Design of an Intrusion Detection Model using Machine Learning Algorithms for IoT-Enabled Smart Home

IOT devices are small sensors which runs on battery to sense its environment data and then used internet connection to transmit sense data to centralized server for further processing. Smart home electricity sensors, CCTV cameras and other surveillance devices are the examples of IOT sensors. This sensors runs on battery and small memory chip and cannot afford to install antivirus software to detect and prevent any malicious activities so it can be easily hack to alter sense data with false information and this false data send to centralized server which may take incorrect action based on false data.

To detect and avoid such intrude attacks author of this paper employing Machine learning algorithms which can analyse packet data to predict weather packet is benign or malicious. In propose paper author using WIRESHARK tool to capture all network packets data and then input to ML algorithms which will predict weather packet is benign or malicious.

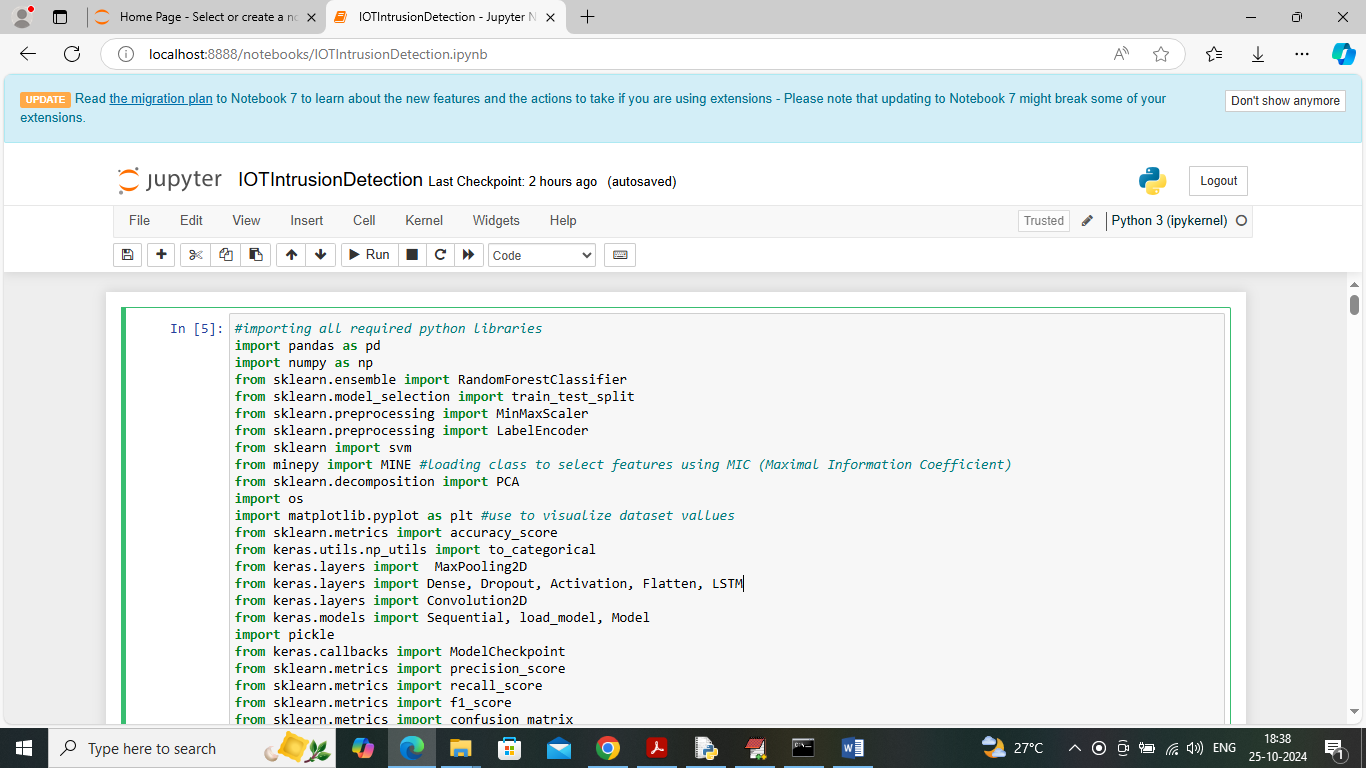
In propose paper author utilizing following modules to detect IOT intrusion

1. Data Collection: data will be collected from the server using WIRESHARK tool which will capture all packets data. we don’t have any server to capture WIRESHARK packets so we are utilizing IOT WIRESHARK dataset from KAGGLE repository which can be download from this URL ‘https://www.kaggle.com/datasets/malqarni/iotdataset’
2. Features Selection: all captured data will be input to ‘Maximal Information Coefficient’ (MIC) features selection algorithm to select features which are capable of yield high prediction accuracy
3. PCA (principal component analysis): PCA will be applied on selected features to reduce dimension and then select only those features which are relevant and reduce all irrelevant features
4. Features Normalization: will be applying MINMAX features normalization algorithm to normalize selected features
5. ML and DL (deep learning) algorithms: in propose paper author has employed various machine and deep learning algorithm such as Random Forest, SVM, LSTM and CNN and then evaluate each algorithm performance in terms of Accuracy, Precision, Recall and FSCORE. Among all algorithms CNN2D is giving best accuracy.

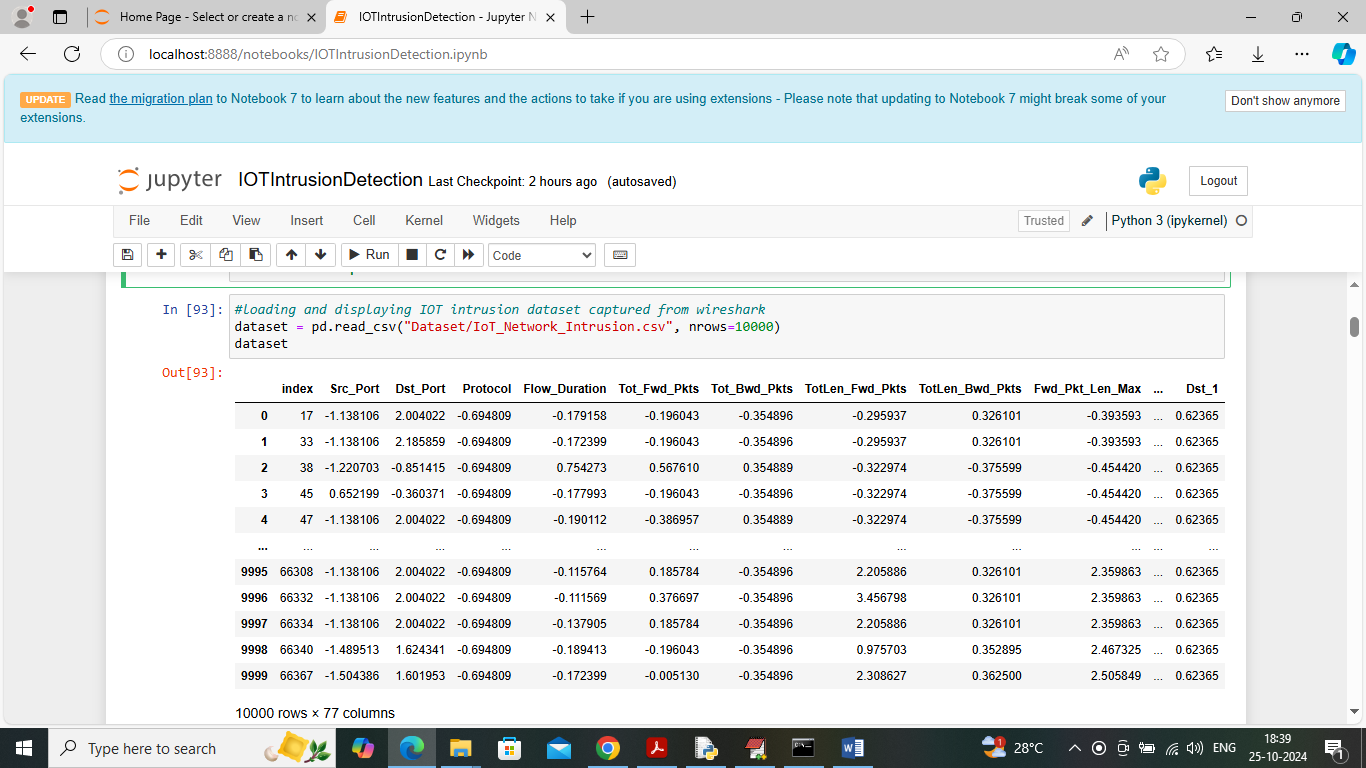
IOT dataset contains 75 training features and then contains two class labels such as 0 (benign) and 1 (malicious) and by using this dataset features will train and test each algorithm performance

SCREEN SHOTS

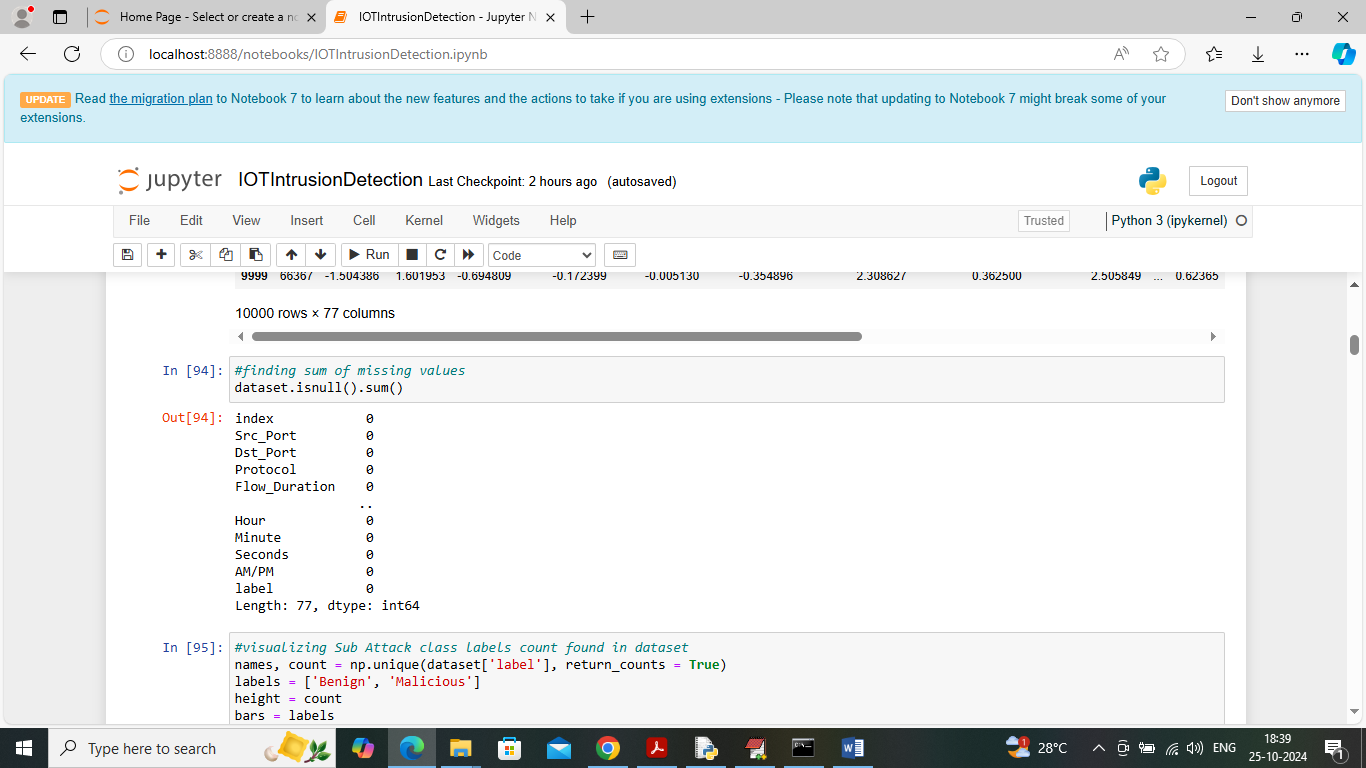
We have coded this project using JUPYTER notebook to show processing of each algorithm describe above and below are the code and output of each algorithm screens



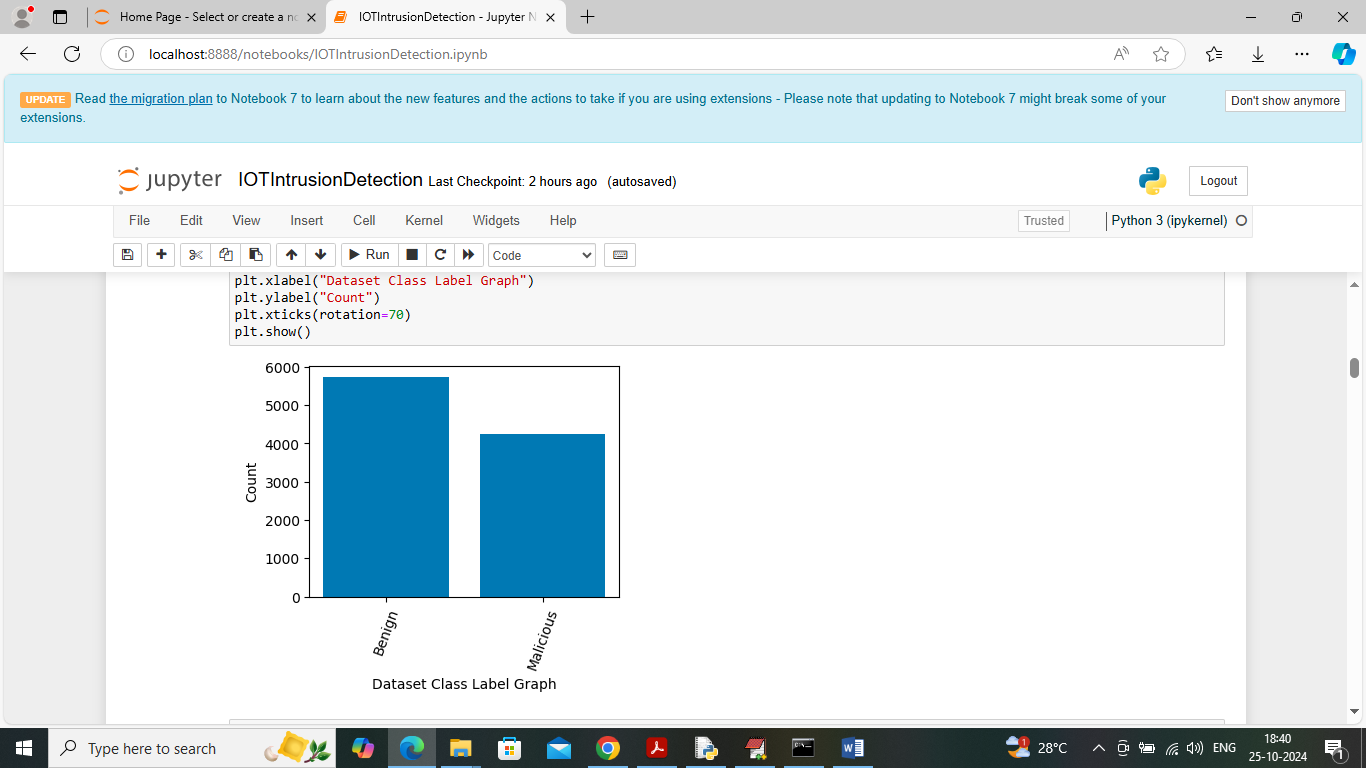
In above screen loading all required python classes and packages



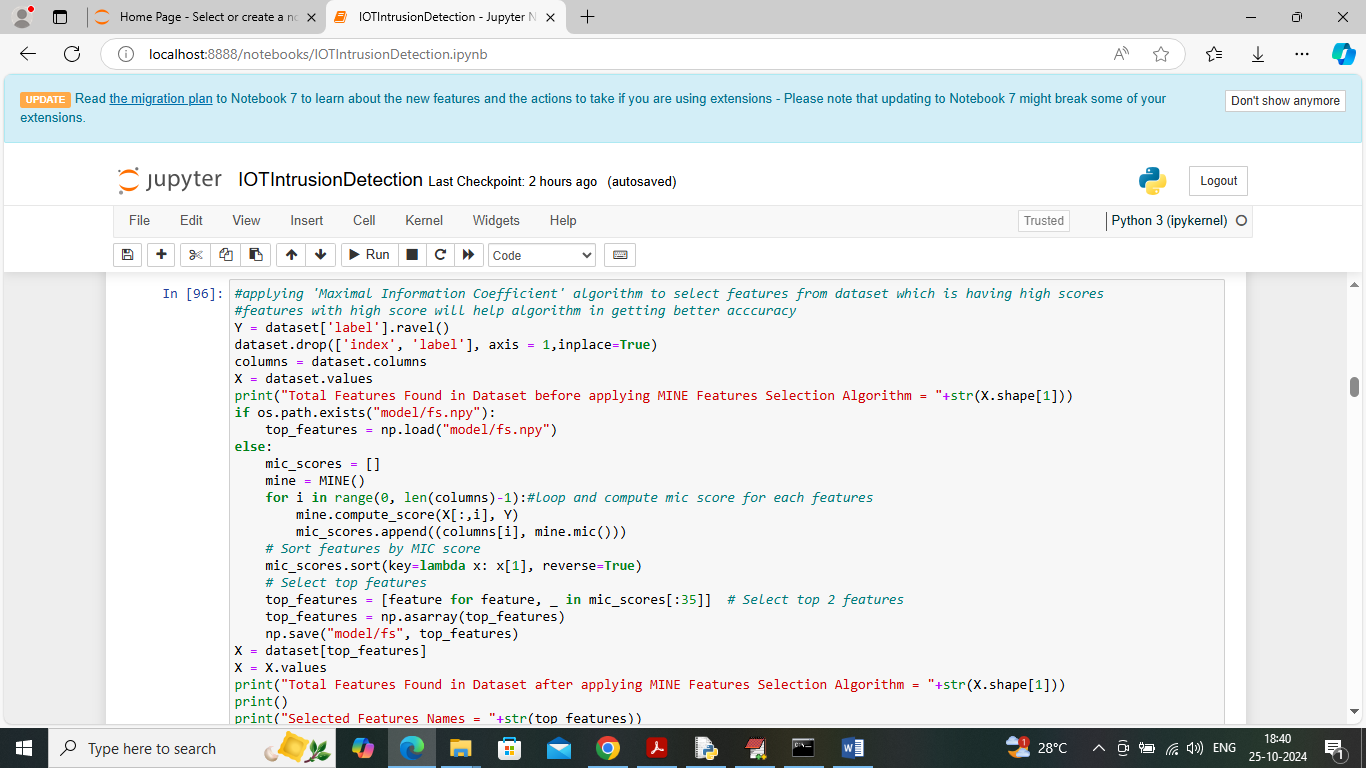
In above screen loading and displaying IOT intrusion dataset



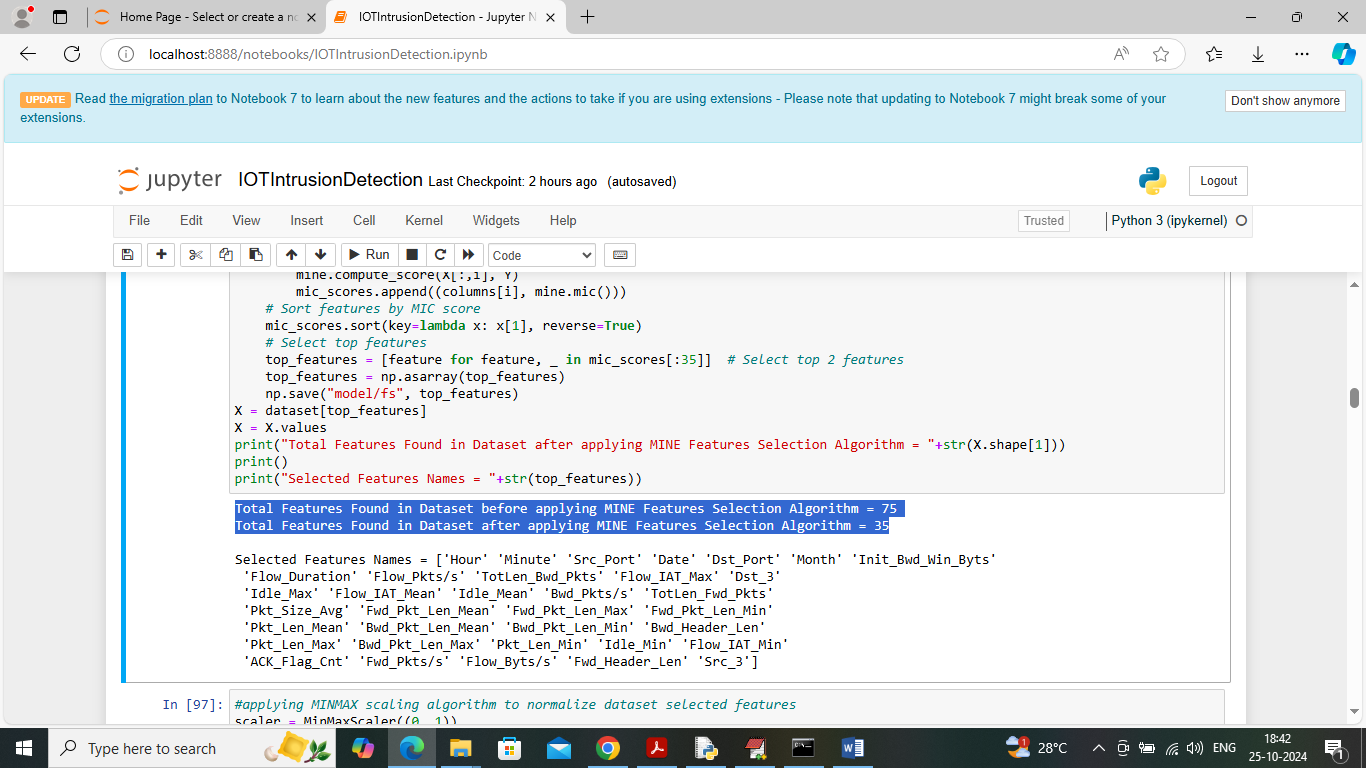
In above screen displaying count of missing values for each features available in dataset



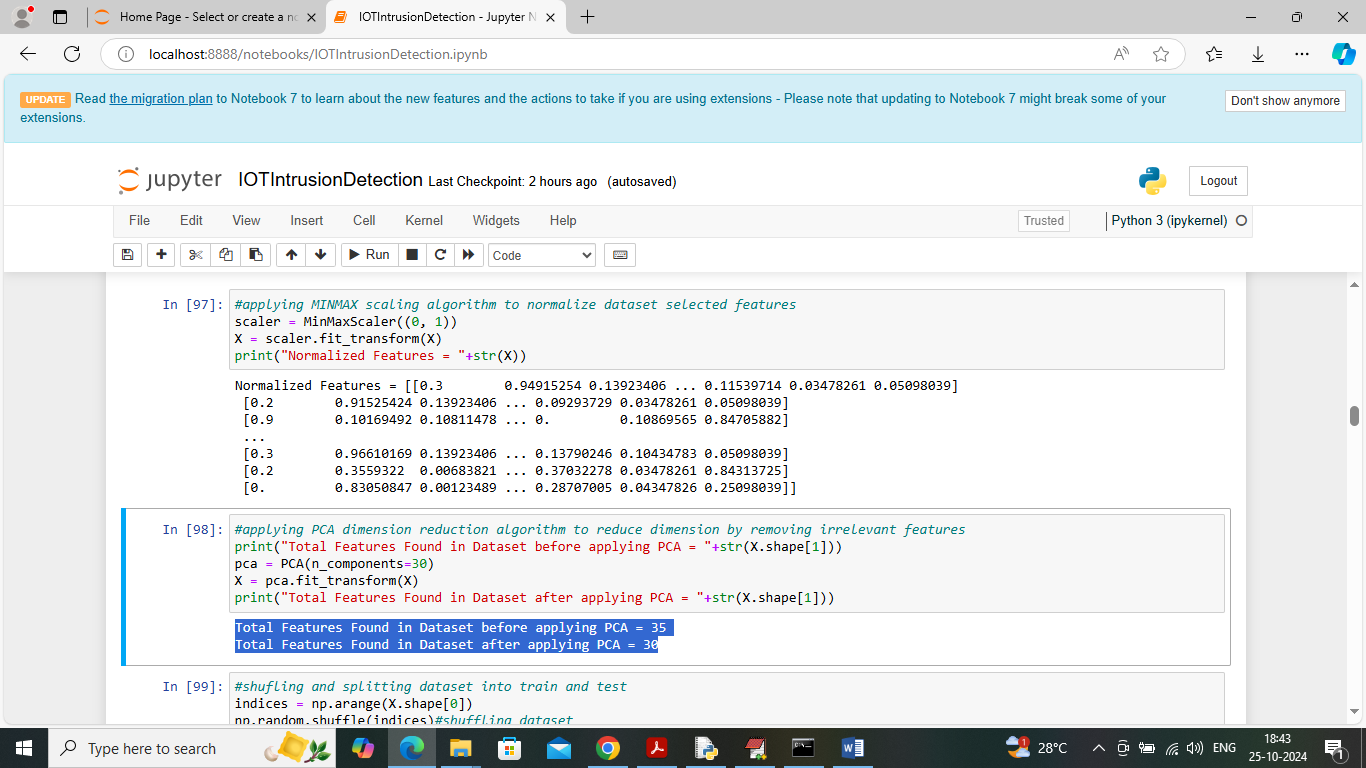
In above screen visualizing graph of different class labels found in dataset where x-axis represents class label and y-axis represents number of records found in that class category



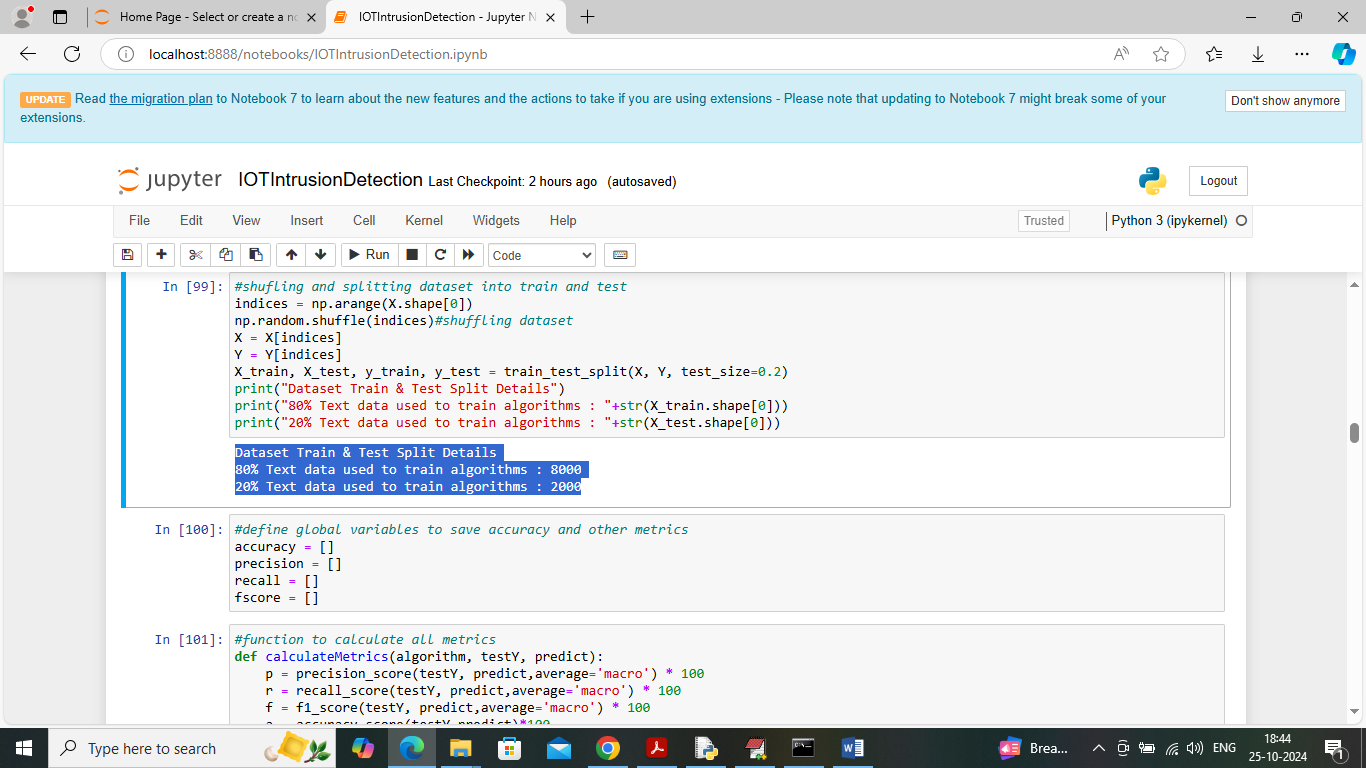
In above screen applying MIC features selection algorithm to select features which are capable of classifying test data as benign or malicious with high accuracy.



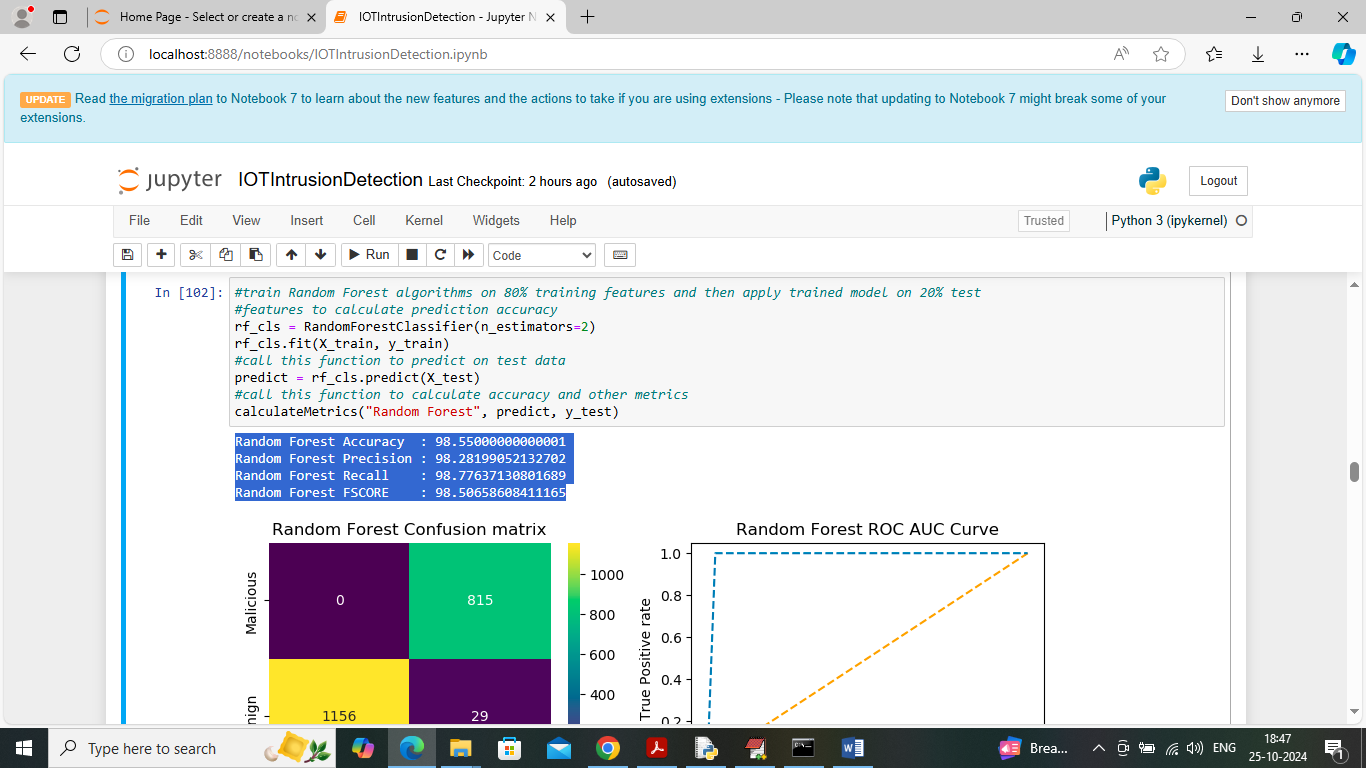
In above screen in first blue line can see dataset having total 75 features and then MIC features selection algorithm selected 35 features out of 75 and then displaying Names of selected features columns from dataset



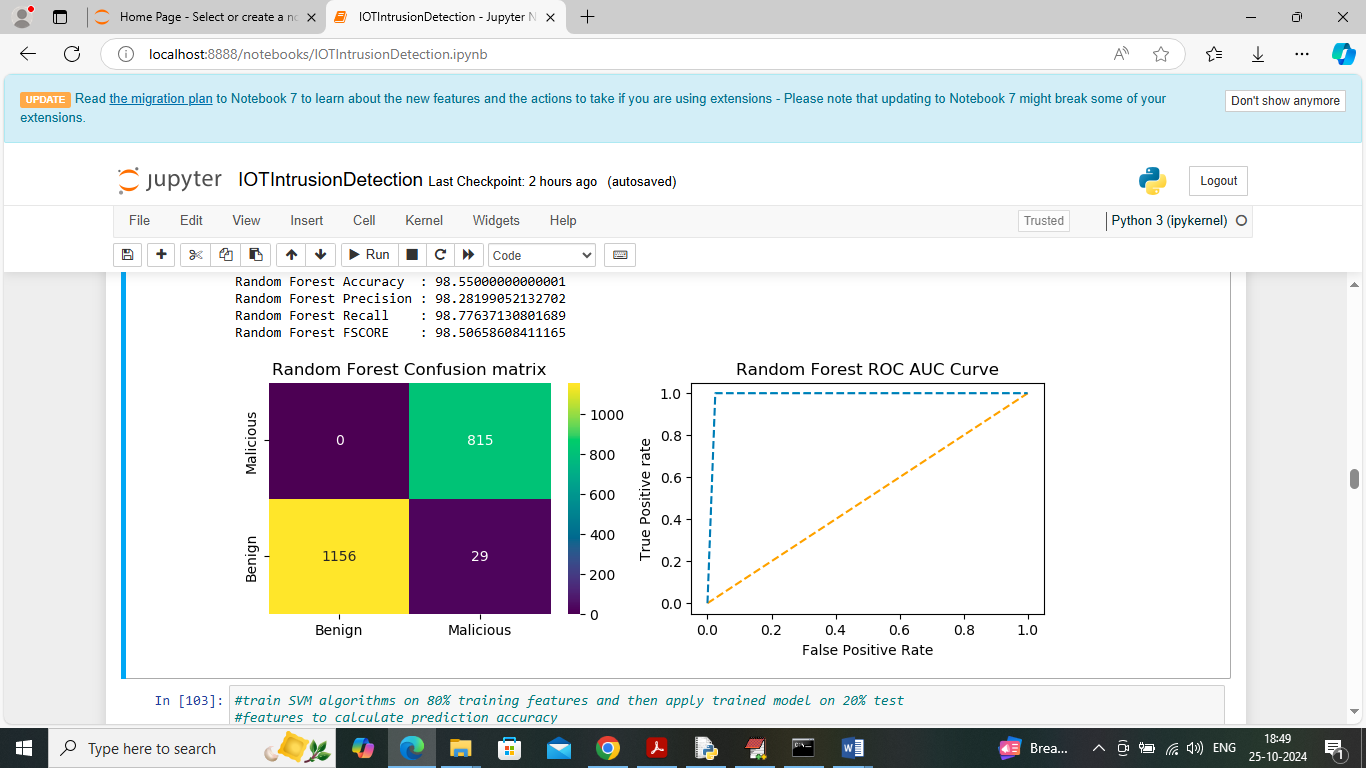
In above screen in first block applying MINMAX normalization algorithm to normalize dataset features and then in second block applying PCA algorithm to reduce features size and before applying PCA dataset where having 35 features and after reduction we got 30 features



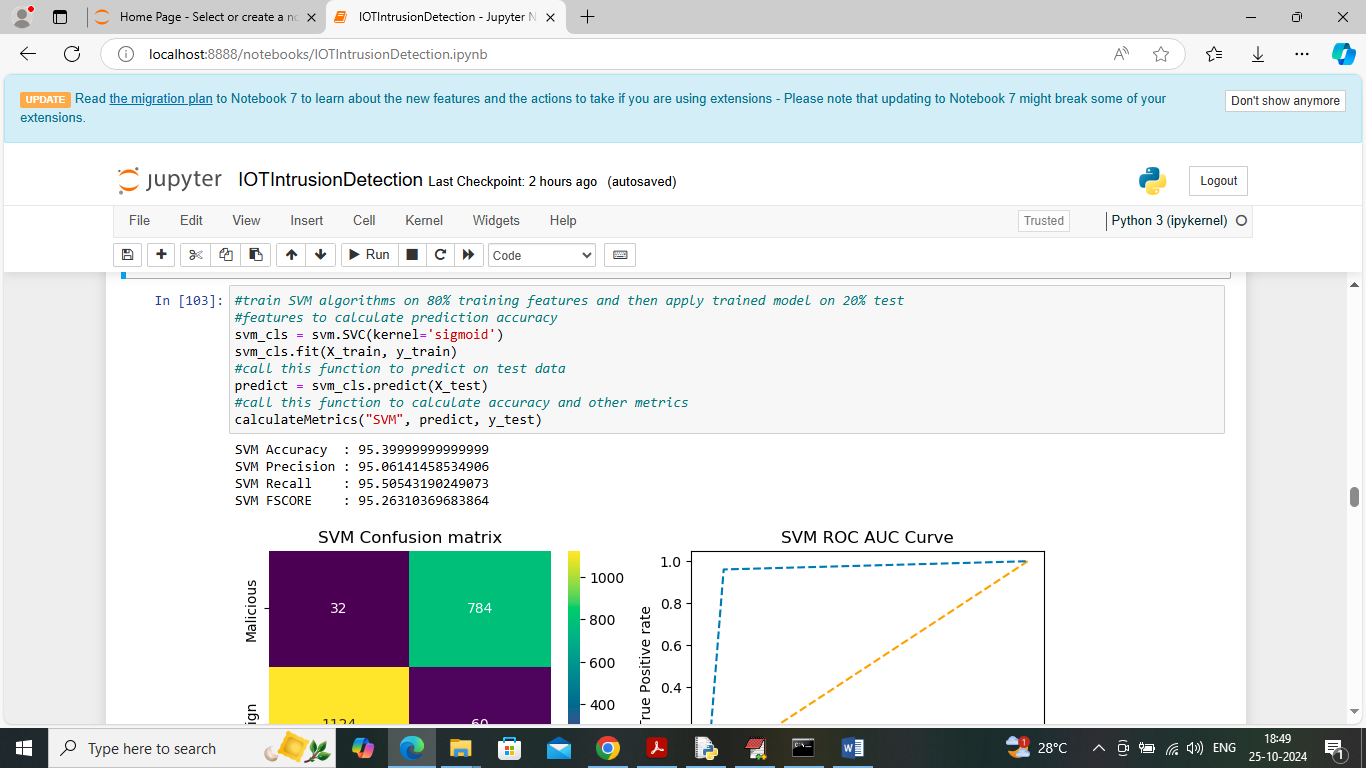
In above screen applying features processing techniques such as shuffling and then splitting dataset into train and test where application using 80% dataset size for training and 20% for testing and then defining function to calculate accuracy and other metrics



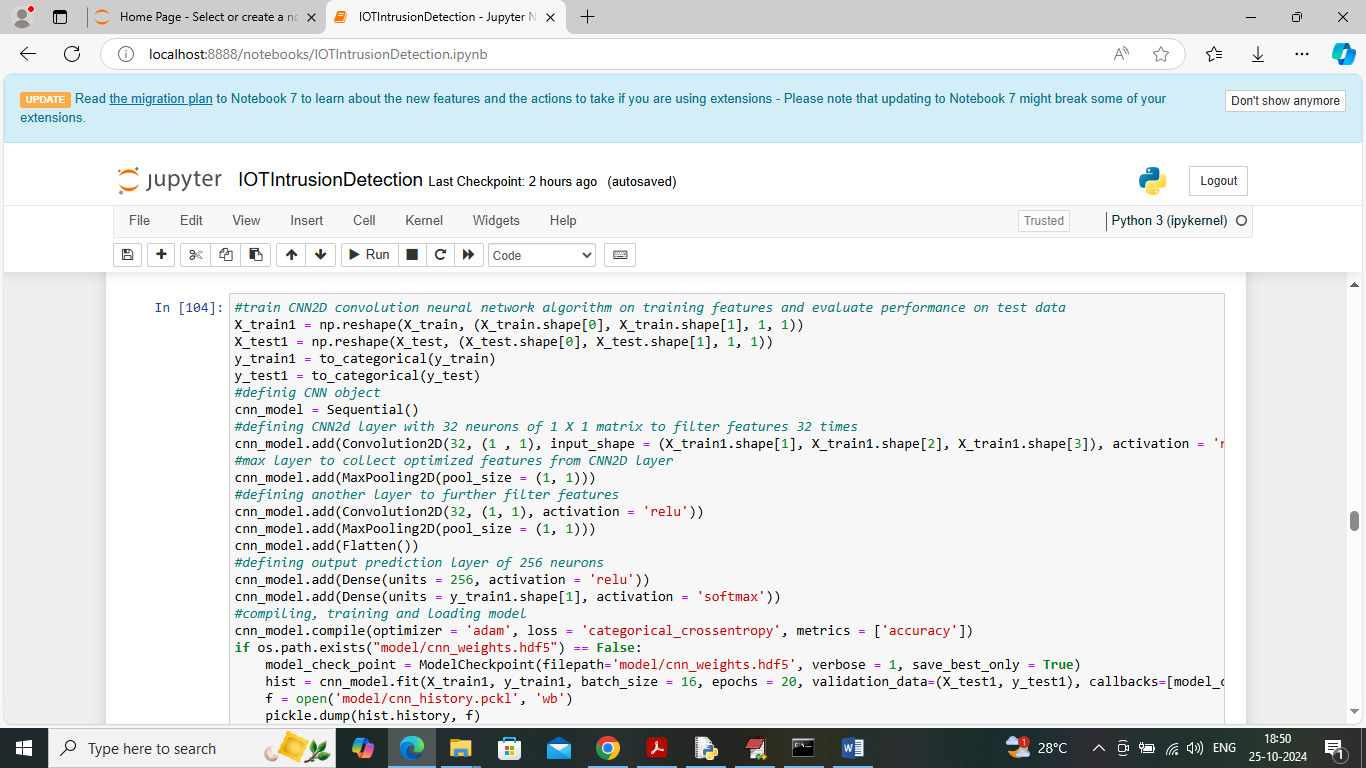
In above screen training Random Forest algorithm on training data and then performing prediction on test data and then Random Forest got 98% prediction accuracy on test data and can see other metrics like precision, recall and FSCORE. In below screen can see confusion matrix and ROC AUU graph



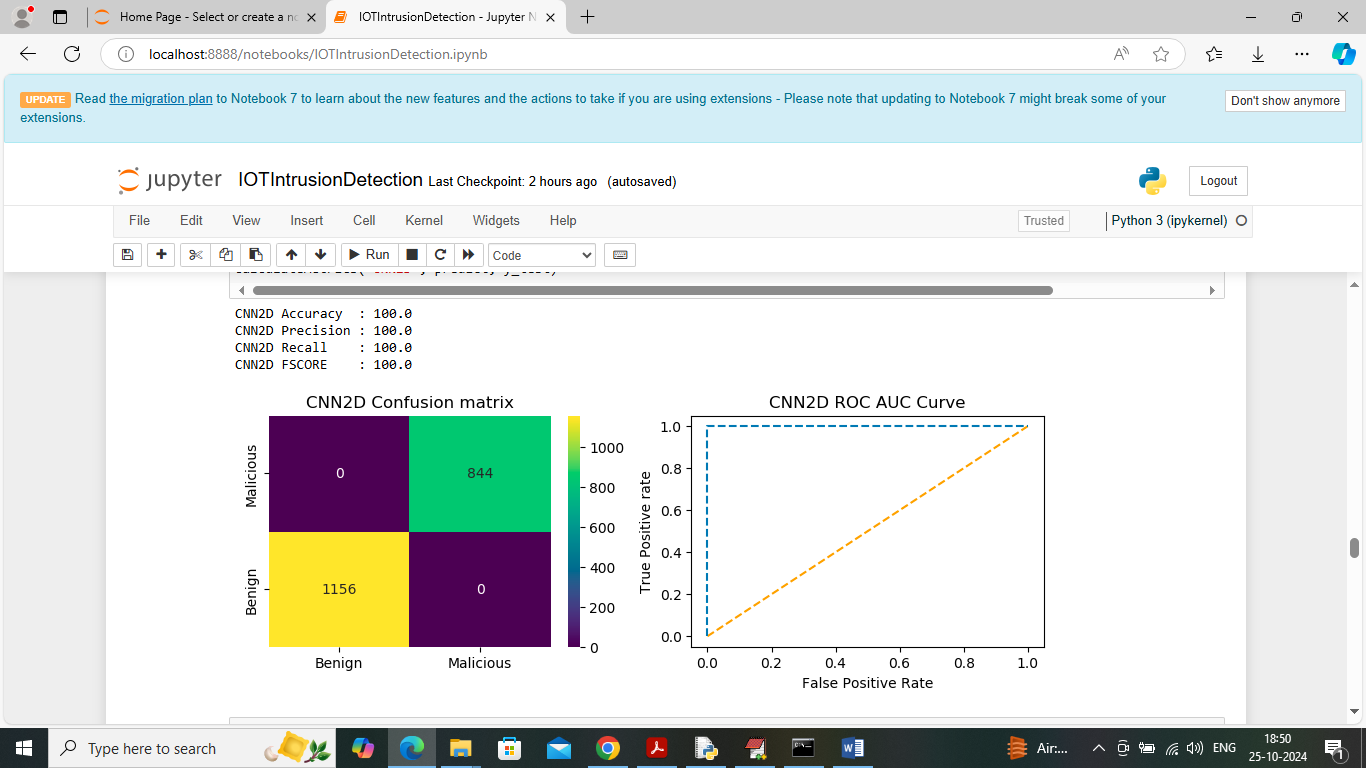
In above confusion matrix graph x-axis represents ‘Predicted Labels’ and y-axis represents ‘True Labels’ and then yellow and green boxes in diagonal represents correct prediction count and blue boxes represents incorrect prediction count which are very few. In above ROC graph x-axis represents ‘False Positive rate’ and y-axis represents True Positive rate and if blue line comes on top of orange line then all predictions are correct and if goes down below orange line then predictions are incorrect.



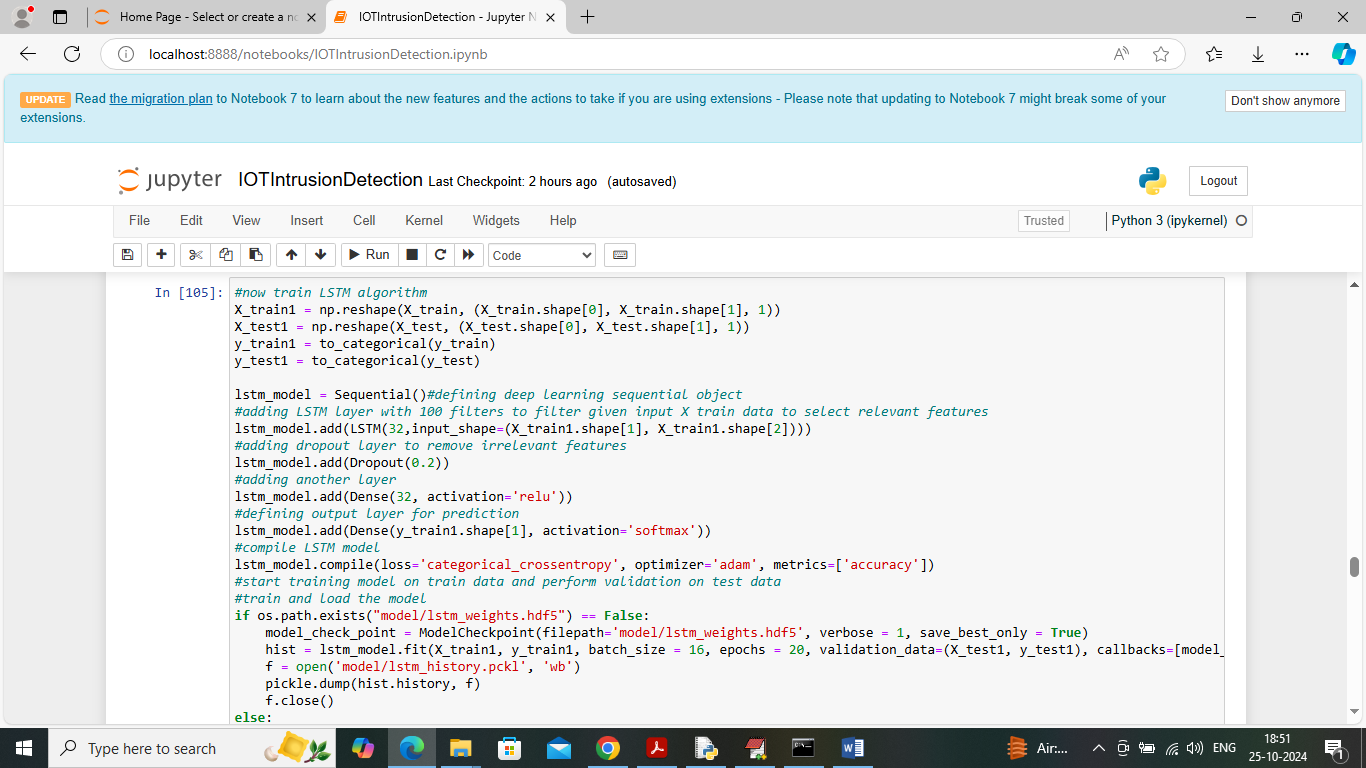
In above screen SVM got 95% accuracy and can see other metrics also



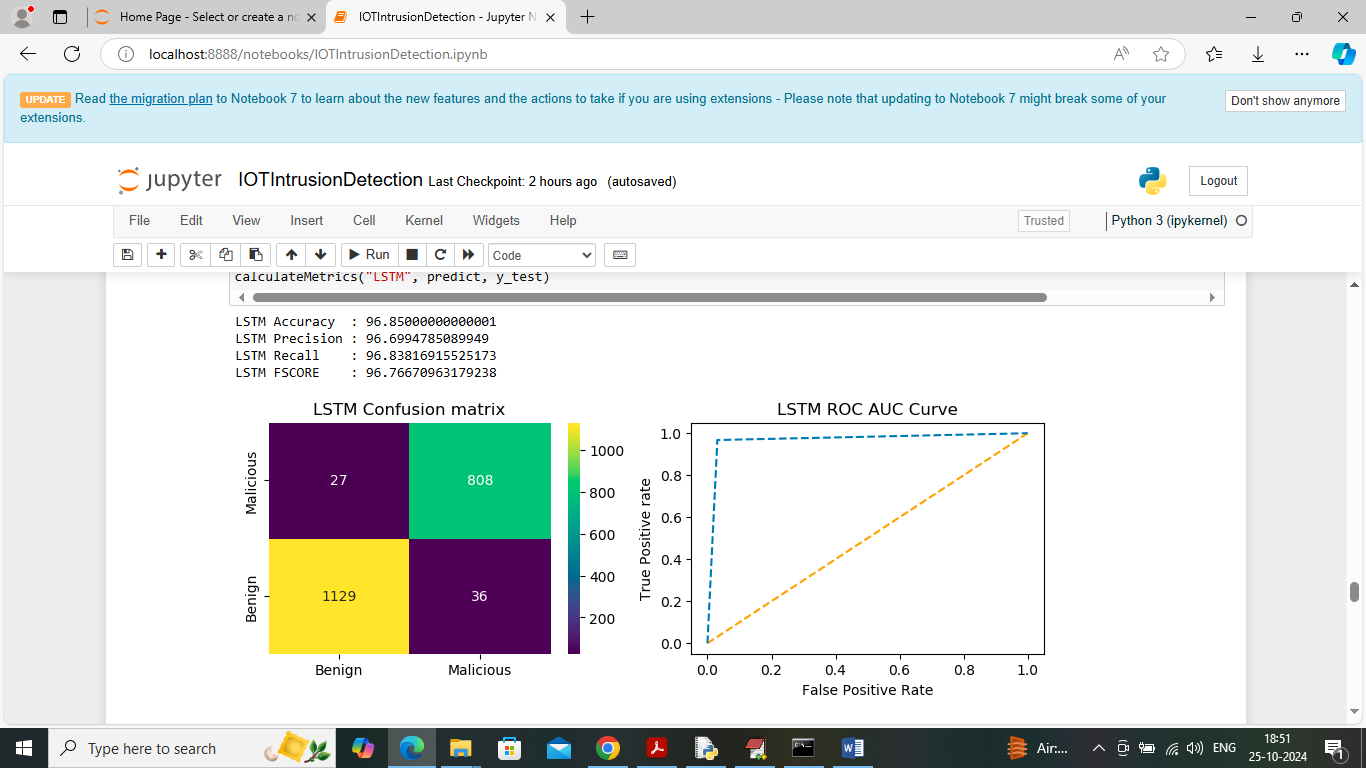
In above screen training CNN2D algorithm and after executing this block will get below output



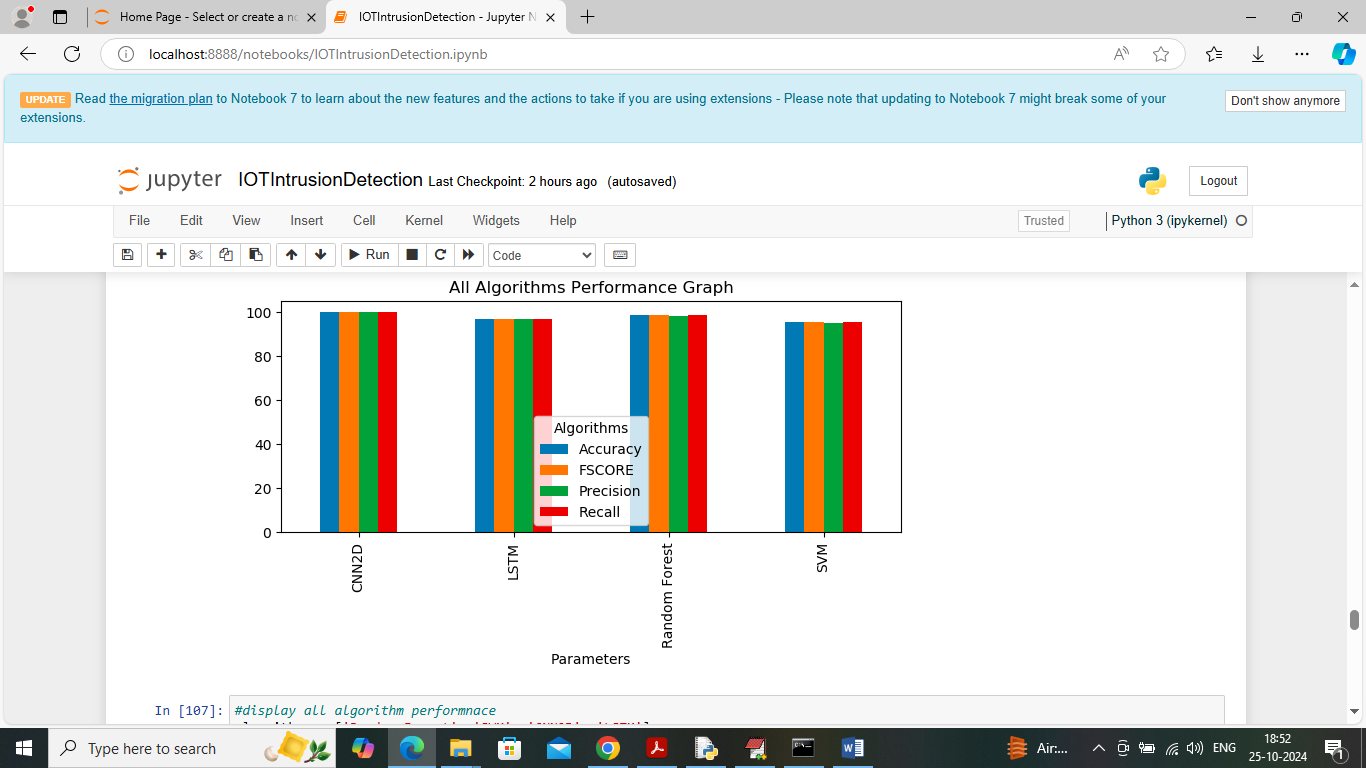
In above screen CNN2D got 100% accuracy and can see other metrics also



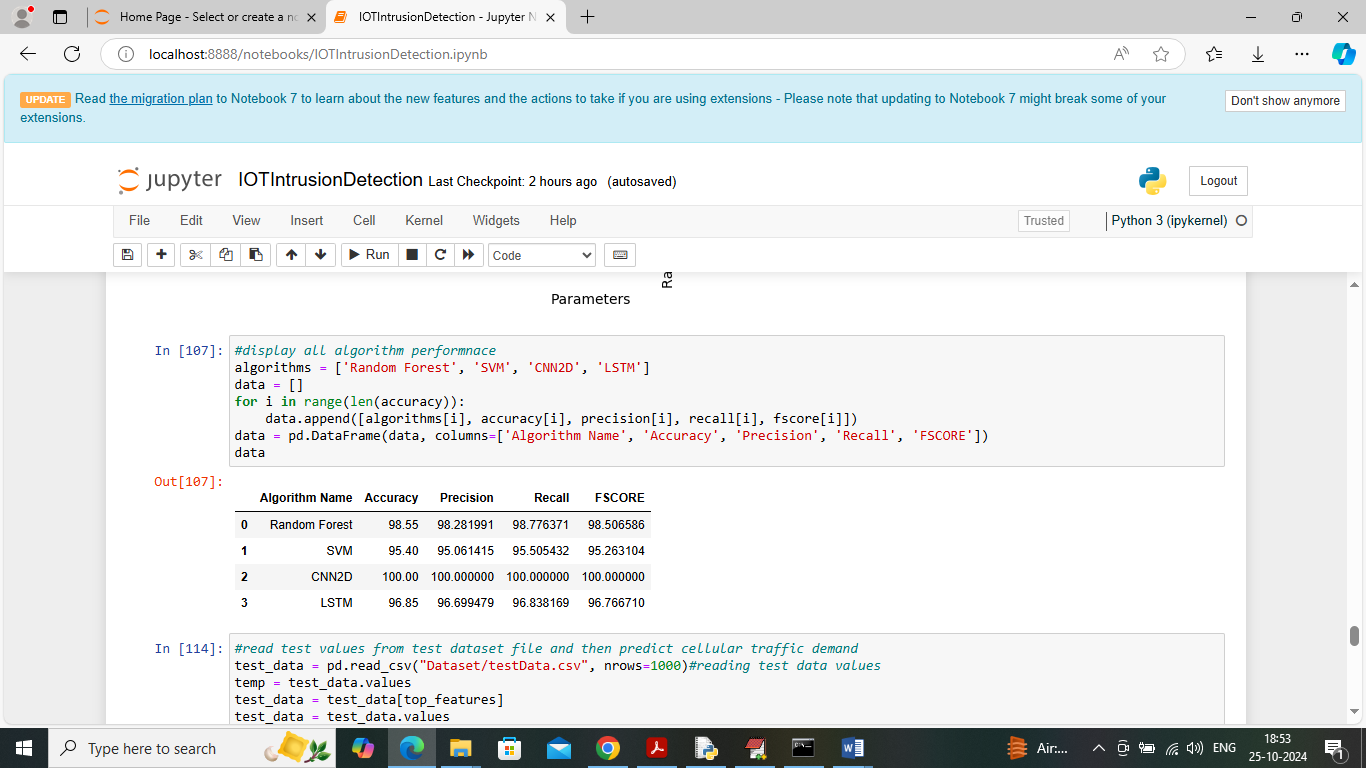
In above screen training LSTM algorithm and can read blue colour comments to know about the algorithm and below is the output of this algorithm



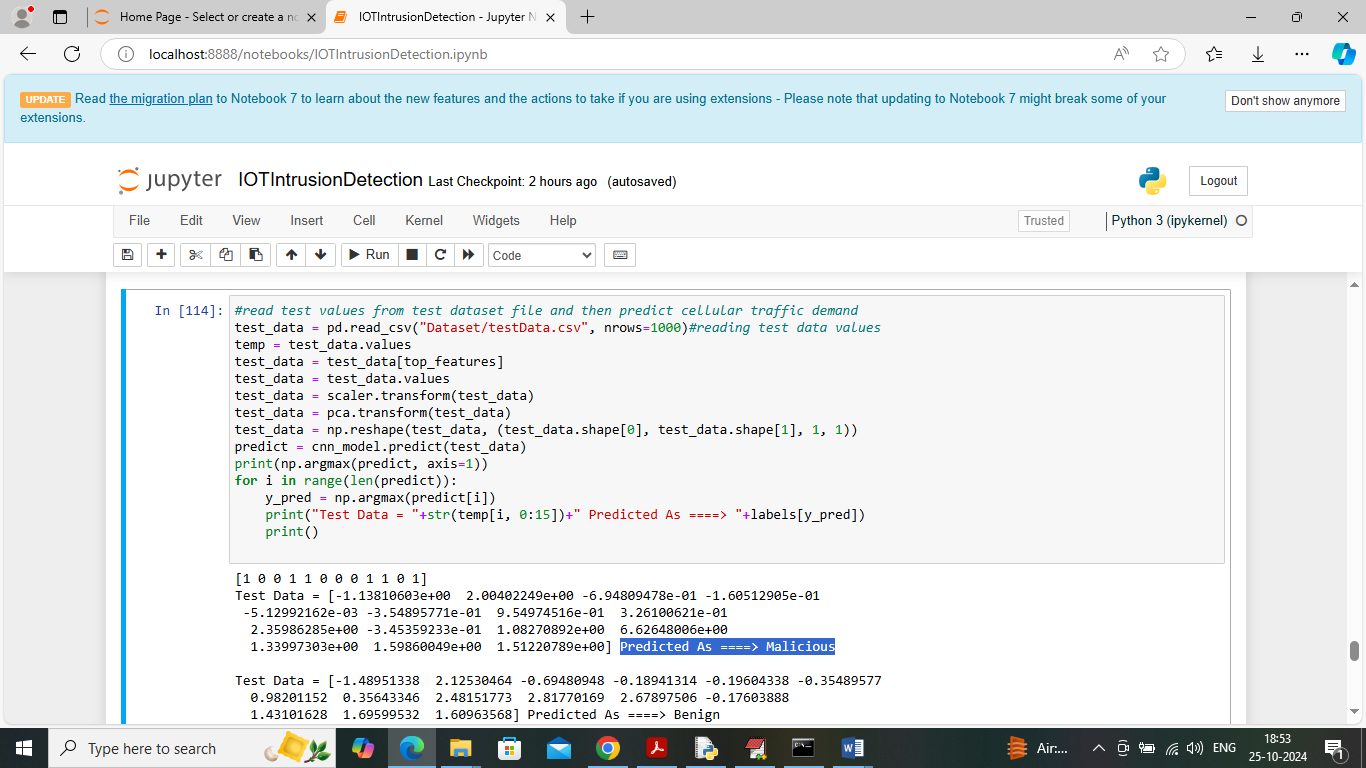
In above screen LSTM got 96% accuracy



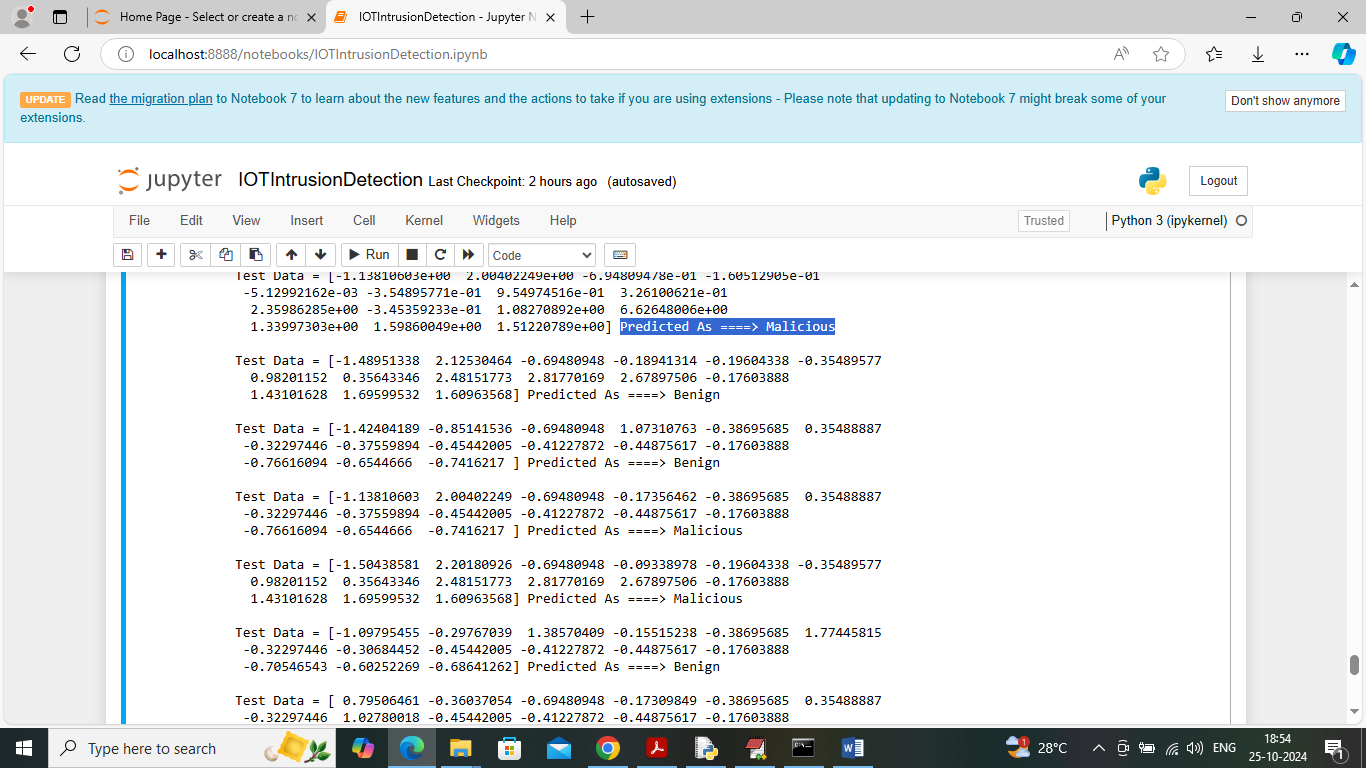
In above screen showing comparison graph between all algorithms where x-axis represents algorithm names and y-axis represents accuracy and other metrics in different colour bars and in all algorithms CNN2D and Random Forest got high performance



In above screen displaying all algorithm performance in tabular format



In above screen reading test data values from test file and then apply processing technique and then applying CNN2D algorithm to predict test data as Benign or Maliciois. In above screen in square bracket can see Test Data values and then after arrow symbol =🡺 can see predicted output as ‘Benign’ or ‘Malicious’.



In above screen can see each test data record classification output as Benign or Malicious.