Packet Inspection to Identify Network Layer Attacks using Machine Learning

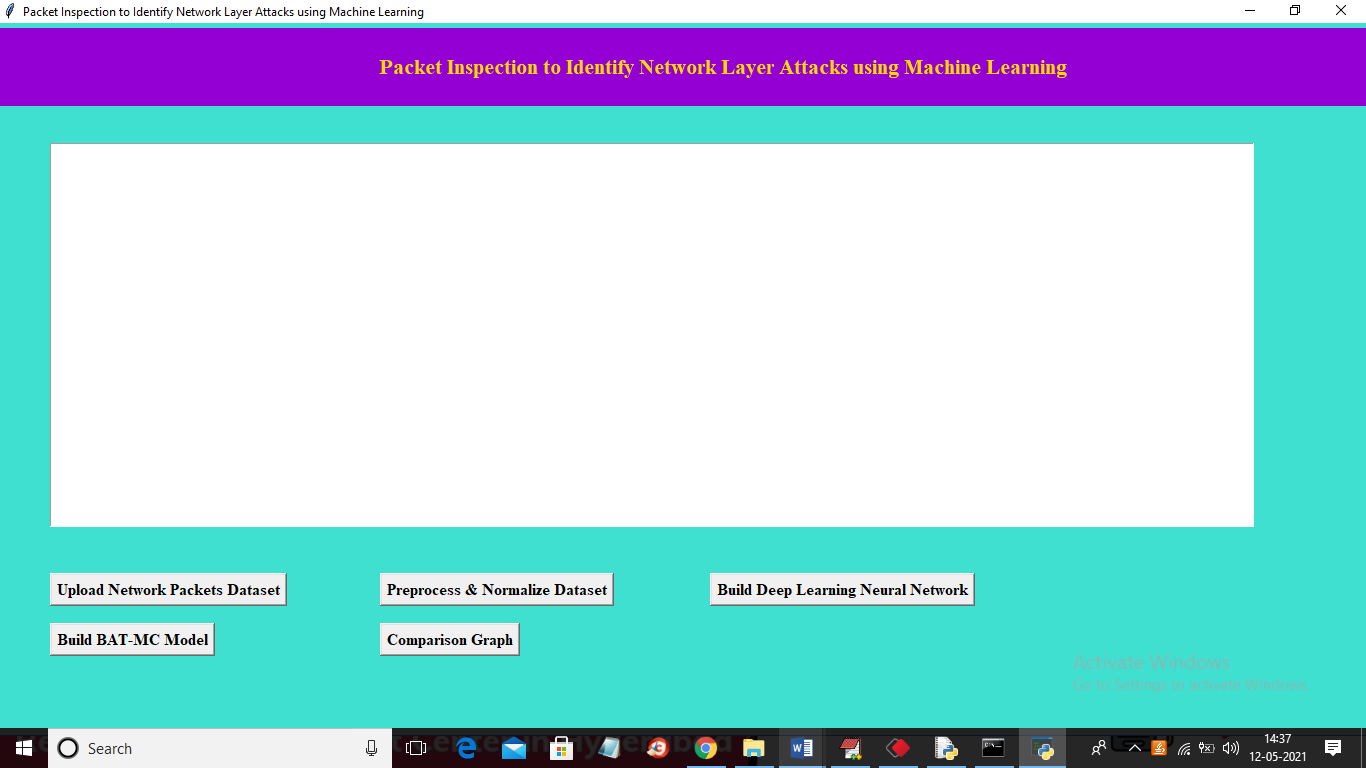
In this paper author is using advance version of LSTM (Long Short Term Memory) algorithm called BLSTM and this algorithm is better in memorizing previous data and can give better prediction result compare to normal LSTM. In this paper author is using BAT-MC BLSTM based deep learning algorithm to predict attacks.

To implement this project we have used KDDCUP and NSL-KDD dataset and then train BAT-MC and Deep learning CNN model to train attack detection model and then compare accuracy between both deep learning CNN and BAT-MC model. From both algorithms BAT-MC is giving better accuracy compare to CNN.

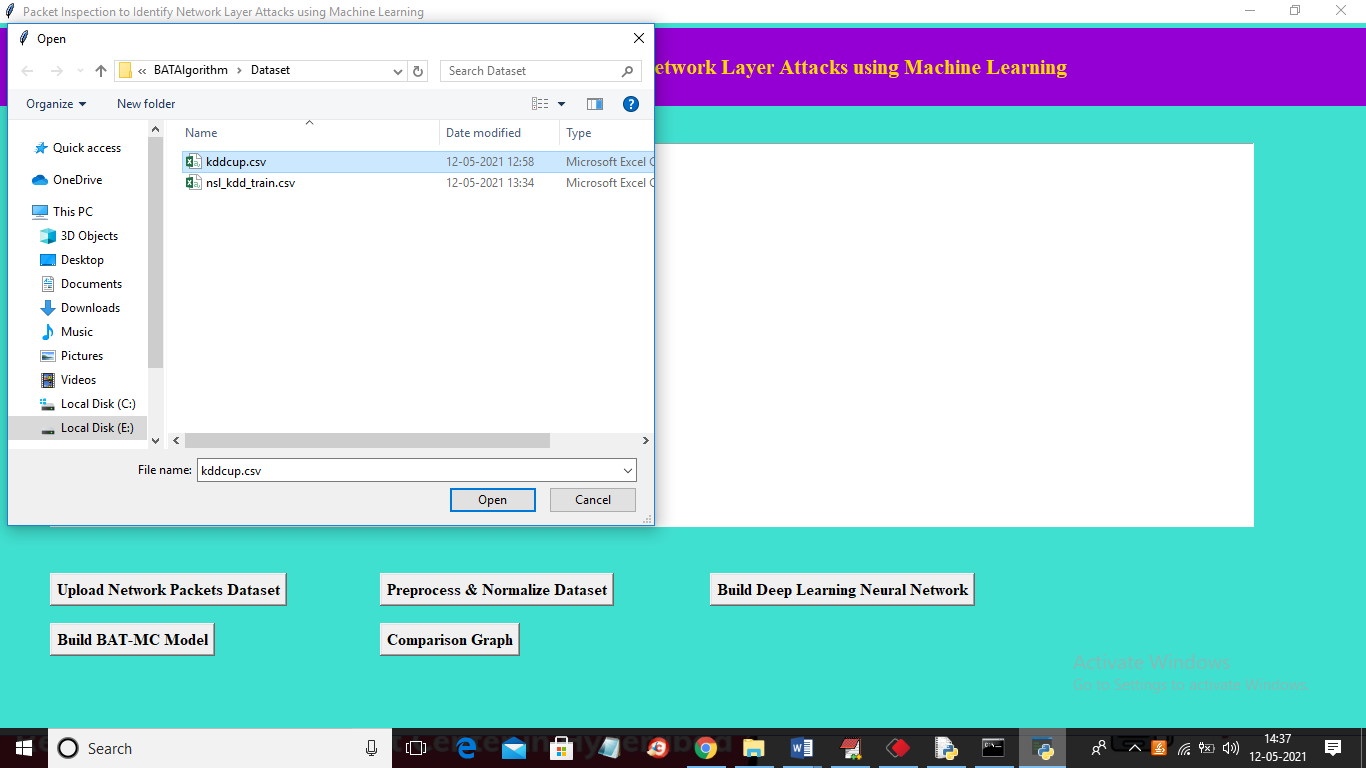
Training dataset is available inside ‘Dataset’ folder

Screen shots

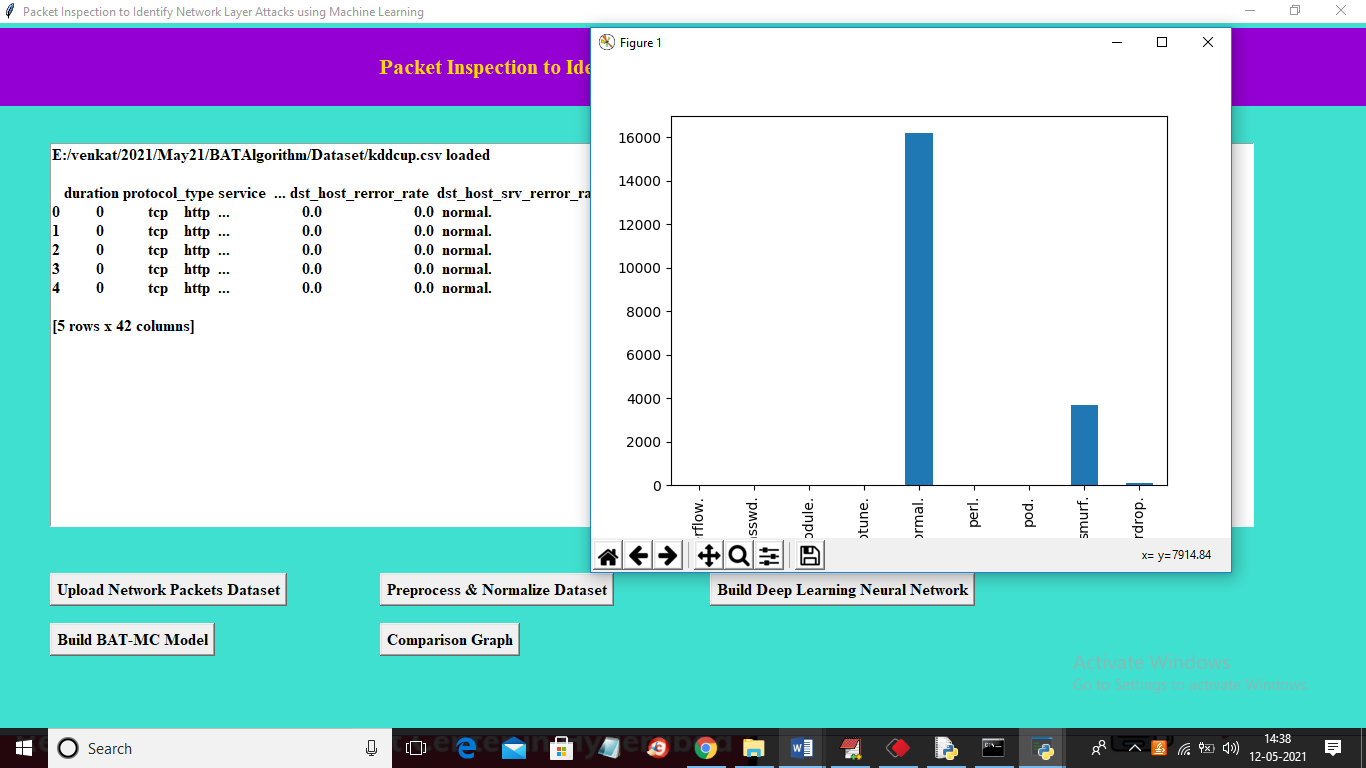
To run project double click on ‘run.bat’ file to get below screen



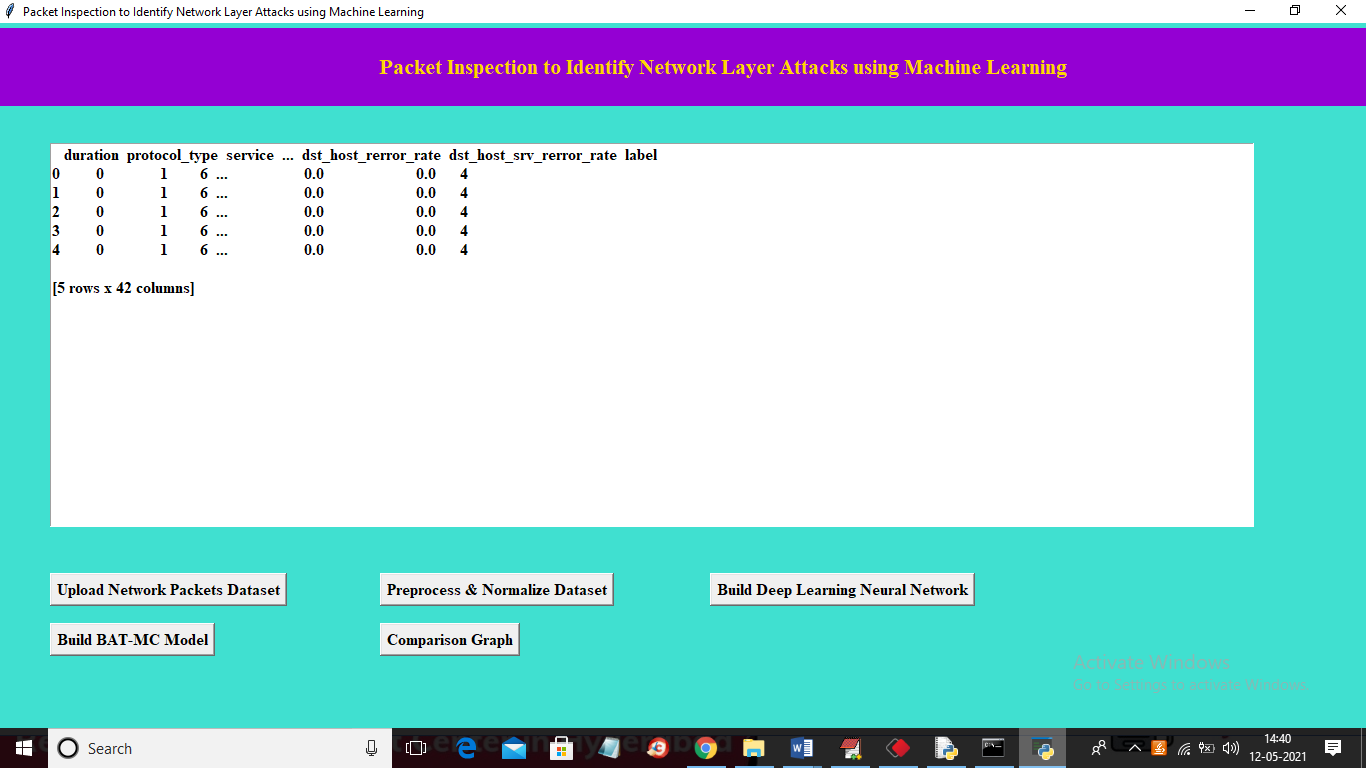
In above screen click on ‘Upload Network Packets Dataset’ button to upload dataset and to get below screen



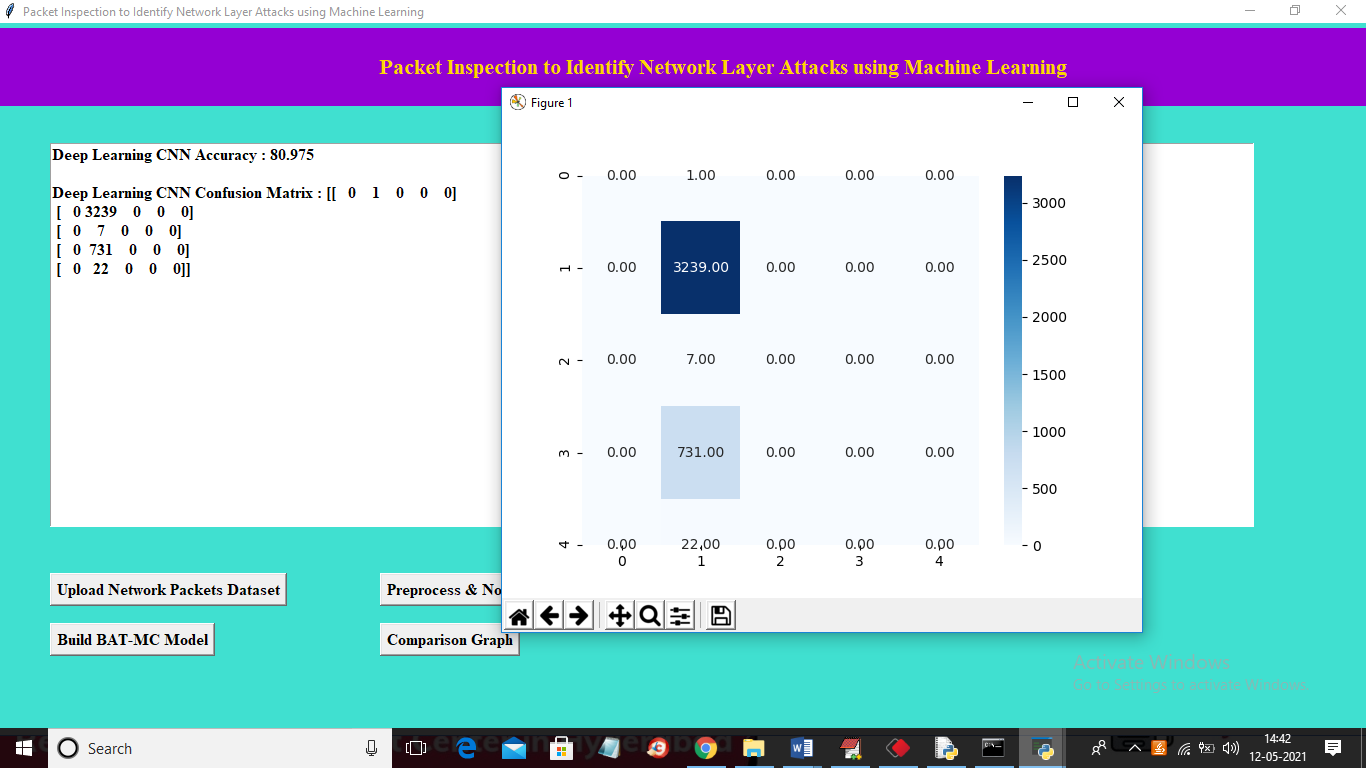
In above screen selecting and uploading ‘kddcup.csv’ file and then click on ‘Open’ button to load dataset and to get below screen



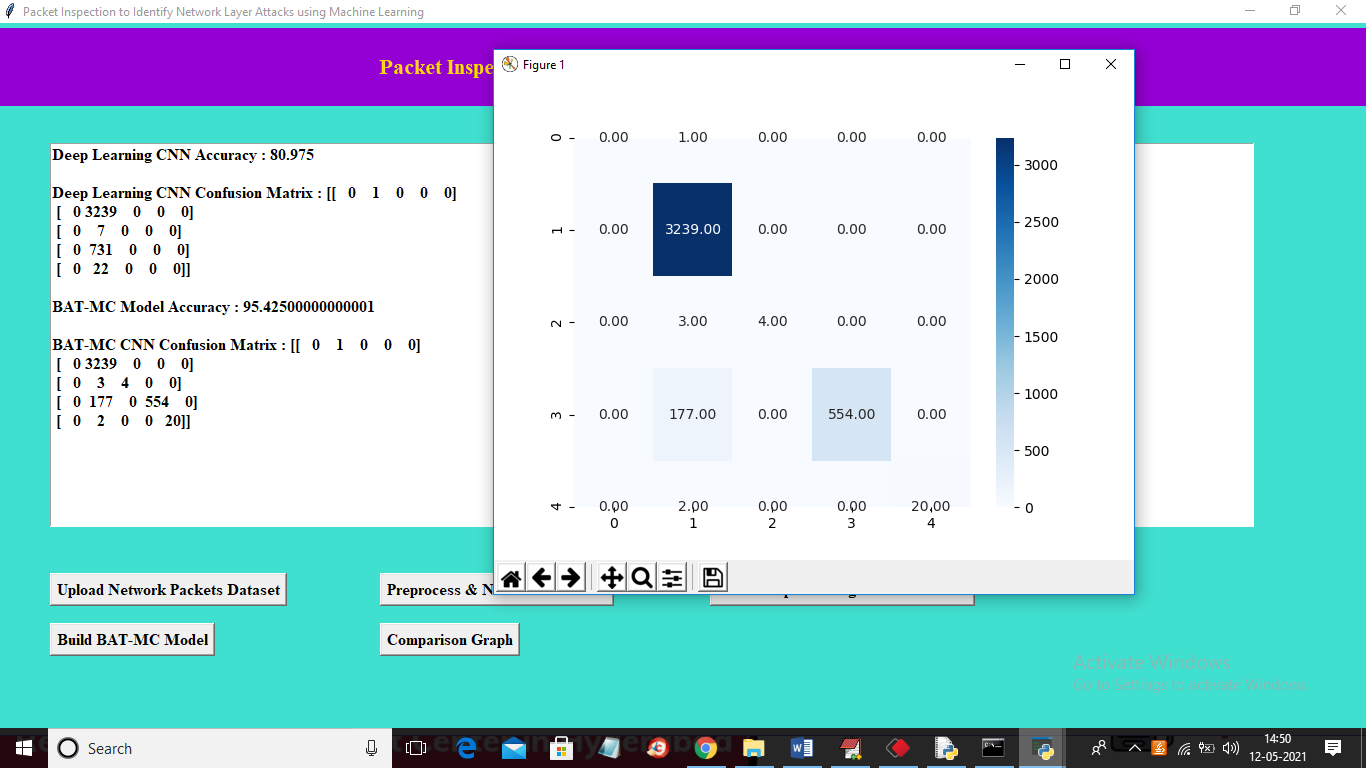
In above screen in text area we can see dataset loaded and we can see data contains alpha numeric data and ML algorithms accept only numeric values so we need to preprocess and normalize them and in graph we can see different attack names in x-axis and total attack types on y-axis and now close above graph and then click on ‘Preprocess & Normalize Dataset’ button to normalize data



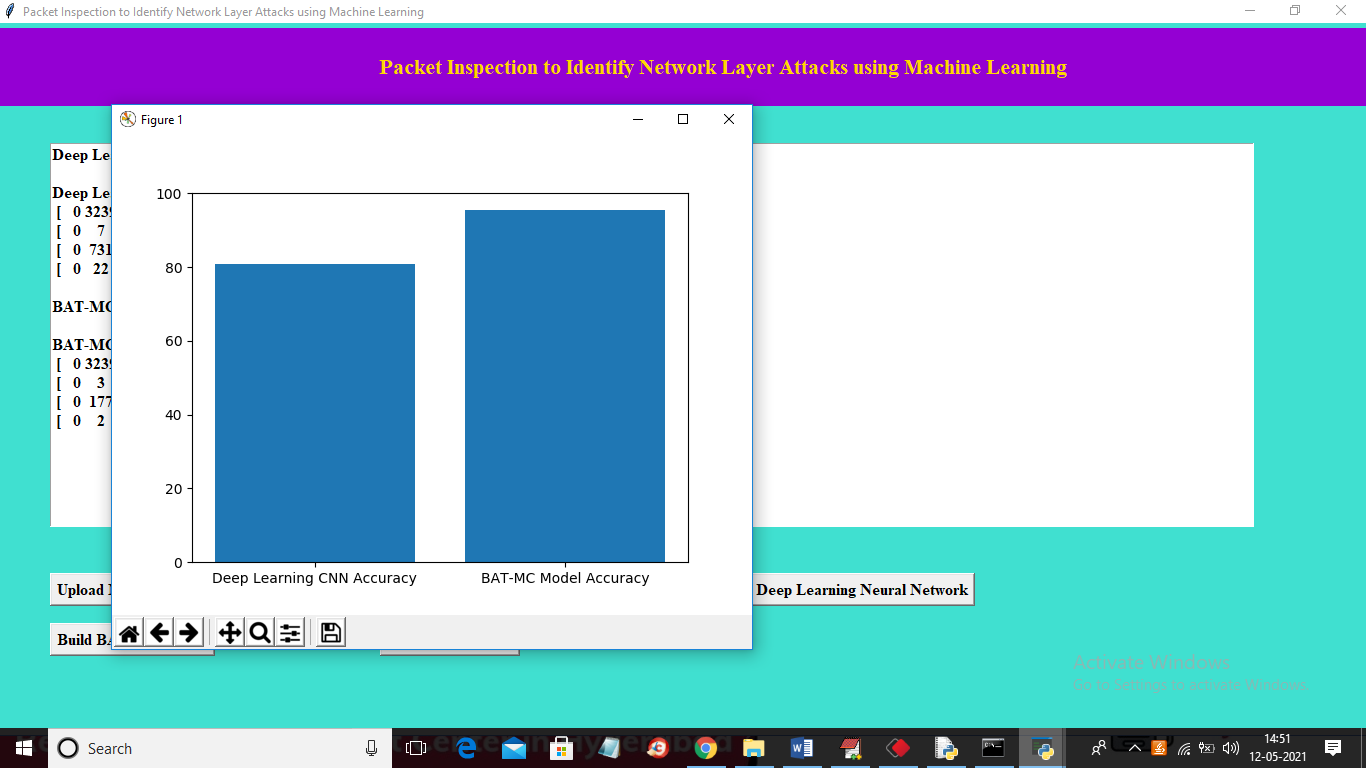
In above screen we can see dataset converted to numeric values by assigning ID’s to each unique non-numeric data and now dataset is ready and now click on ‘Build Dee Learning Neural Network’ button to train CNN above dataset and then calculate prediction accuracy



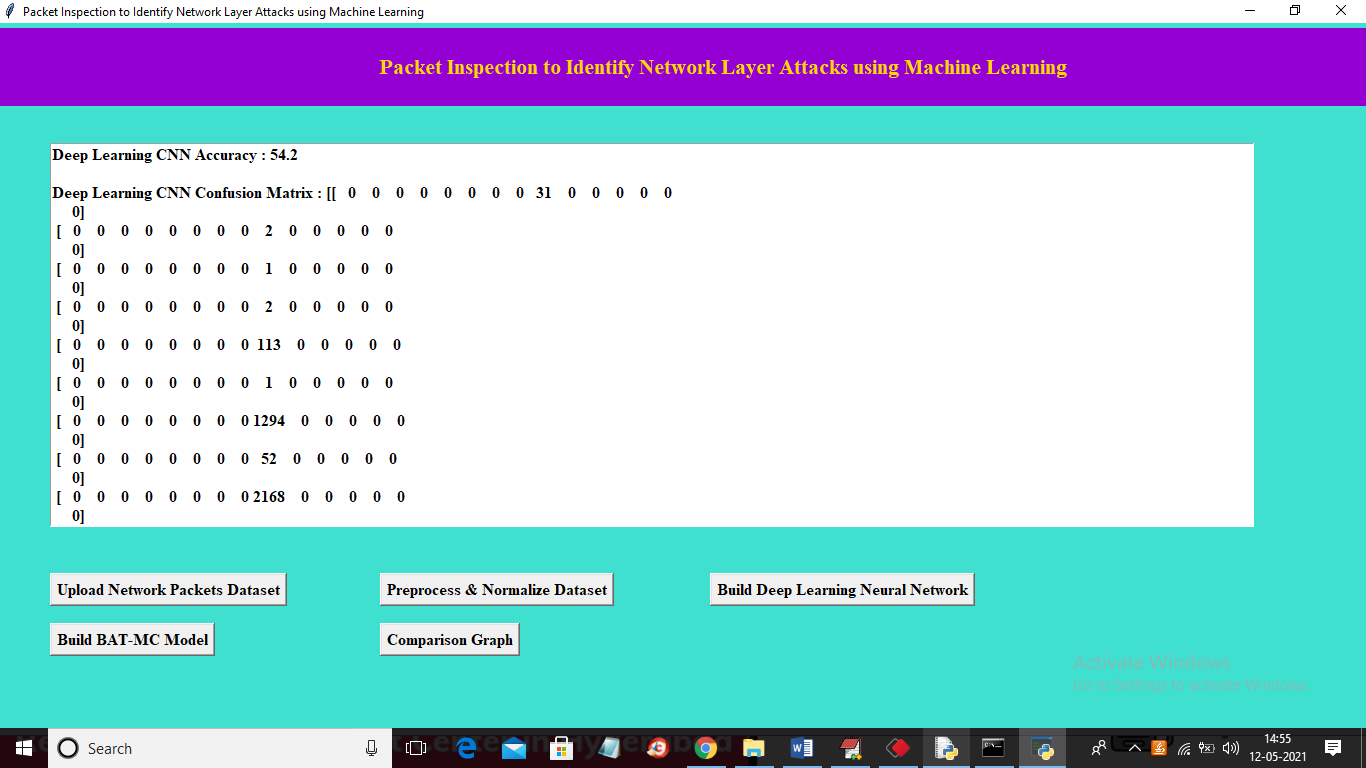
In above screen we can see CNN algorithm got 80% accuracy and in confusion matrix we can see total 5 different attacks are found and in confusion matrix we can see which attack predicted how many times. For example attack 2 predicted 3239 times in entire test data. Now close above graph and then click on ‘Build BAT-MC Model’ to train above dataset with BLSTM algorithm and then calculate prediction accuracy on test data.



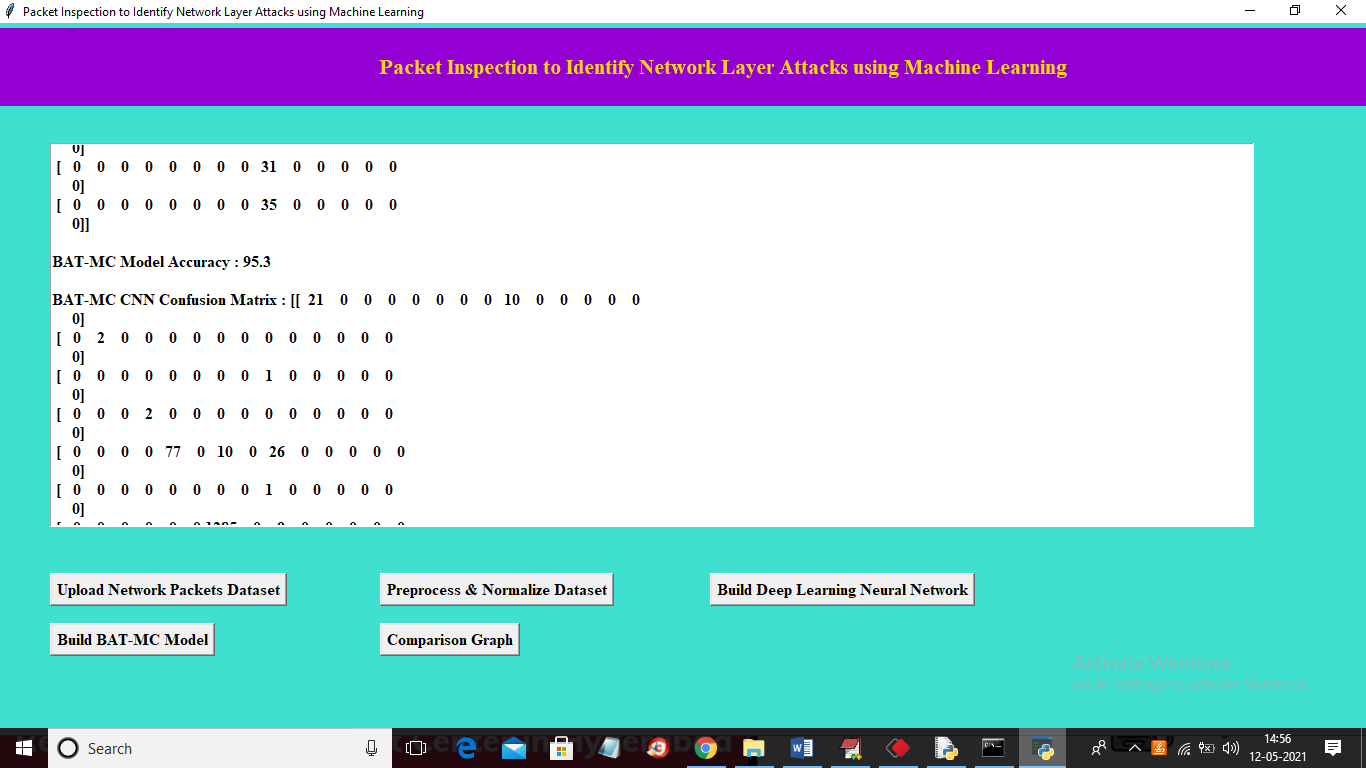
In above screen BAT-MC model generated and its prediction accuracy is 95 and now close above graph and then click on ‘Comparison Graph’ button to get below graph



In above graph x-axis represents algorithm name and y-axis represents accuracy and in both algorithm BAT-MC model is giving better accuracy. Similarly you can upload other dataset and can build CNN and BAT-MC model. In below screen you can see NSL dataset accuracy

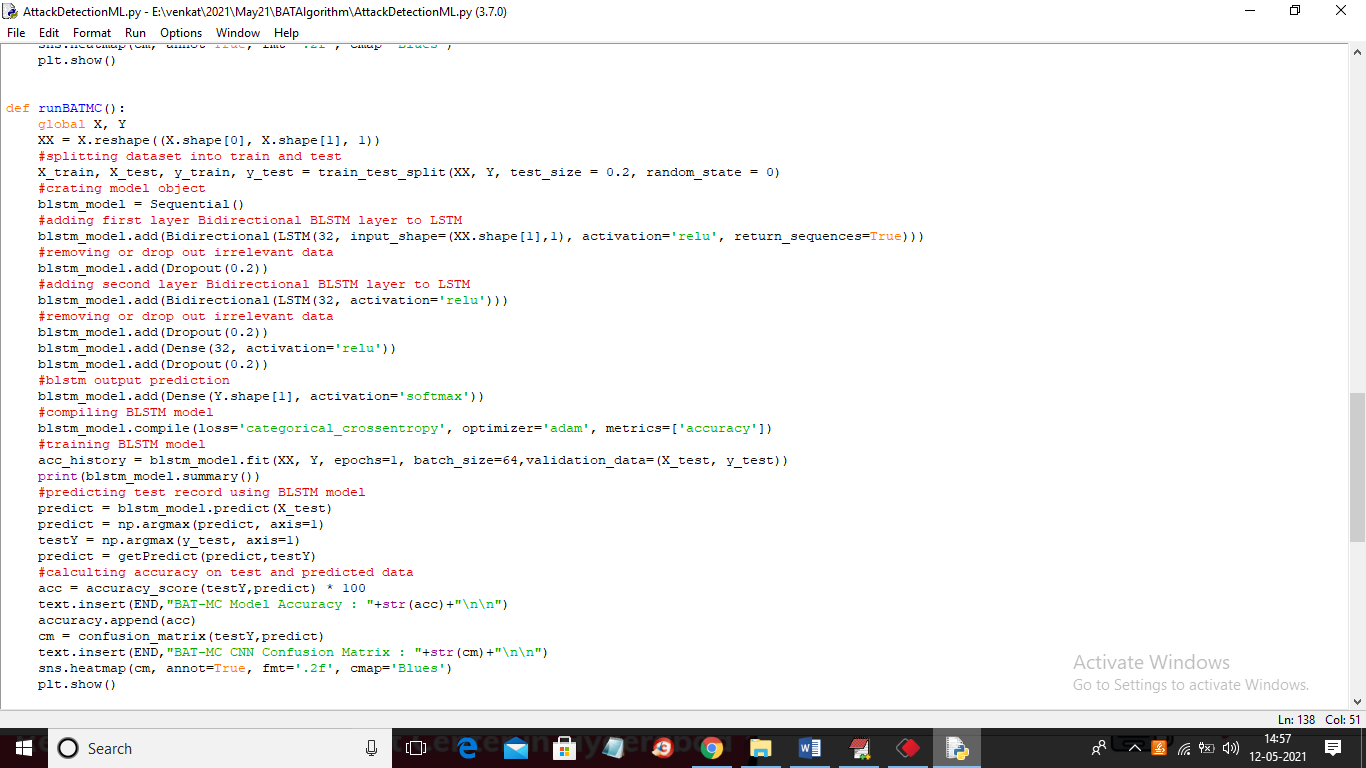


In above screen CNN got 54% accuracy and then scroll down above text area to get BAT-MC accuracy



In above screen BAT-MC got 95% accuracy

Below code screen showing how we are creating BLSTM model to build attack detection model



In above screen read red colour comments to understand development of BAT-MC model