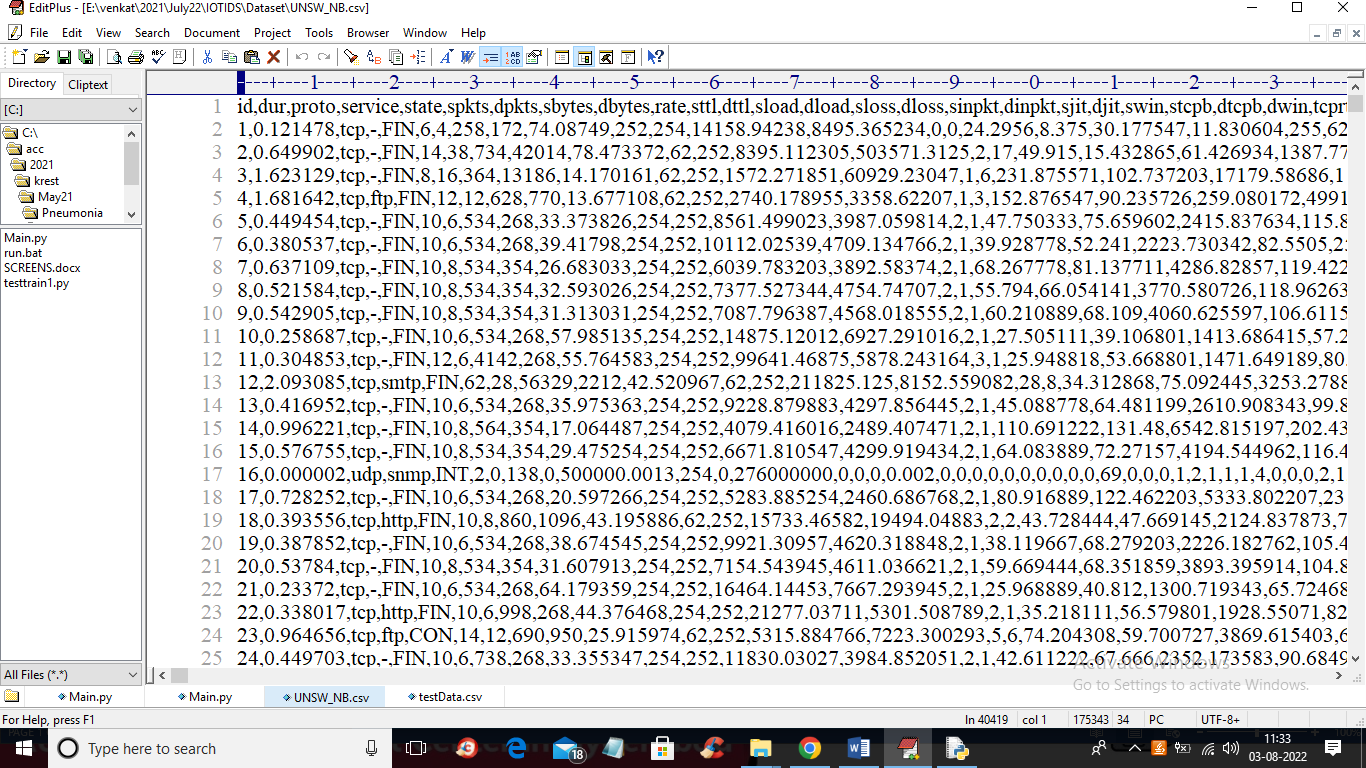
DL-IDF: Deep Learning Based Intrusion Detection Framework in Industrial Internet of Things

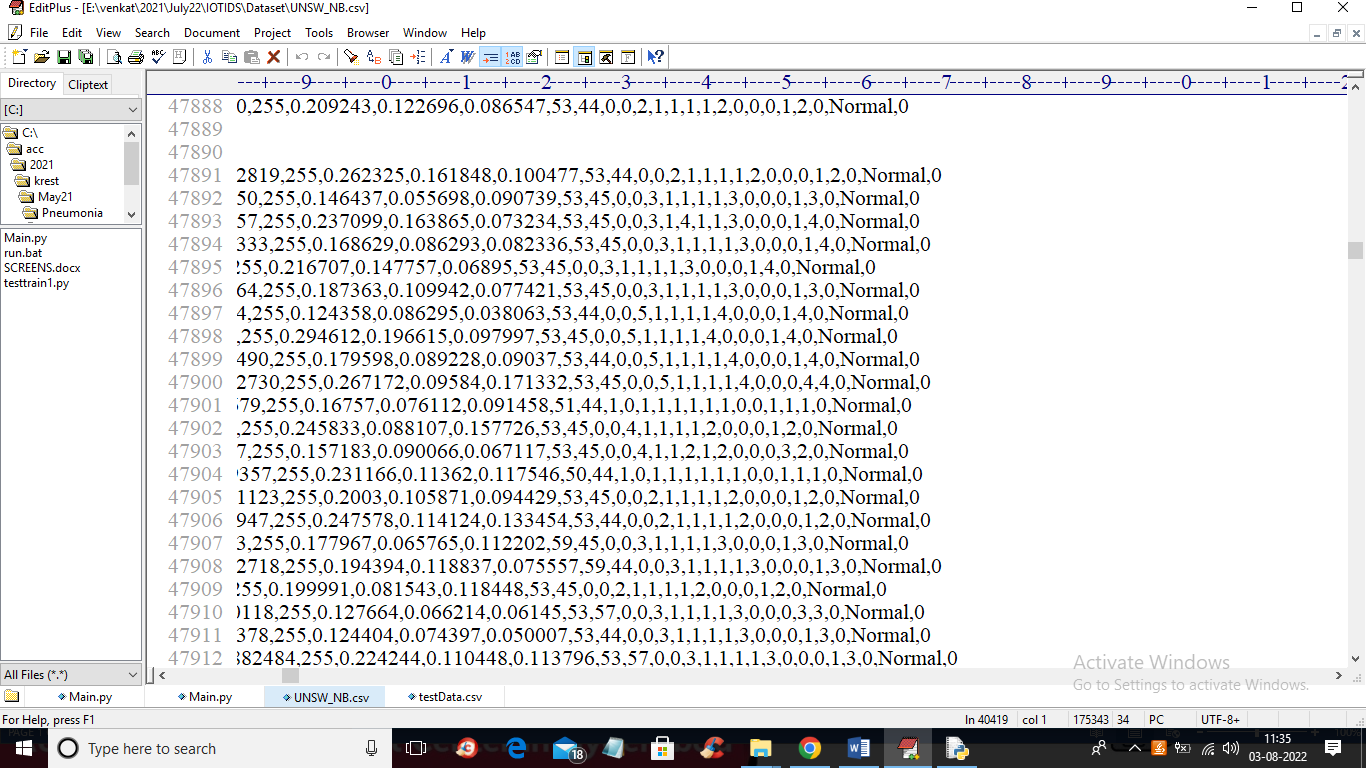
IOT devices are small sensors which can be deployed in any environment such as Road Traffic Monitoring, patient health monitoring, home CCTV monitoring and many more. IOT devices are used to sense data from its environment and then using Internet connection will send that sense data to centralized server for monitoring. Sometime some malicious user can alter IOT network data to report false information for example they can later traffic sensor IOT to report false traffic data and this false information will be spread in to entire network.

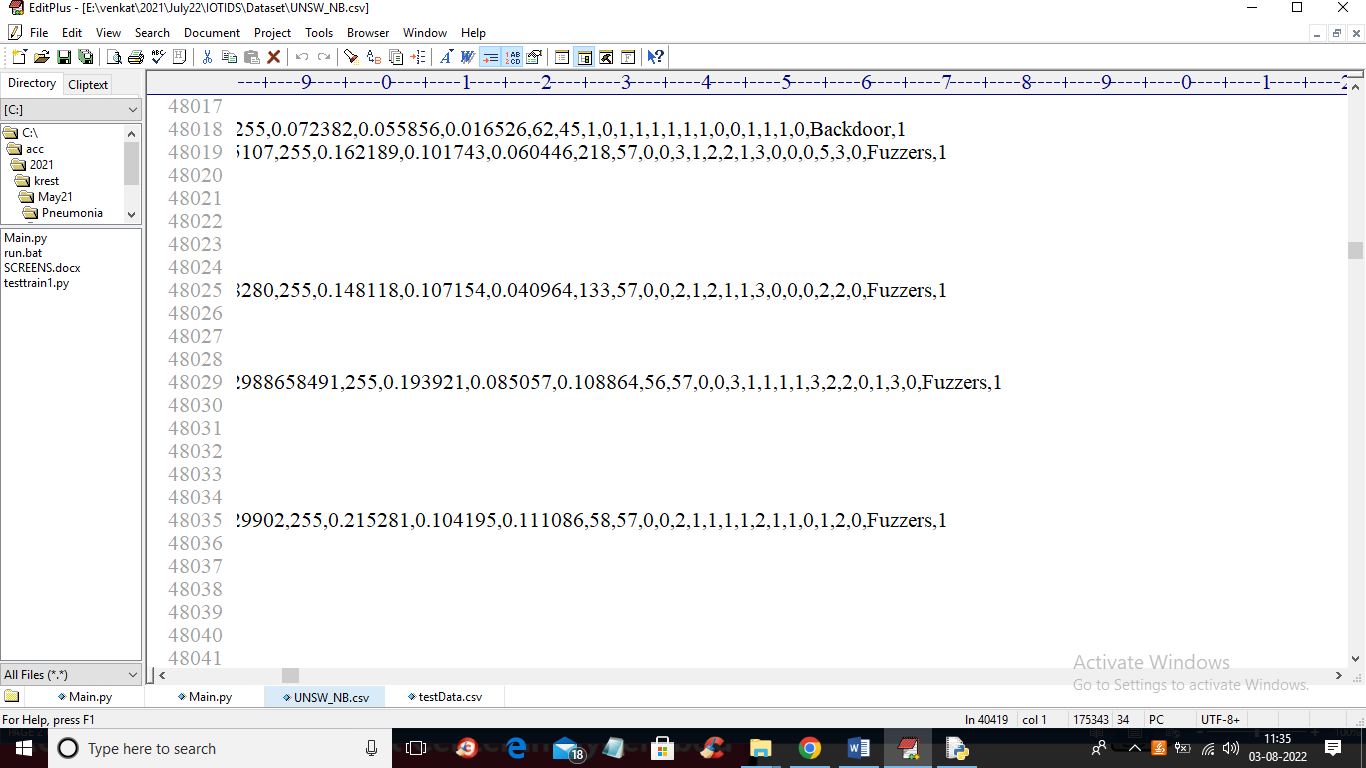
To detect such attack many signature based and machine learning and deep learning AUTO ENCODER based CNN algorithms are introduced but their detection rate is not satisfactory. To increase detection performance we are introducing Deep Learning IDS based on Convolution2D Deep Learning algorithm which contains multiple layers to filter IOT data and this filtration helps in obtaining optimize features which result into IOT attack detection with a prediction accuracy of 99%.

To train existing Auto Encoder and propose Deep Learning IDS we have used UNSW-NB15 dataset and below screen showing dataset details



In above screen first row contains dataset column names and remaining rows contains dataset value and in last column we have class label as Normal or ATTACK which means IOT request record contains normal signature or attack





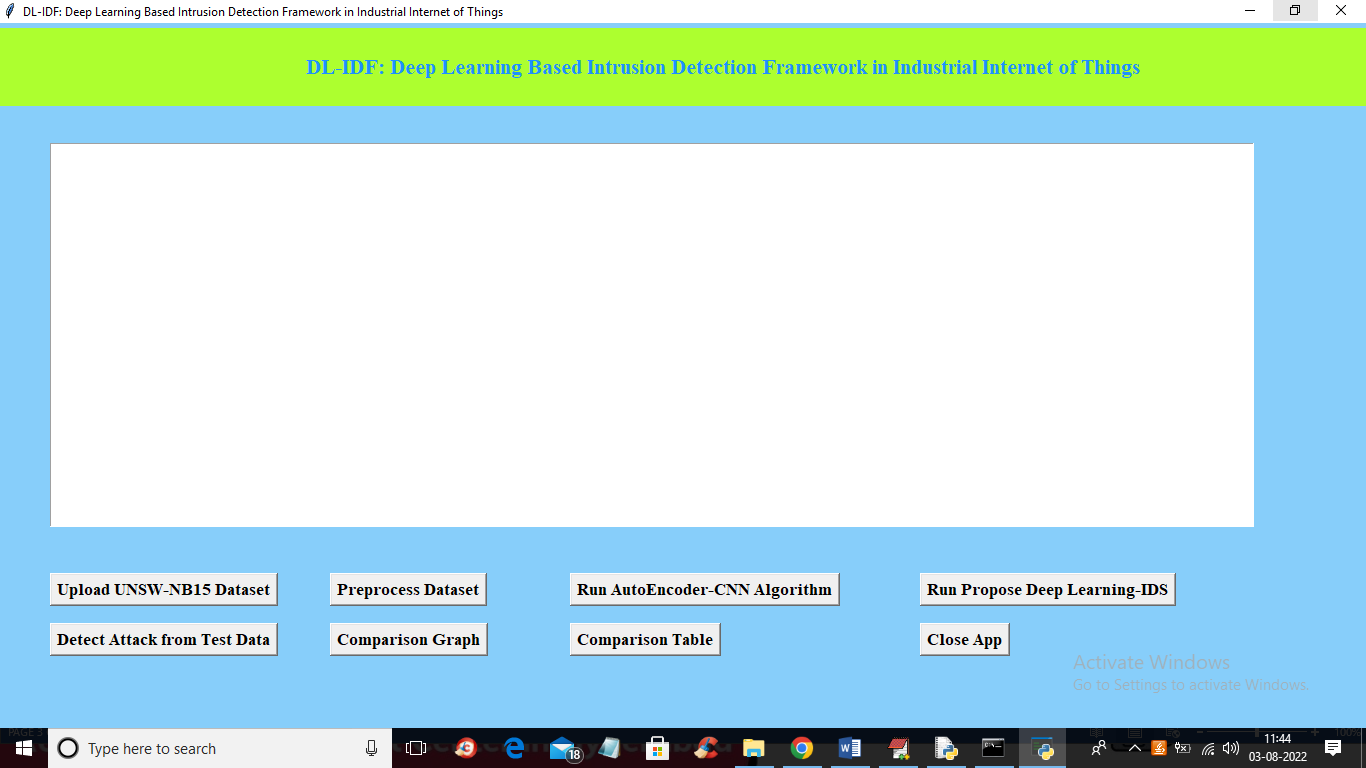
In above screens in last column we can see label as 0 or 1 where 0 means Normal and 1 means attack. By using above dataset we are training both existing and propose algorithm and then calculating their performance in terms of accuracy and precision and confusion matrix.

To implement this project we have designed following modules

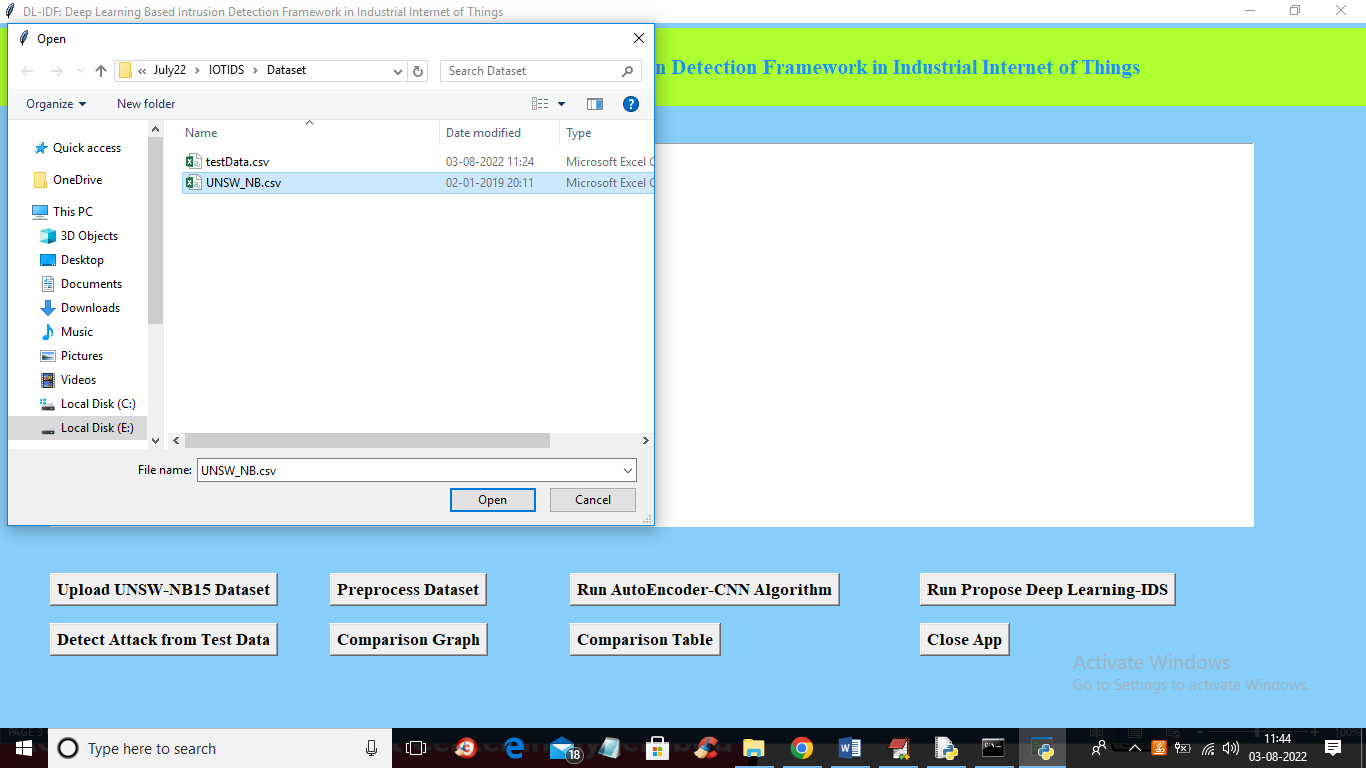
1. Upload UNSW-NB15 Dataset: using this module we will upload and read dataset values and then plot graph with normal and attack records
2. Preprocess Dataset: dataset contains missing and non-numeric values but deep learning algorithms only accept numeric values so by applying Preprocessing technique we are replacing missing values with 0 and then converting non-numeric data to numeric data by applying Label Encoding algorithm which will assigned unique Integer ID to each non-numeric values. After processing dataset we are splitting into train and test where application using 80% dataset for training and 20% dataset for testing
3. Run AutoEncoder-CNN Algorithm: using this module we will input 80% training data to Auto Encoder algorithm and then trained a model and this trained model applied on 20% test data to calculate prediction accuracy
4. Run Propose Deep Learning-IDS: using this module we will input 80% training data to Propose Deep Learning Convolution2d algorithm and then trained a model and this trained model applied on 20% test data to calculate prediction accuracy
5. Detect Attack from Test Data: using this module we will upload test data and then Propose DL-IDS will predict weather test data is normal or contains attack
6. Comparison Graph: using this module we will plot comparison graph between existing and propose algorithms
7. Comparison Table: using this module we will display both algorithms performance in tabular format

SCREEN SHOTS

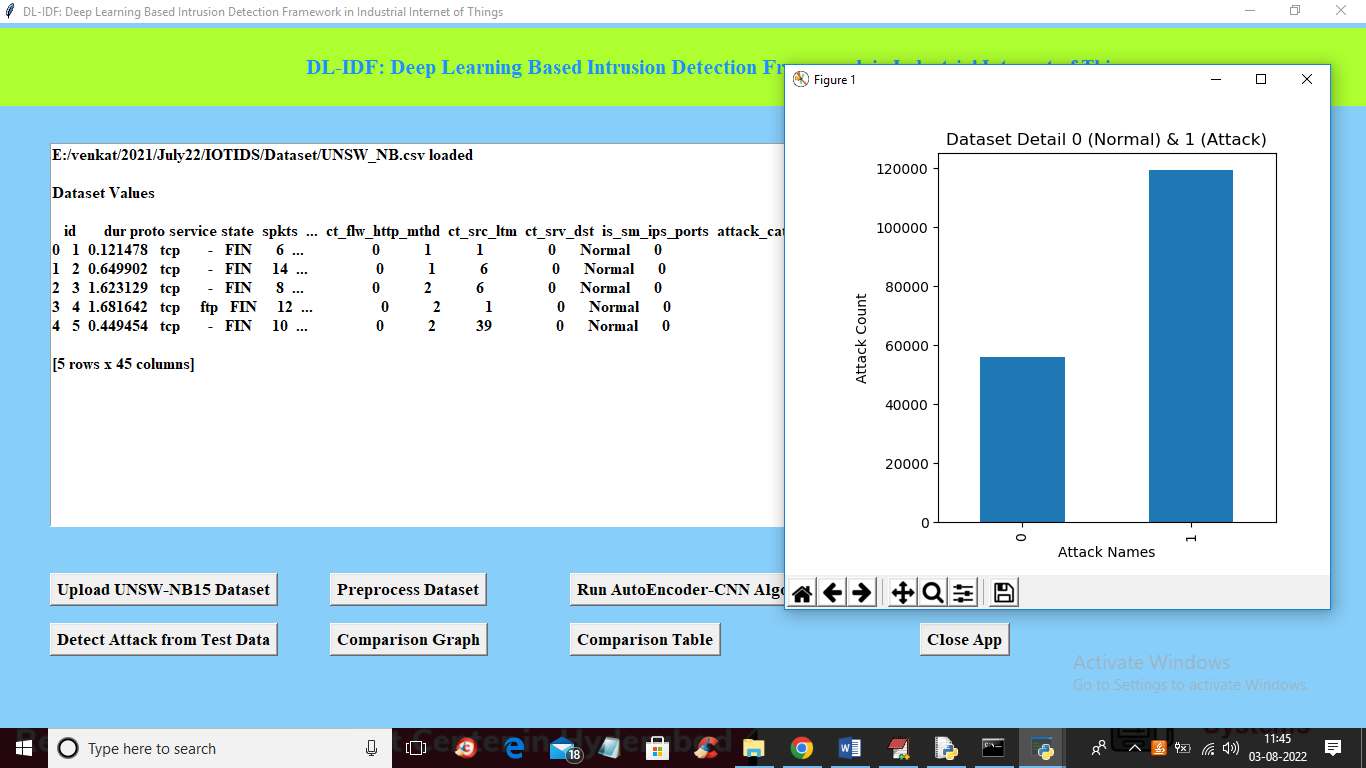
To run project double click on ‘run.bat’ file to get below screen



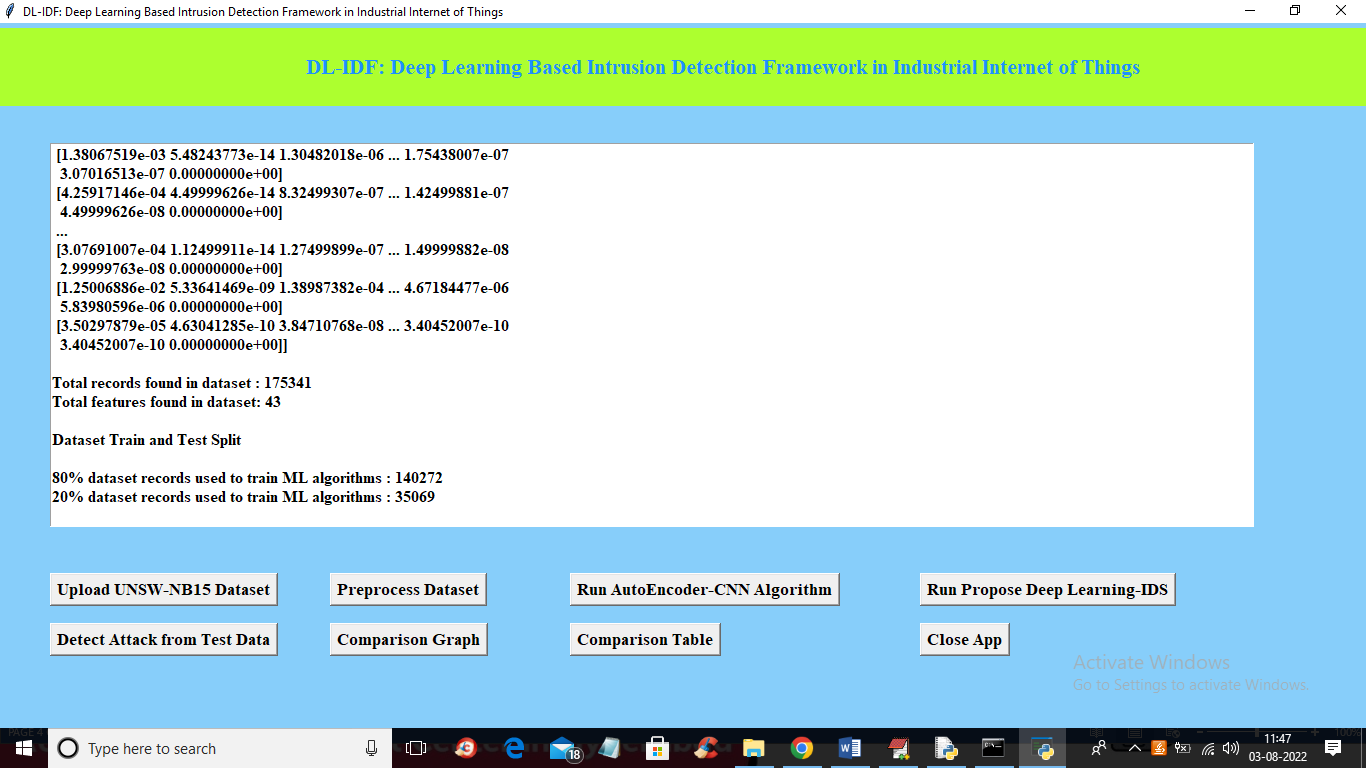
In above screen click on ‘Upload UNSW-NB15 Dataset’ button to upload dataset and get below output



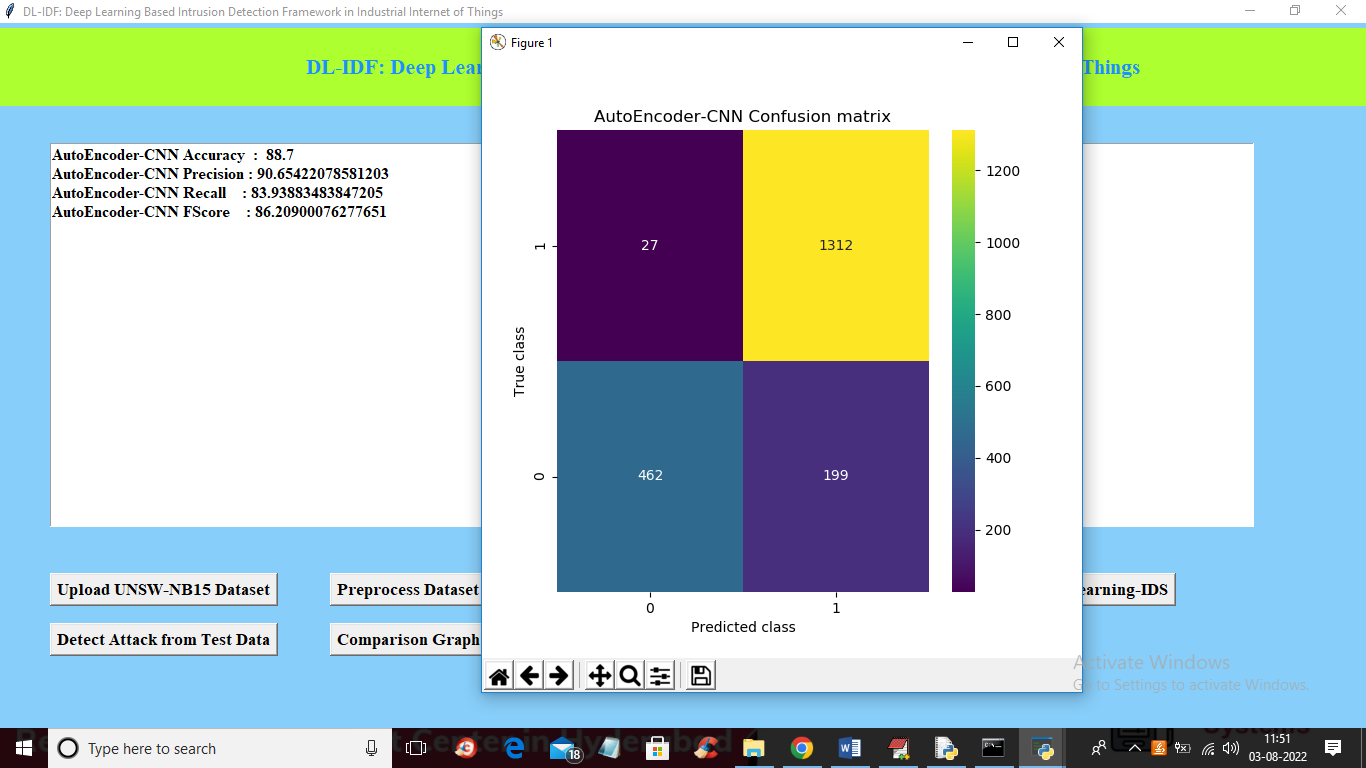
In above screen selecting and uploading UNSW-NB dataset and then click on ‘Open’ button to load dataset and get below output



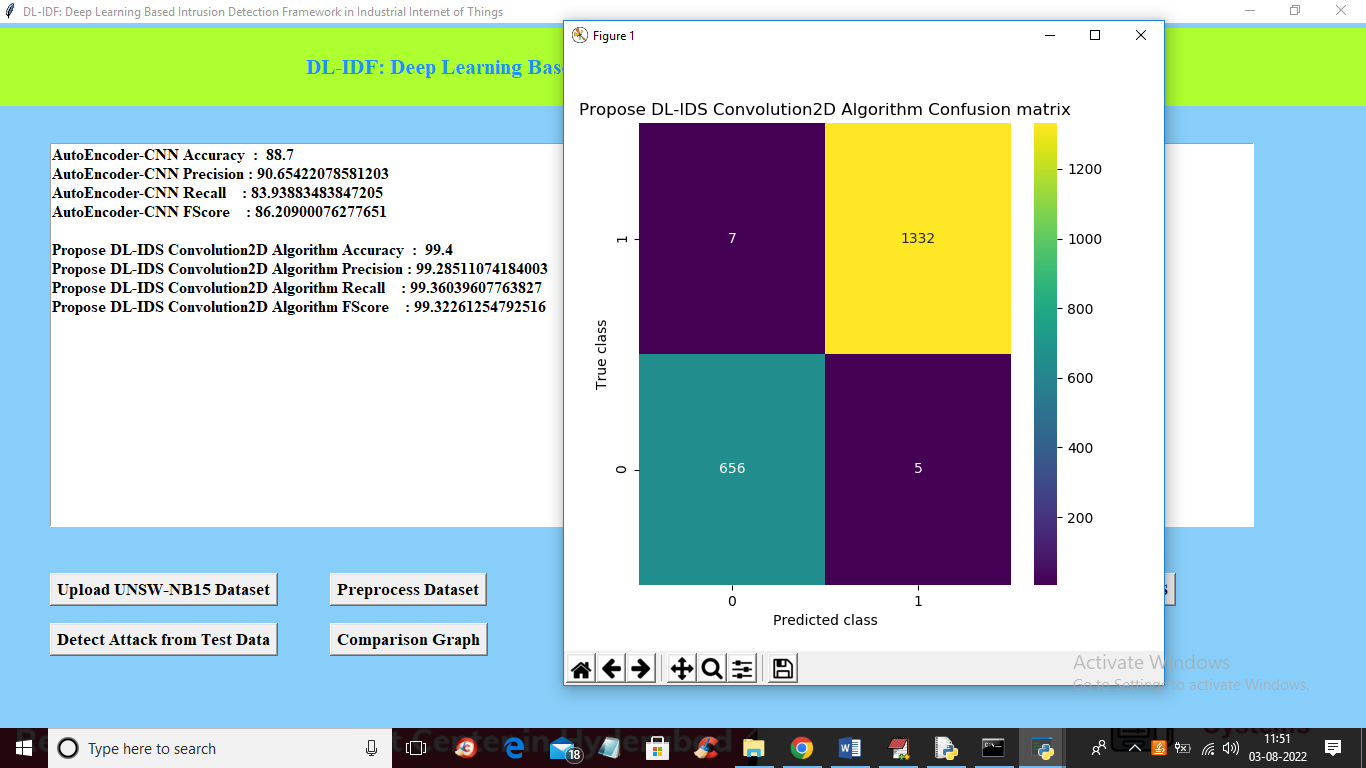
In above screen dataset loaded and in above graph x-axis contains class labels y-axis represents count of that class label record where 0 means normal and 1 means attack. In above dataset we can see it contains non-numeric data so close above graph and the click on ‘Preprocess Dataset’ button to convert non-numeric to numeric and get below output



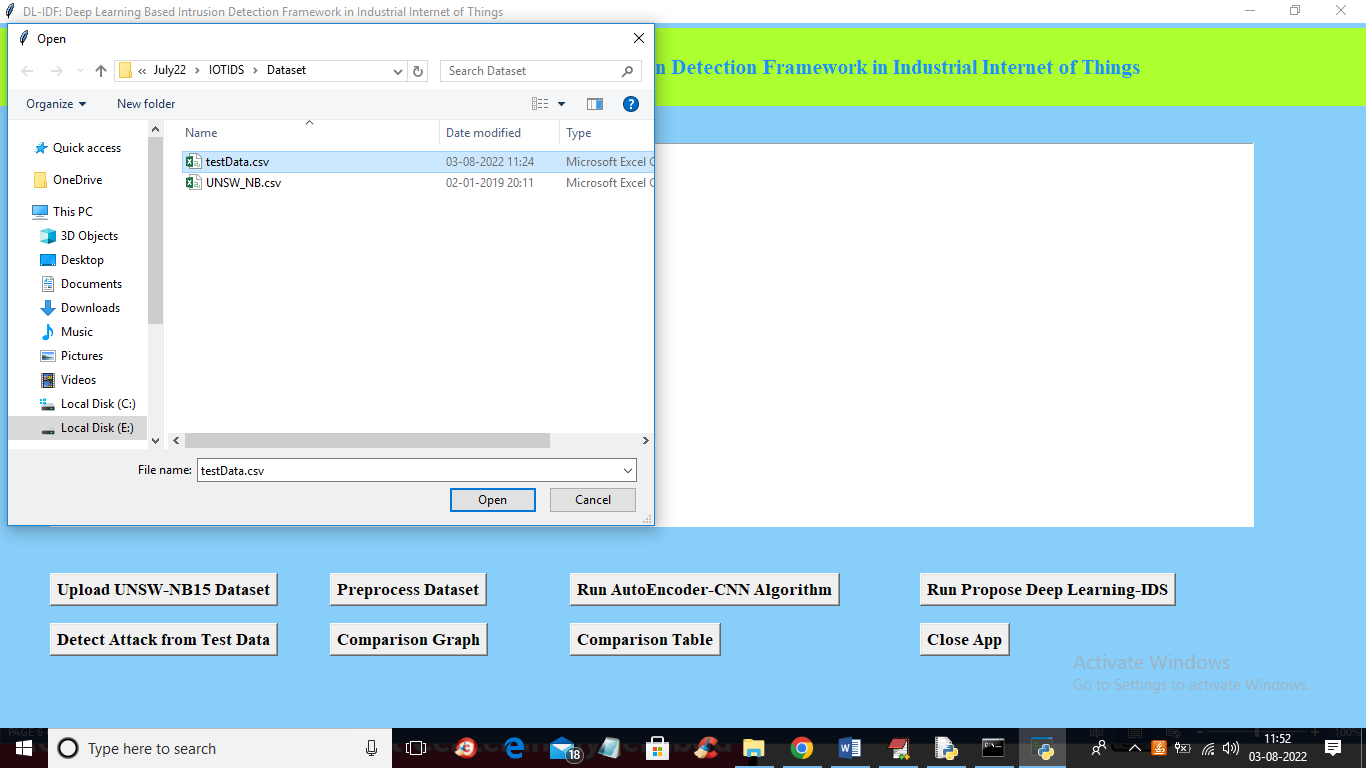
In above screen we can see entire dataset converted to numeric format and then we can see train and test split of dataset and now click on ‘Run AutoEncoder-CNN Algorithm’ to train Auto Encoder algorithm and get below output



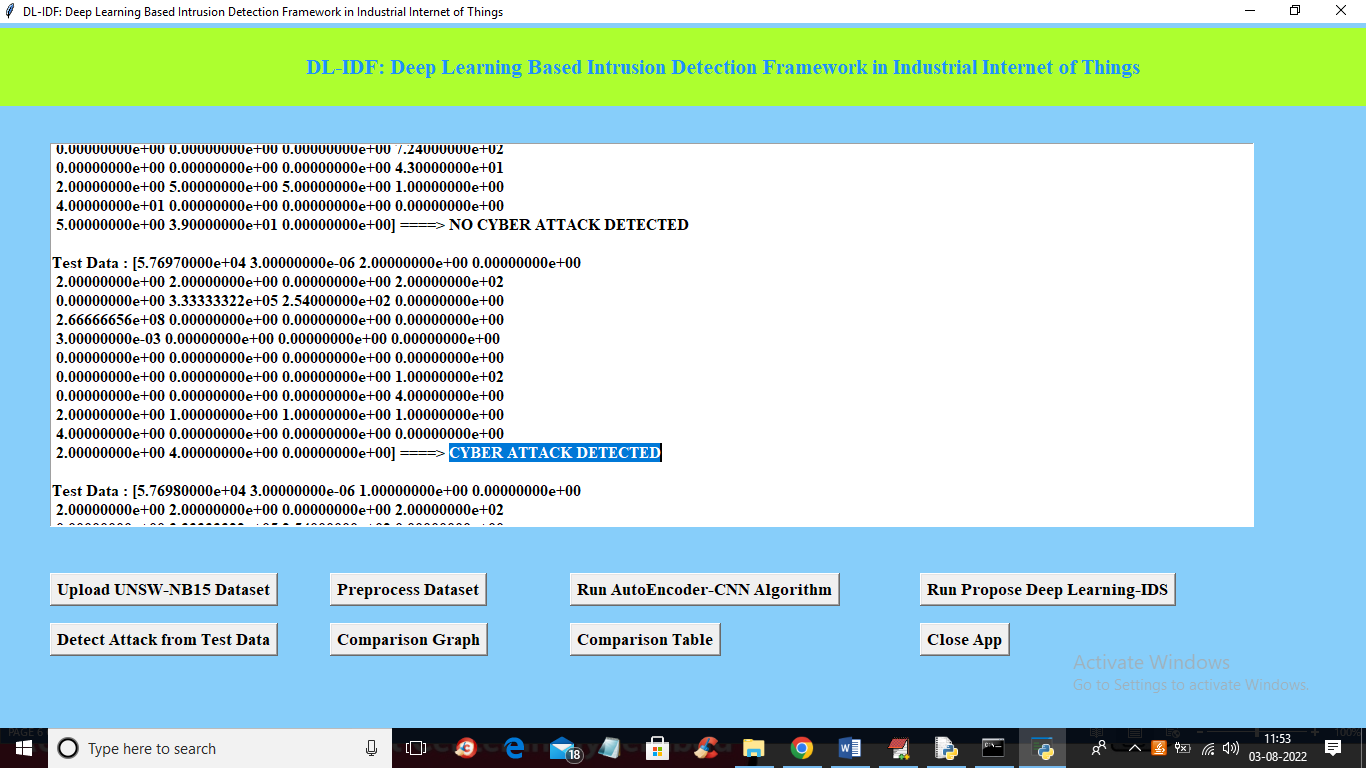
In above screen with existing Auto encoder algorithm we got 88% accuracy and in confusion matrix graph x-axis represents Predicted class label and y-axis represents True class labels and prediction count in blue colour boxes are wrong prediction and non-blue colour boxes count are correct prediction. Now close above graph and then click on ‘Run Propose Deep Learning-IDS’ button to train propose algorithm and get below output



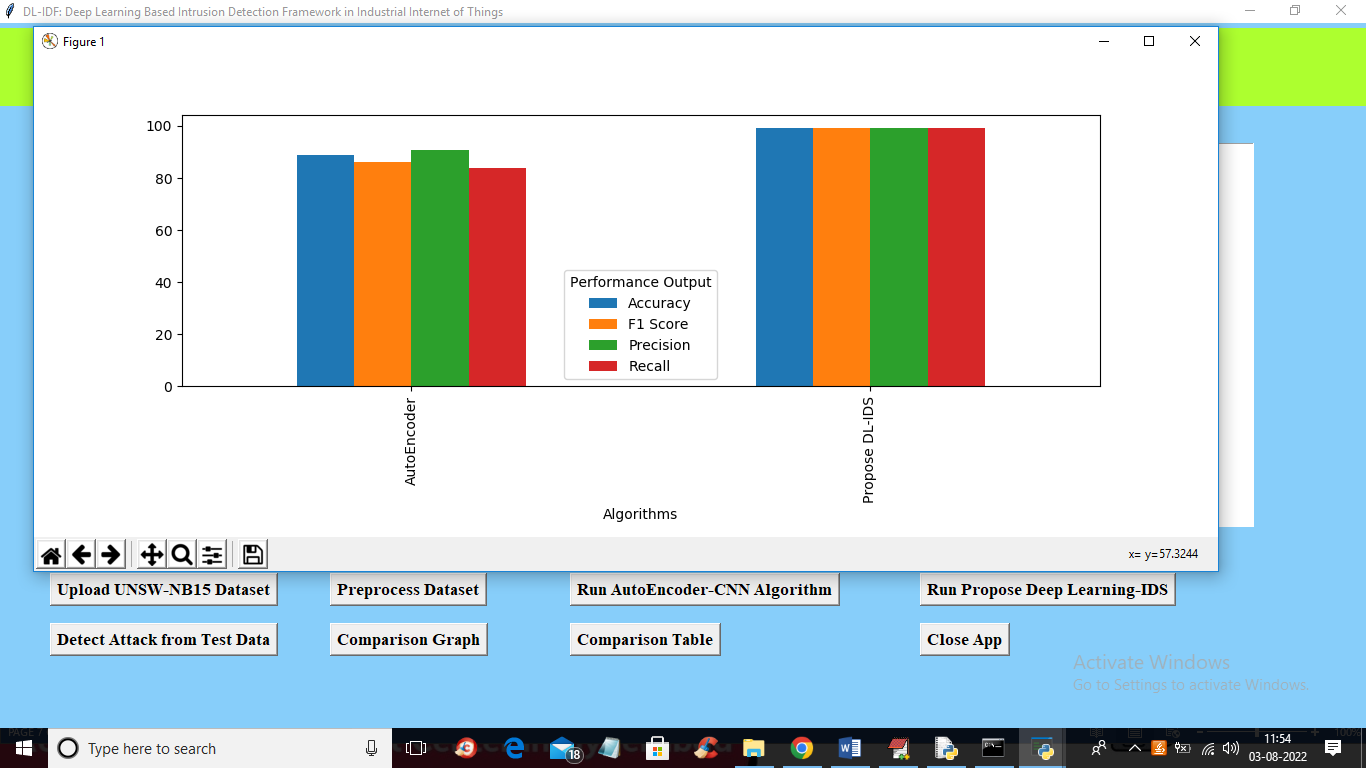
In above screen with Propose DL-IDS algorithm we got 99% accuracy and now close above graph and then click on ‘Detect Attack from Test Data’ button to upload TEST data and then propose algorithm will predict attack from test data



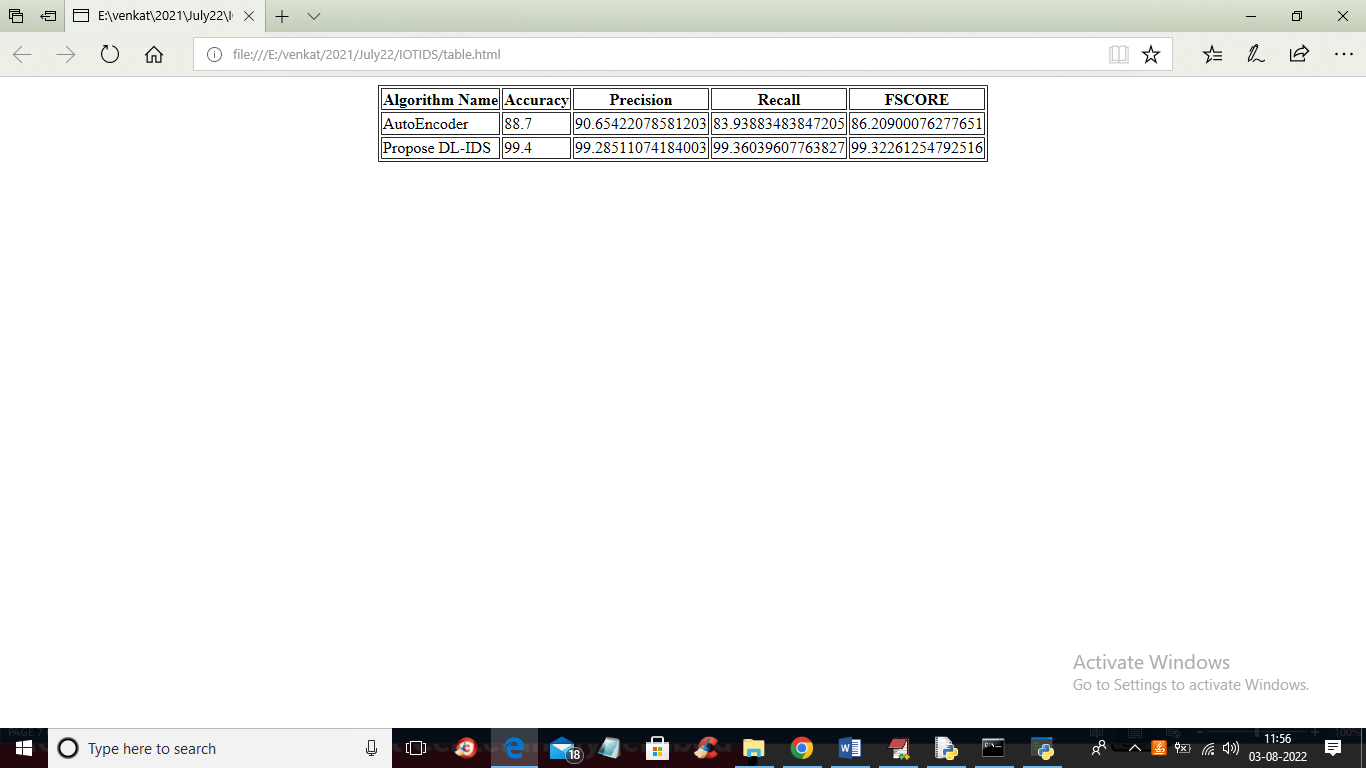
In above screen selecting and uploading ‘testData.csv’ file and then click on ‘Open’ button to get below output



In above screen in square bracket we can see TEST data values and after arrow symbol =🡺 we can see predicted output as ‘Attack Detected” or NO Attack Detected and now click on ‘Comparison Graph’ button to get below graph



In above graph x-axis represents algorithm names and y-axis represents accuracy and other metrics such as precision, recall etc. In above graph different bar colour represents different metrics. Now close above graph and then click on ‘Comparison Table’ button to get below output



In above screen in tabular format we can see accuracy and other values for both algorithms