Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection

In this project author has used Traditional SVM algorithms as existing work and Artificial Neural Network as propose algorithm (ANN). SVM will get trained on dataset without optimizing its features and ANN will filter dataset with different number of input and hidden layers to extract important features or to optimize dataset feature and due to this features optimization ANN will get better prediction accuracy.

After the success of ANN another advance version was introduced called Convolution2D neural network (CNN). CNN will use more number of input and hidden layers to filter dataset and to get more optimized features and due to this reason CNN is better than ANN.

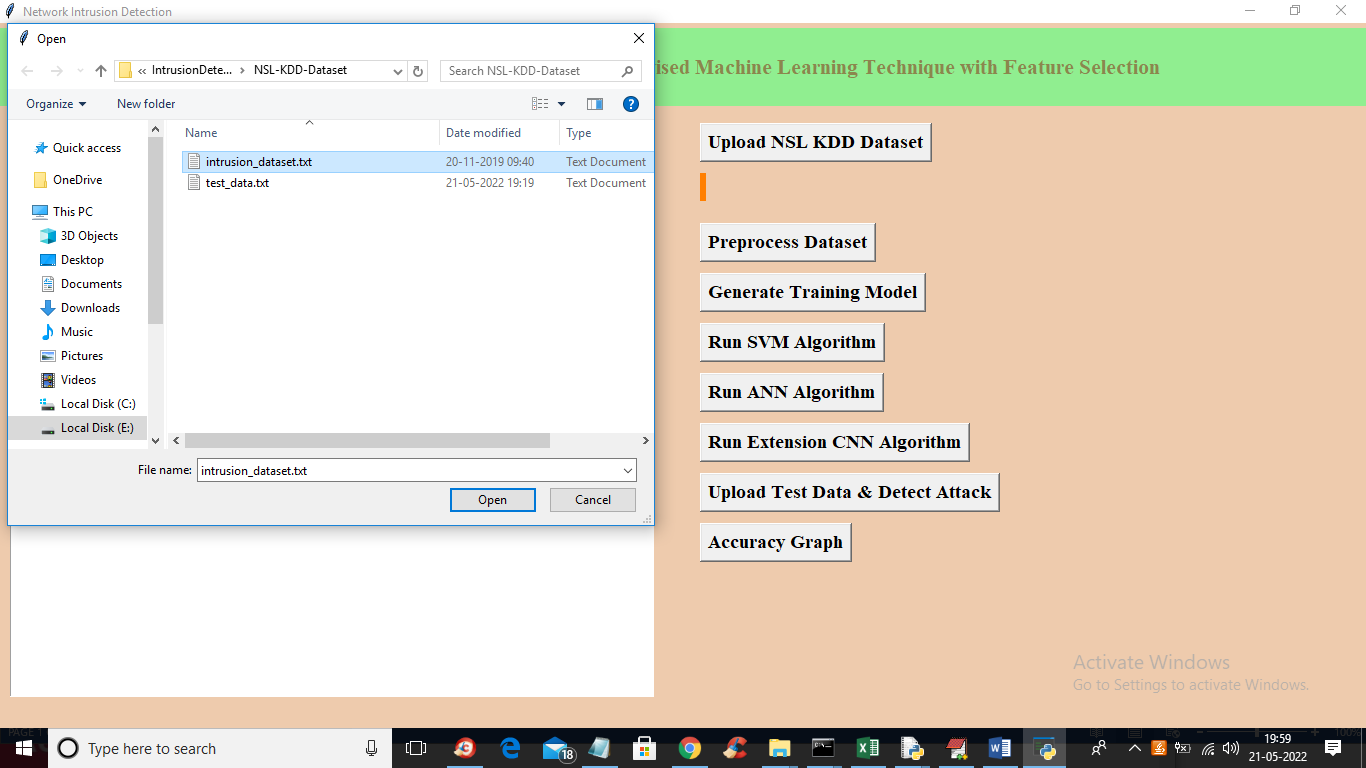
Essential facts about CNNs:

1. CNNs are neuro-biologically-driven by the findings of locally sensitive and orientation-selective nerve cells in the visual cortex.
2. They are a multi-layer neural network.
3. They implicitly extract relevant features.
4. They are a feed-forward network that can extract topological features from dataset.
5. They recognize visual patterns directly from pixel images with minimal Preprocessing.
6. They are astonishingly powerful because they can easily recognize patterns that have extreme variability. e.g., attack NSL dataset.
7. CNNs are trained with a version of the back-propagation algorithm.
8. CNNs have the neuronal cells in the visual cortex, making the base behind CNNs and watches for particular features.

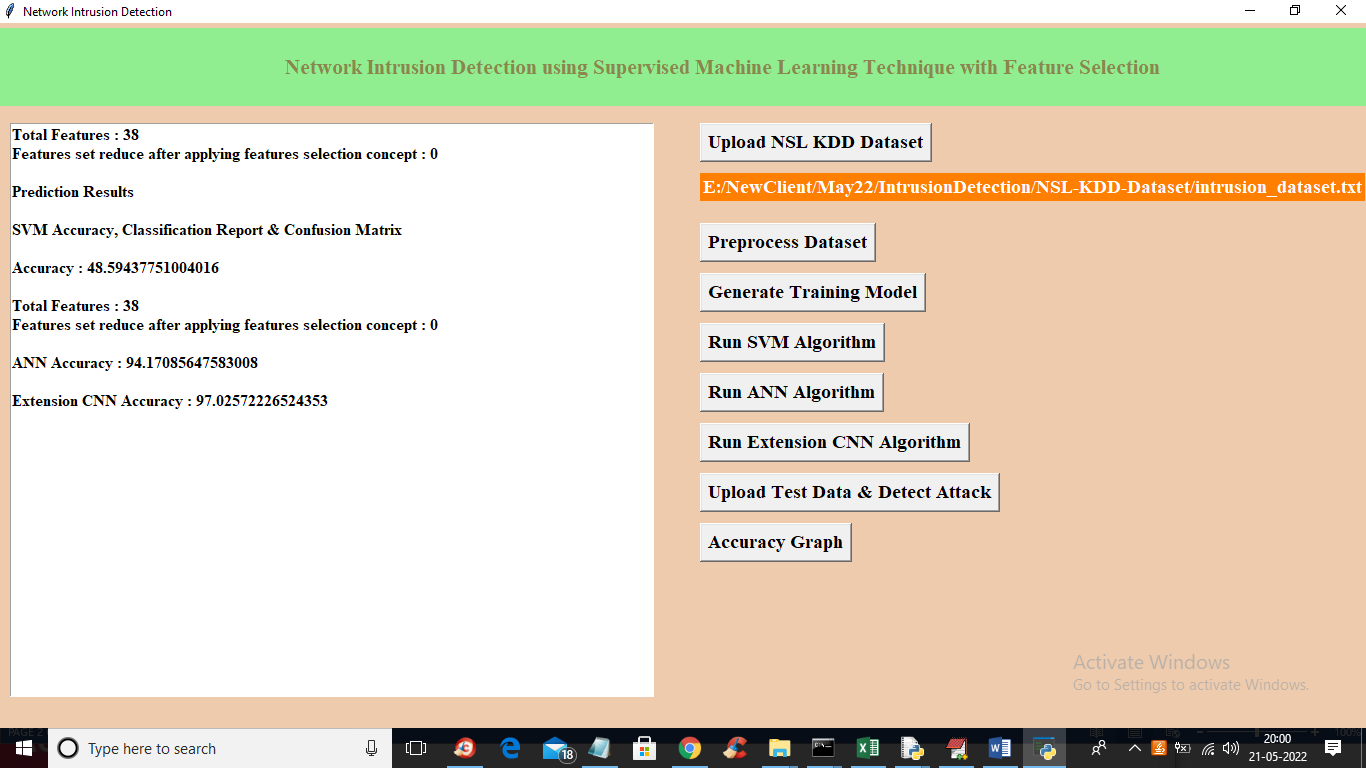
So as extension we have experiment with CNN algorithm and we are getting better accuracy than CNN and then we apply CNN model on test data to predict both NORMAL and malicious signatures.

SCREEN SHOTS

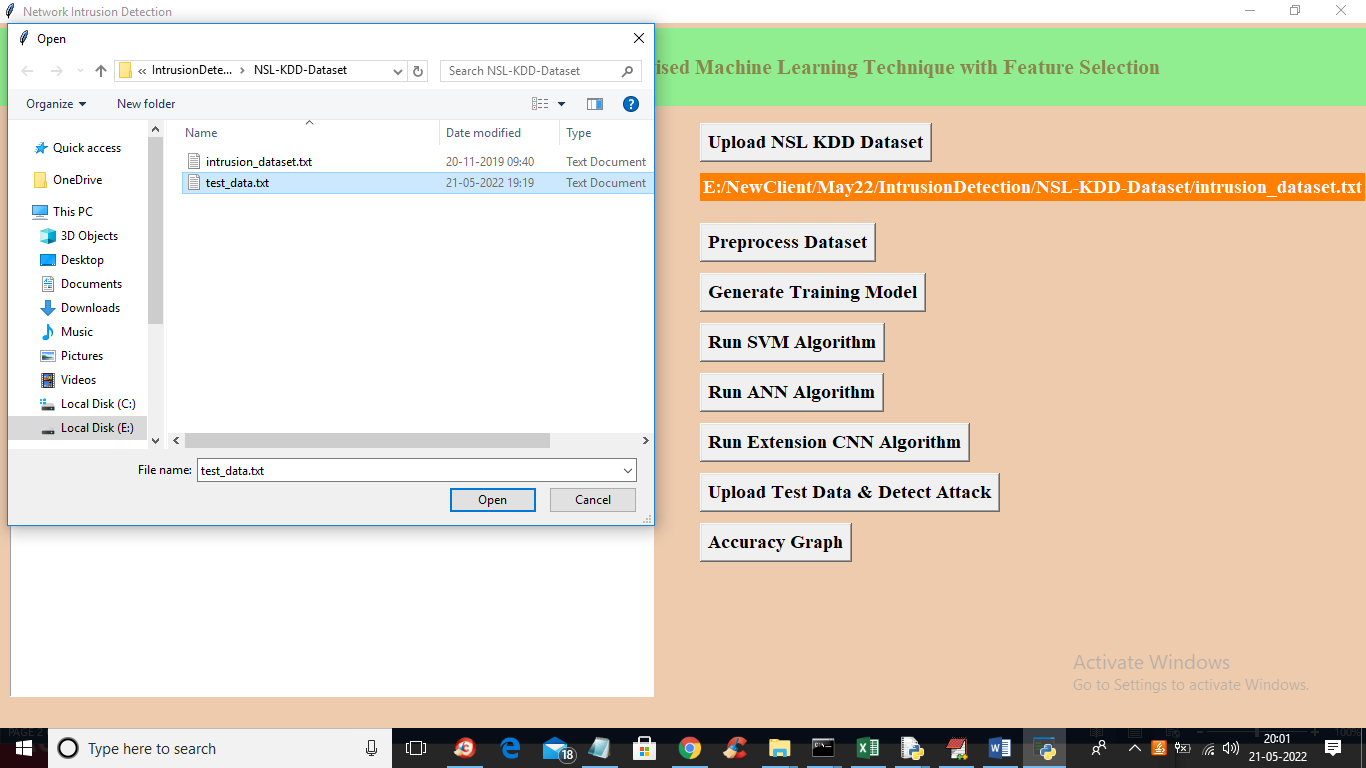
Run project in similar old fashion just I added extra algorithm called CNN and now double click on ‘run.bat’ file to get below output



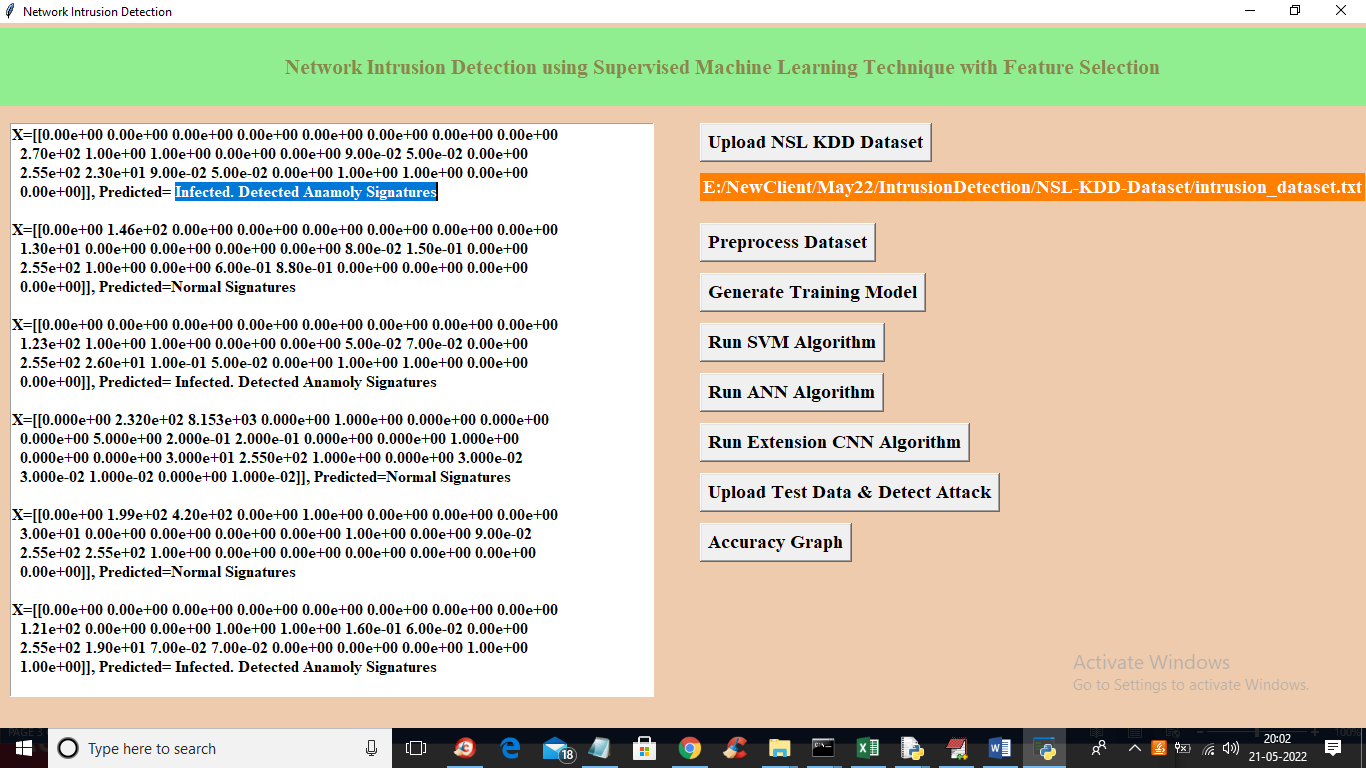
In above screen uploading dataset and then click on all buttons one by one to get below output



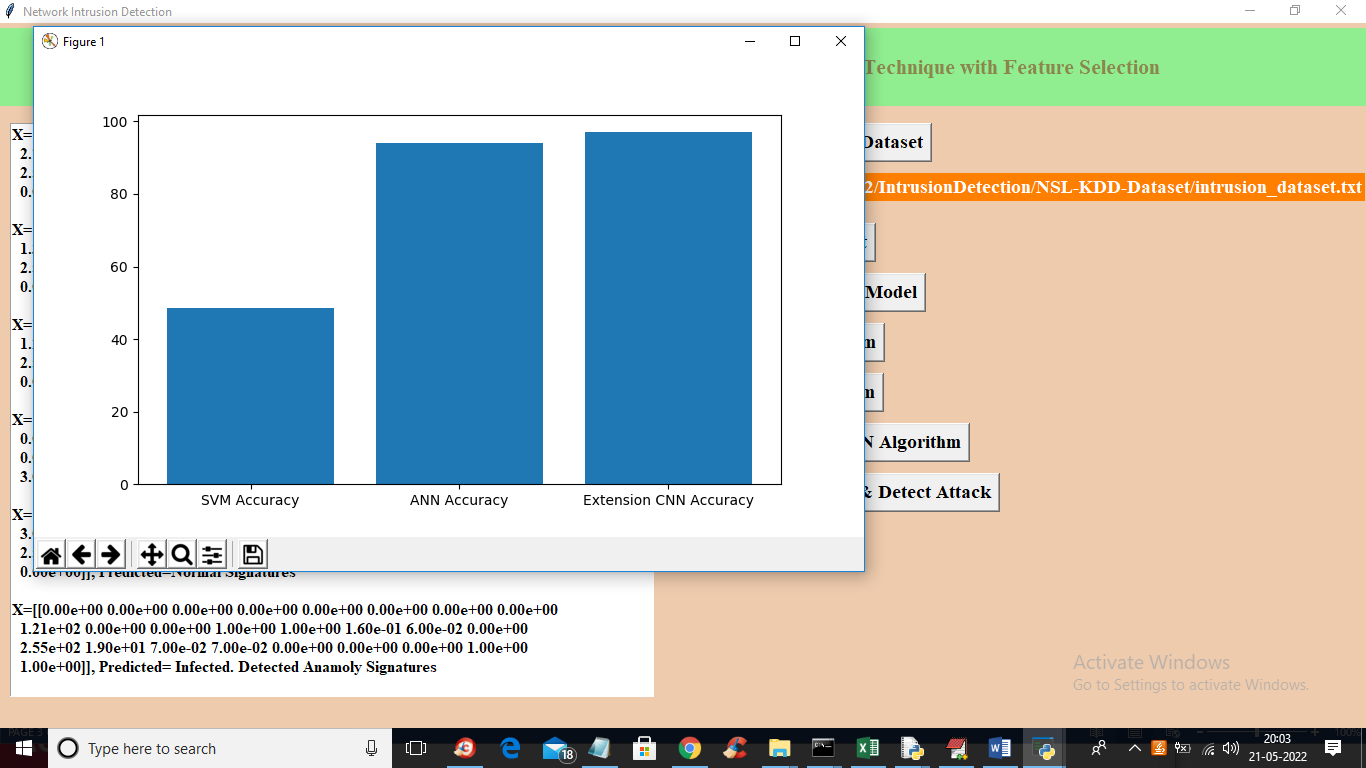
In above screen with SVM we got 48% accuracy and with ANN we got 94% accuracy and with extension CNN we got 97% accuracy and now click on ‘Upload Test Data & Detect Attack’ button to upload test data and get below output



In above screen selecting and uploading test\_data.txt file and then click on ‘Open’ button to get below output



In above screen square bracket contains TEST data and then after square bracket we can see predicted classes as INFECTED or NORMAL and now click on ‘Accuracy Graph’ button to get below output



In above graph x-axis represents algorithm names and y-axis represents accuracy and in all algorithms extension got high accuracy