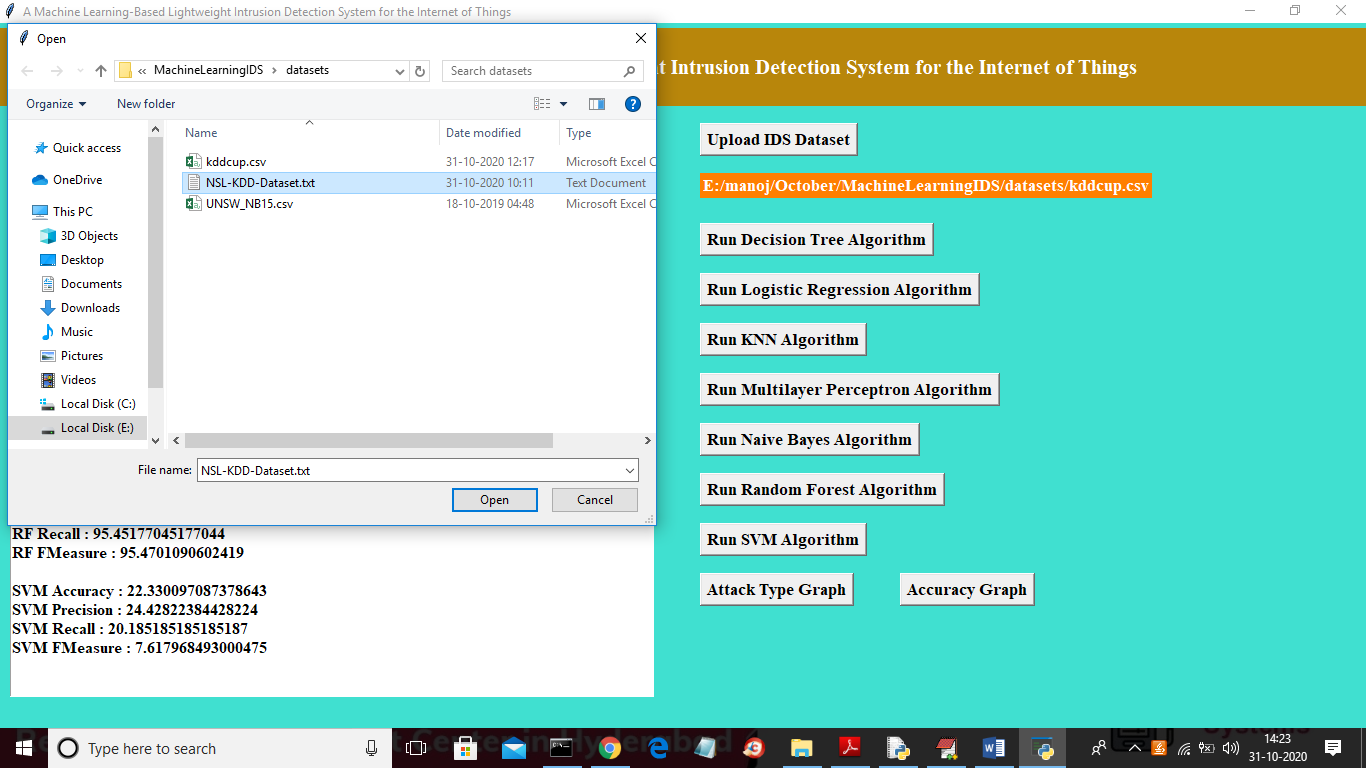
In above screen application displaying various attacks size available in dataset and then displaying total features and then displaying selected features and then displaying names of all selected features and then displaying total dataset size and total records used for training and testing. Now both train and test data ready and now run all algorithms by clicking on each button and then calculate accuracy, precision, recall and FScore on test data.



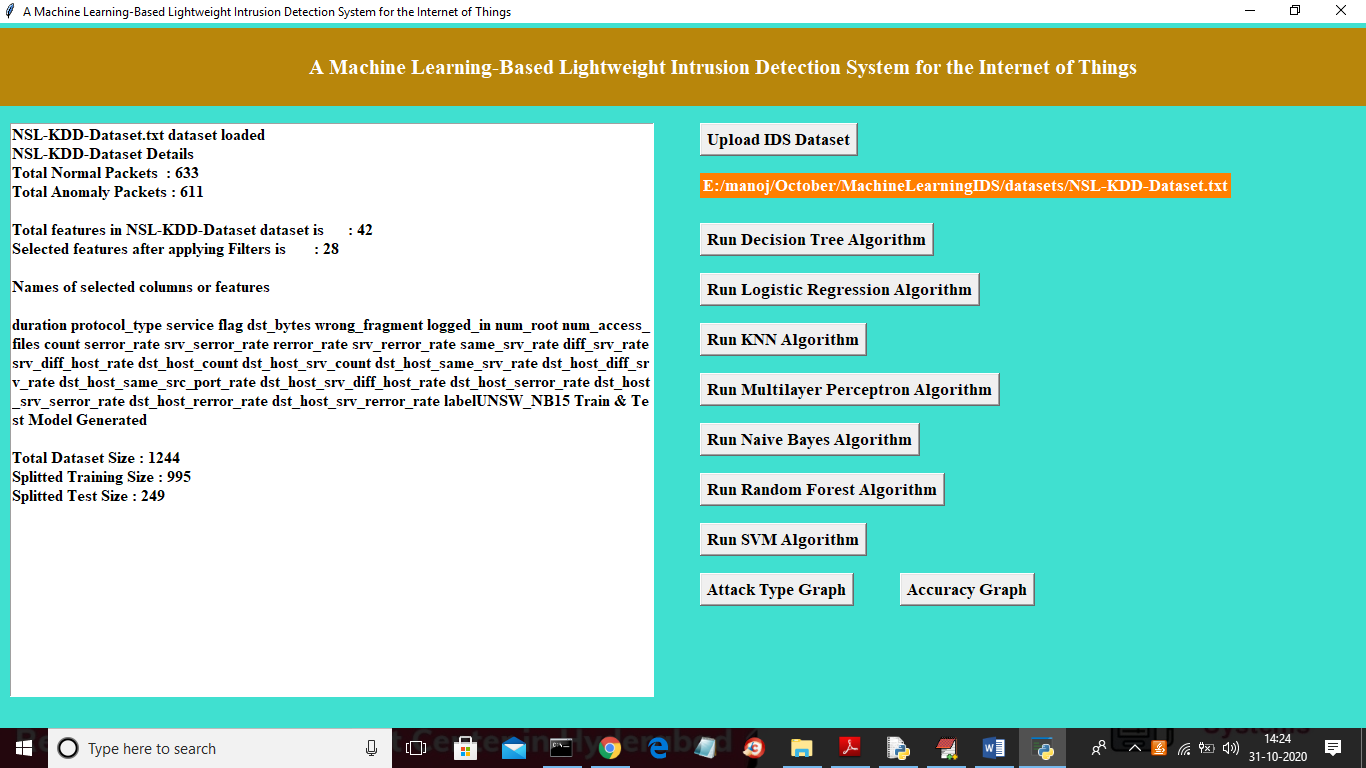
In above screen after clicking on each button we algorithm will generate model by using trained data and then classify test data to calculate accuracy and other metrics. In above screen decision tree is giving better performance. Below screen showing SVM result for KDDCUP dataset



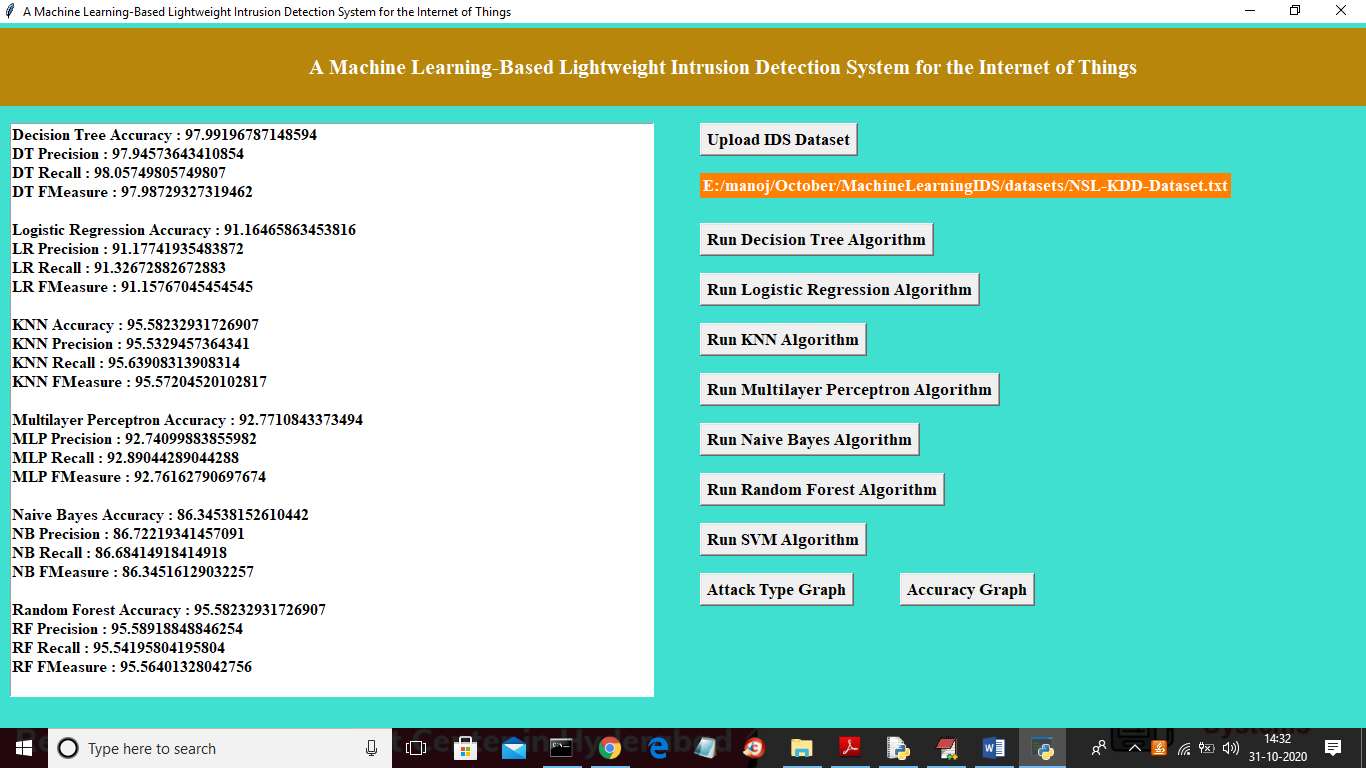
Now upload NSLKDD dataset and run all algorithms on that dataset



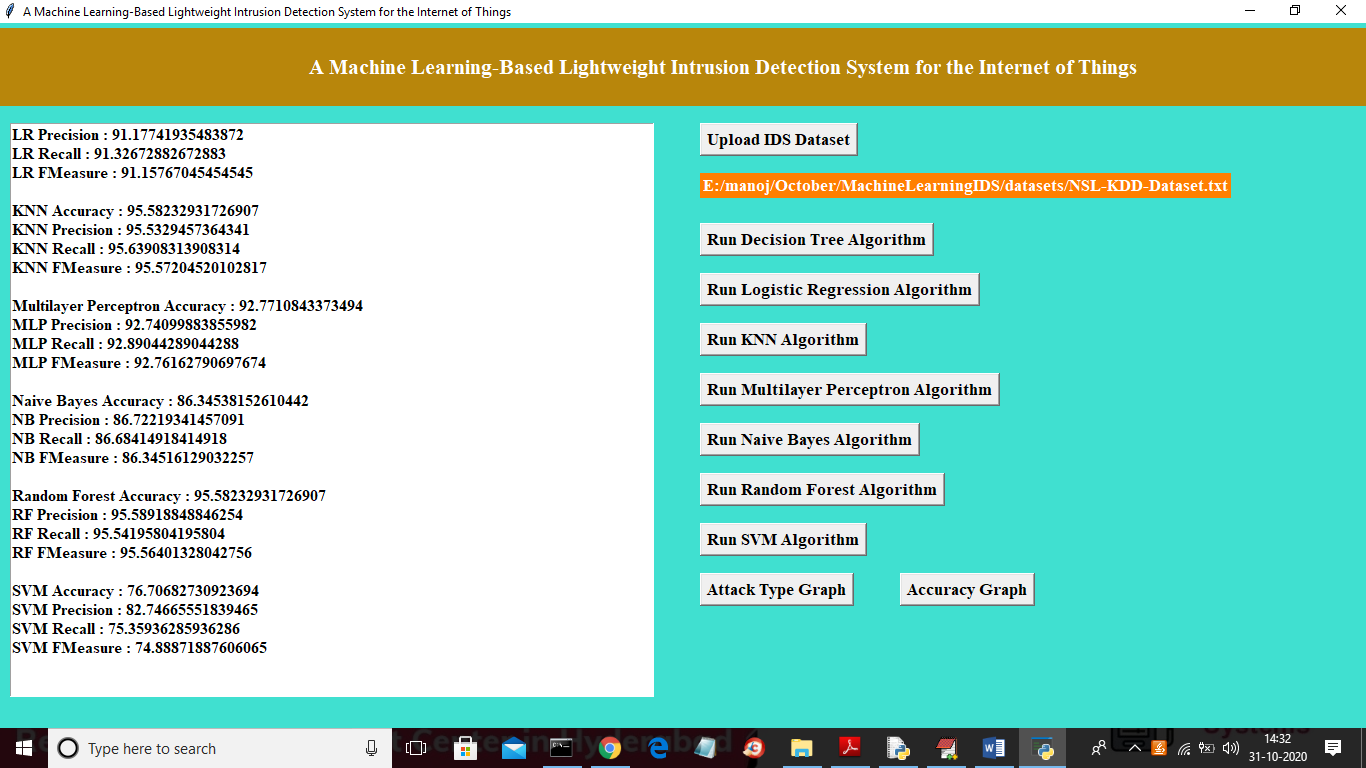
In above screen by clicking on first button uploading ‘NSL-KDD-Dataset.txt’ file and now click on ‘Open’ button to load dataset and to get below screen



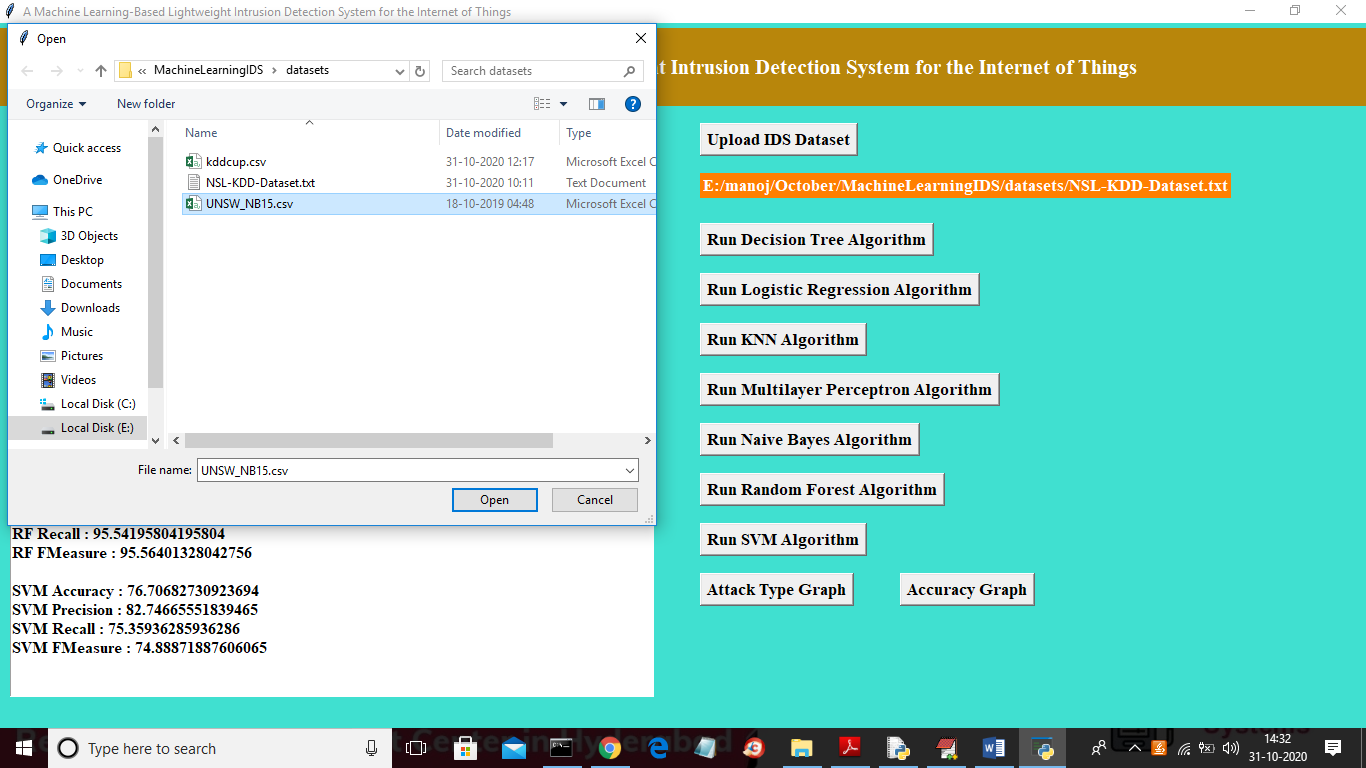
In above screen we can see all dataset details from NSL KDD data and now click on each algorithm button to calculate its accuracy



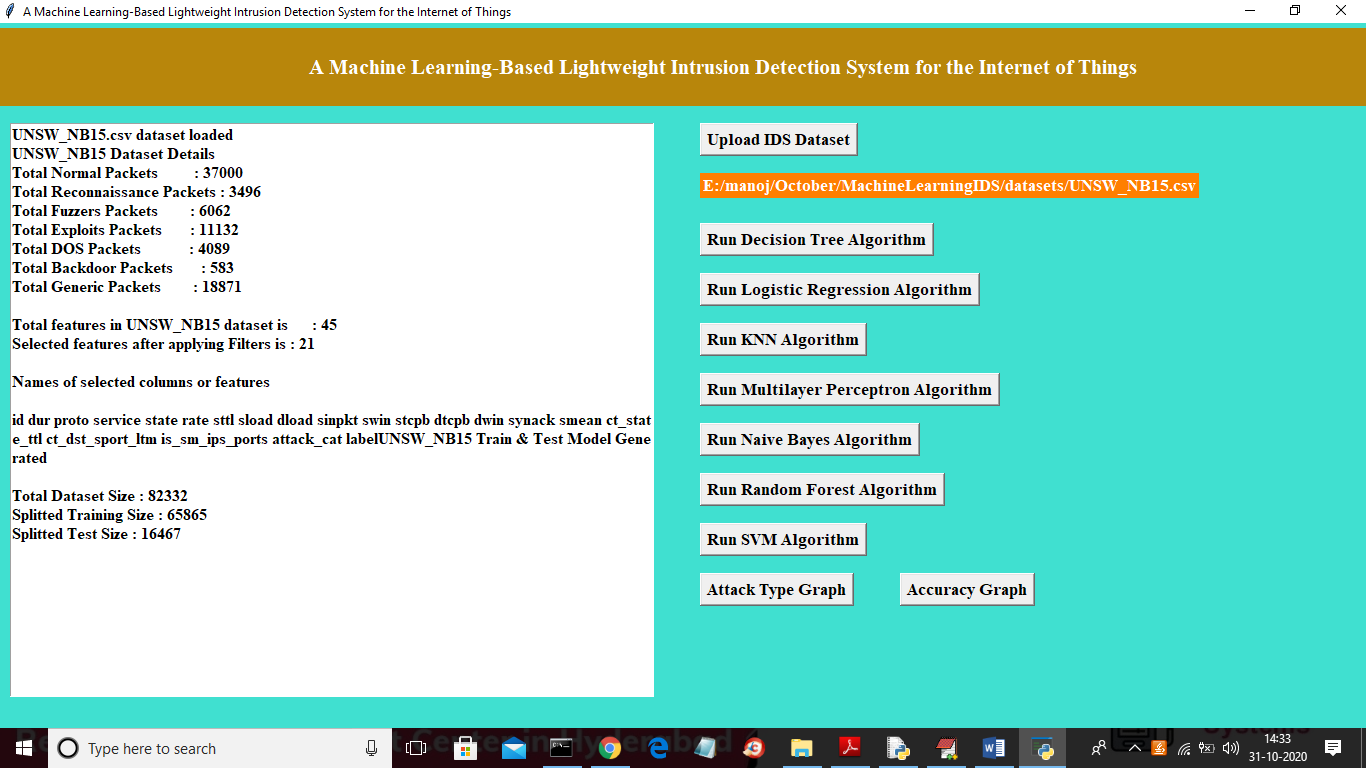
In above screen we can see algorithms accuracy for NSL KDD dataset and below is the SVM accuracy for NSL KDD



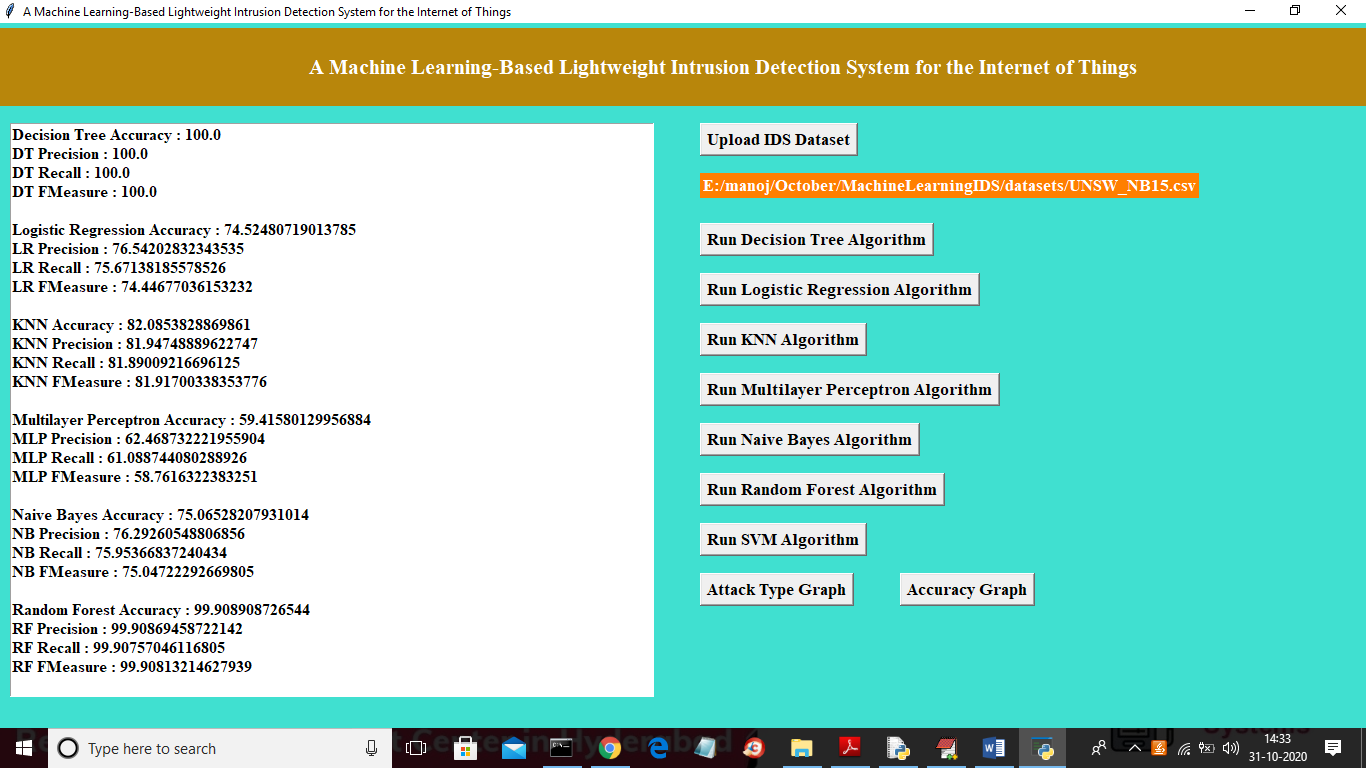
Now once again click on first button and upload UNSW dataset



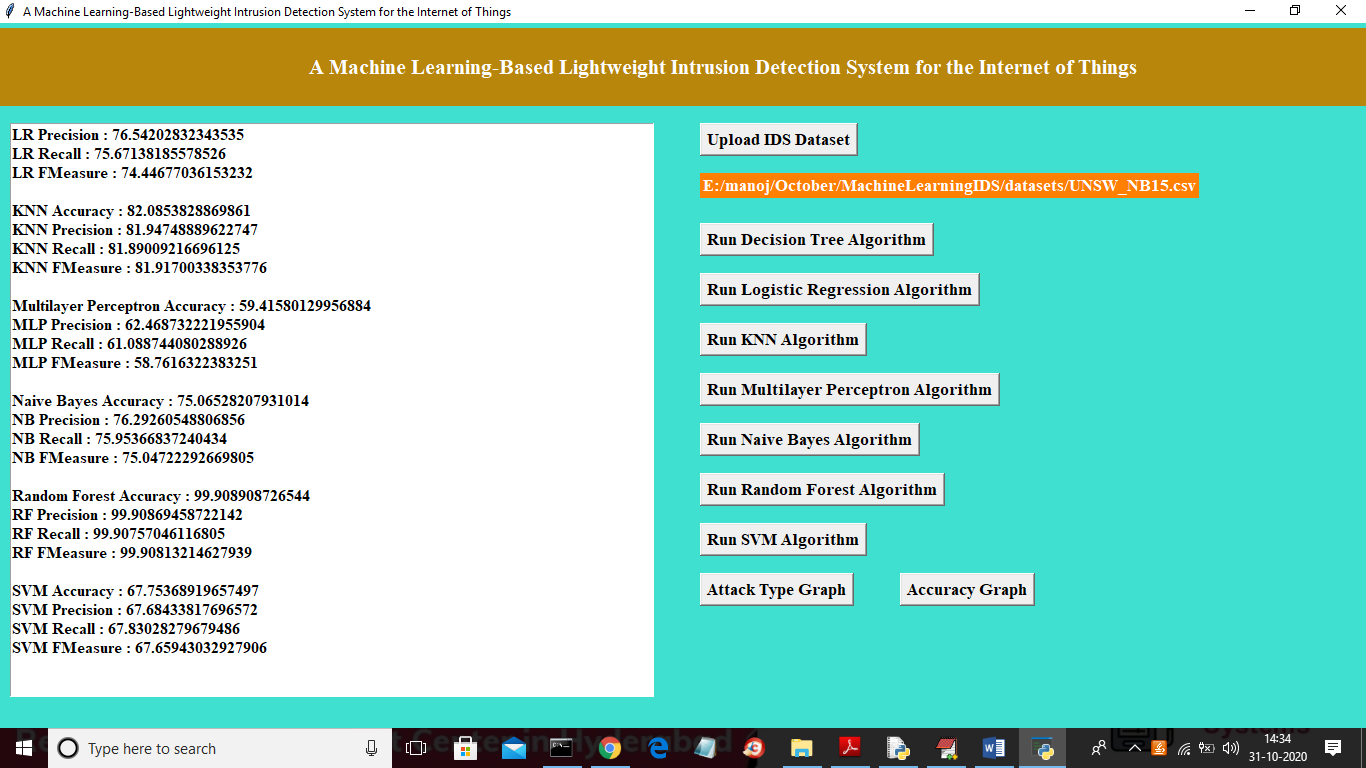
In above screen uploading third dataset called ‘UNSW\_NB15.csv’ file and now click on ‘Open’ button to load dataset and to get below screen



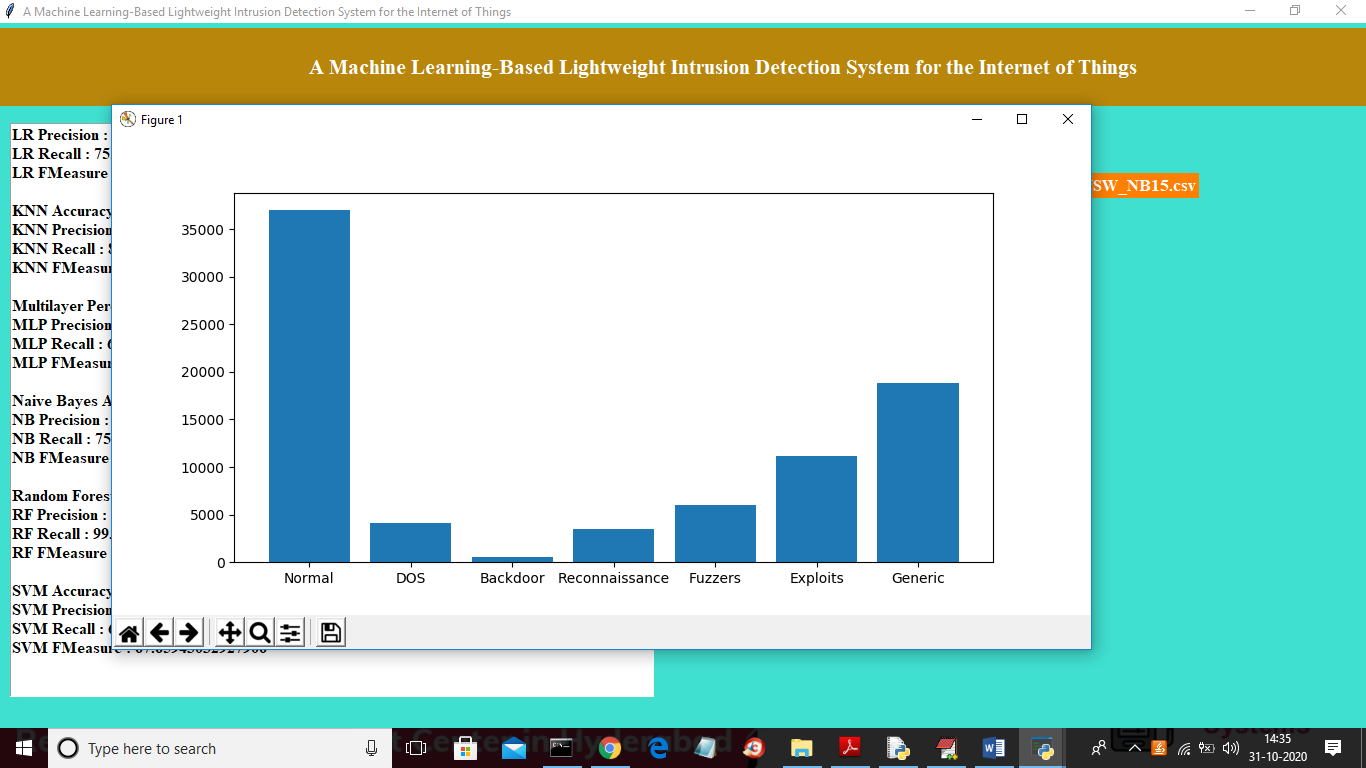
In above screen we can see all details from UNSW dataset and now both train and test data is ready and now click on each algorithm button to calculate accuracy



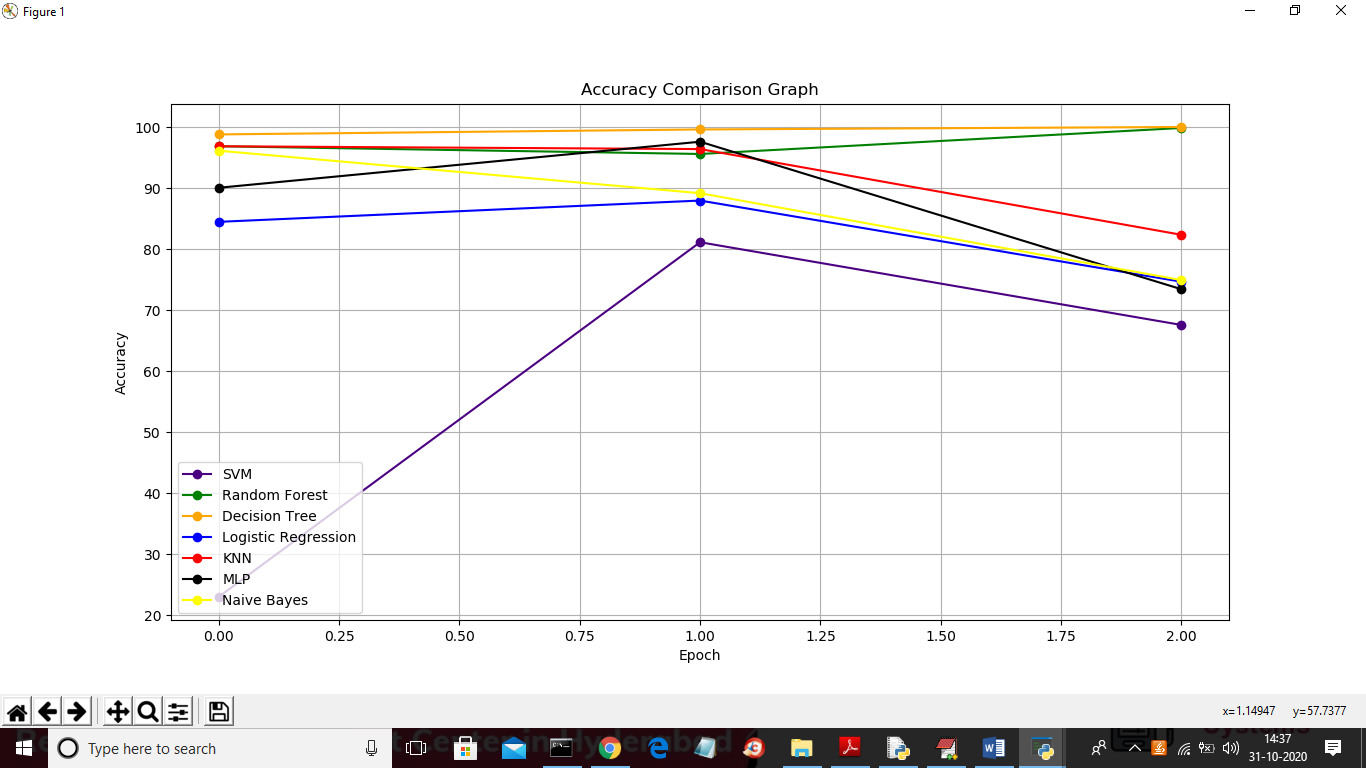
Now in below screen we can see SVM accuracy for UNSW dataset



In all datasets and in all algorithms Decision Tree and KNN is giving better results and now click on ‘Attack Type Graph’ button to get below graph



In above graph x-axis represents attack name and y-axis represents count of each attack and now click on ‘Accuracy Graph’ button to get below accuracy graph



In above graph x-axis represents 3 datasets and y-axis represents accuracy of each algorithm for that dataset. From all algorithms we can decision tree is giving good performance.