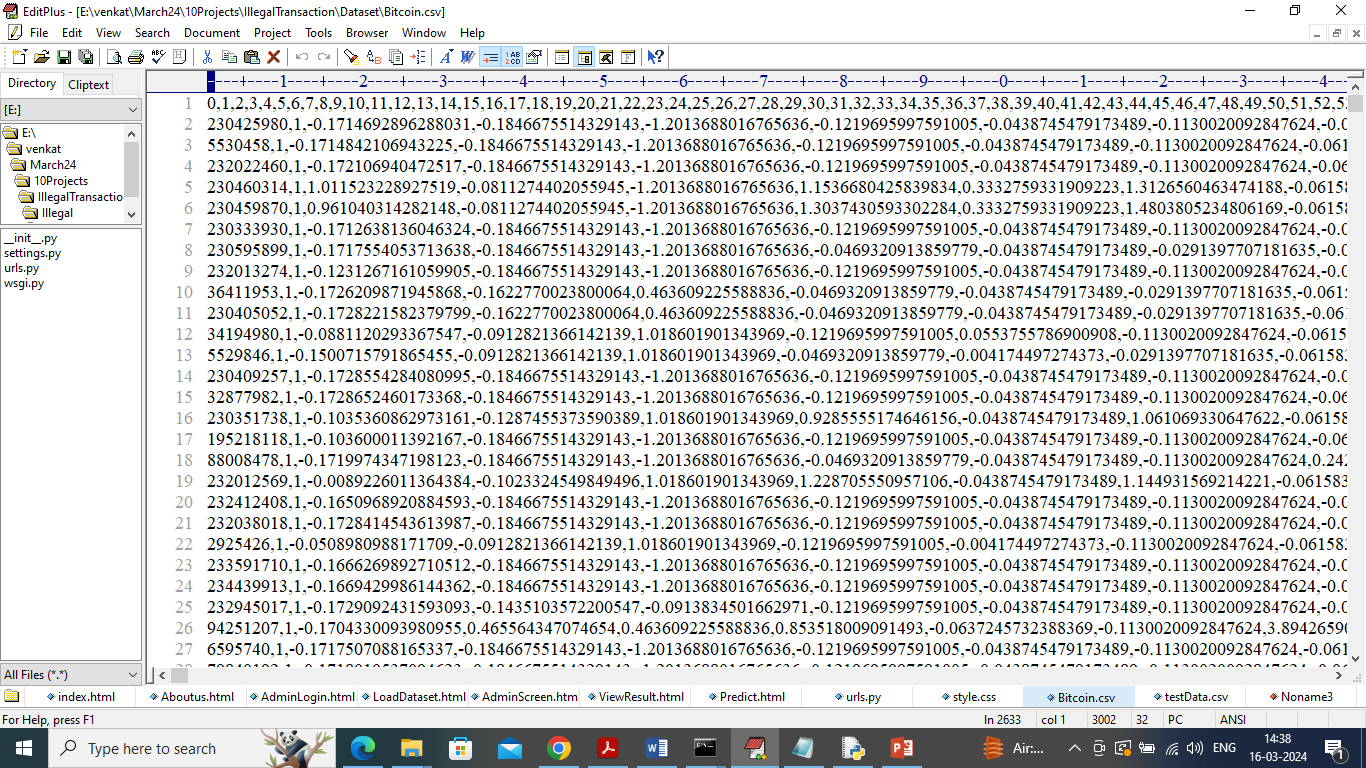
A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain

The rapid growth of cryptocurrency transactions has led to an increase in illegal activities, posing a threat to the security and legality of the digital financial ecosystem. This paper proposes a robust application to detect and prevent illegal cryptocurrency transactions using a deep learning approach. The proposed application extracts patterns from a large dataset of cryptocurrency transactions to train a convolutional neural network (CNN) model. The CNN model is then used to identify suspicious transactions and flag them for further investigation.

The proposed application has the potential to help law enforcement agencies and financial institutions to detect and prevent illegal cryptocurrency transactions, thereby improving the security and legality of the digital financial ecosystem.

We have compared propose CNN algorithm performance using various ML algorithms like Decision Tree, Gradient Boosting, Logistic Regression, KNN etc. Each algorithm performance is evaluated in terms of accuracy, precision, recall and FSCORE.

To train and test above algorithms we have utilized CHAINANALYSIS dataset which contains various illegal transaction dataset details. In below screen showing dataset details



In above dataset screen first row contains dataset column names and remaining rows contains dataset values and in last column we have class labels as ‘Exchange, Gambling or darknet-market’.

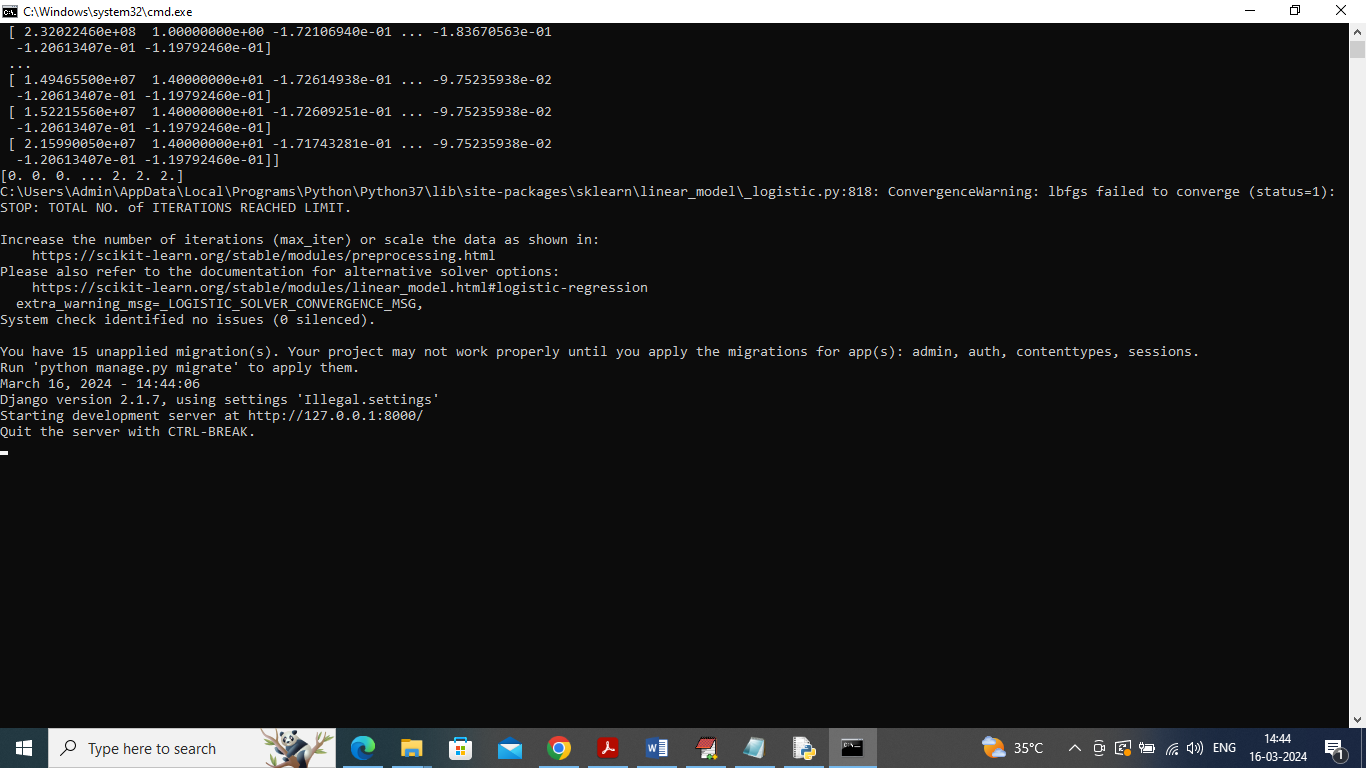
So by using above dataset we will train and test all algorithm performances

To designed this project we have designed following modules

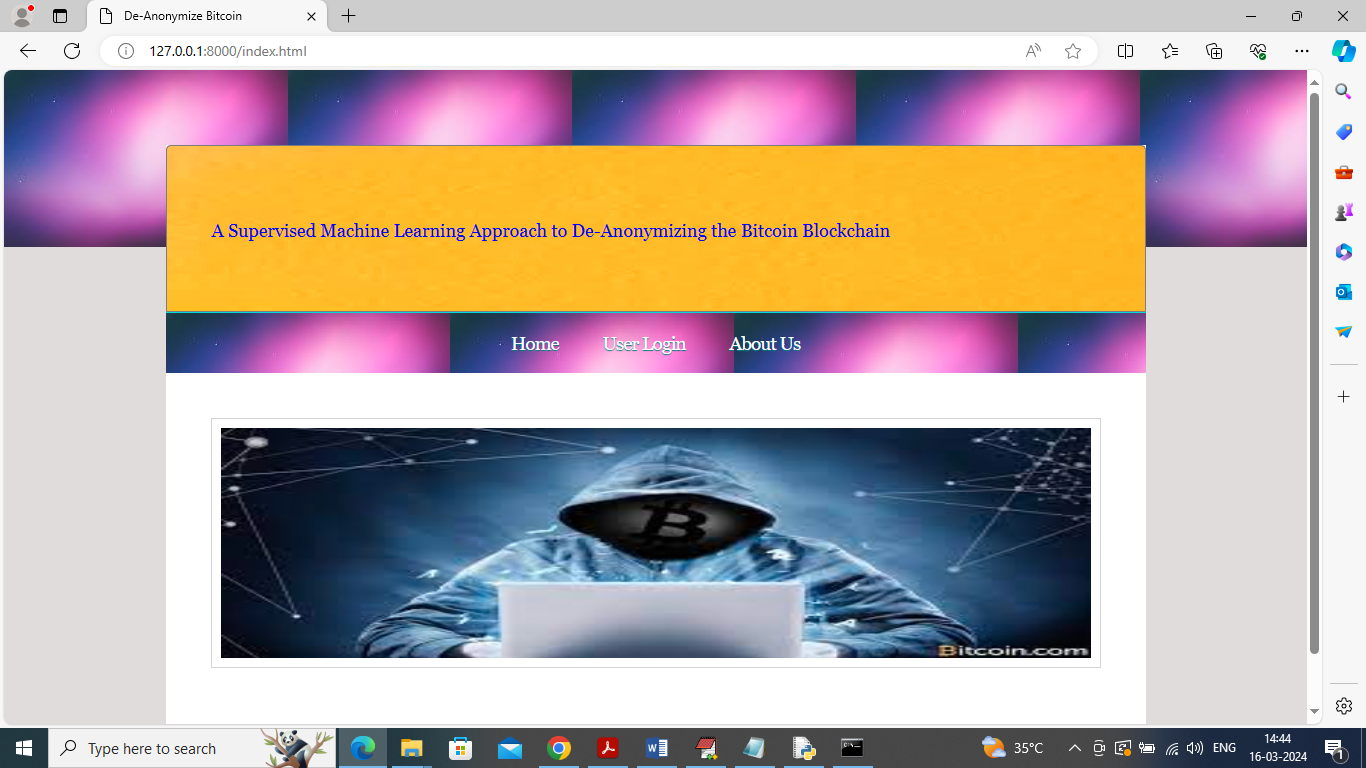
1. User Login: user can login to system using username and password as admin and admin
2. Load & Process Dataset: using this module user can upload dataset to application and then application will remove missing values, shuffles and normalize dataset values. After processing application will split dataset into train and test where application using 70% for training and 20% for testing
3. Train ML Algorithms: using this module application will train ML and propose CNN algorithm and then calculate accuracy on test data
4. De-Anonymize Transaction: using this module user can upload test data and then CNN will predict transaction type

SCREEN SHOTS

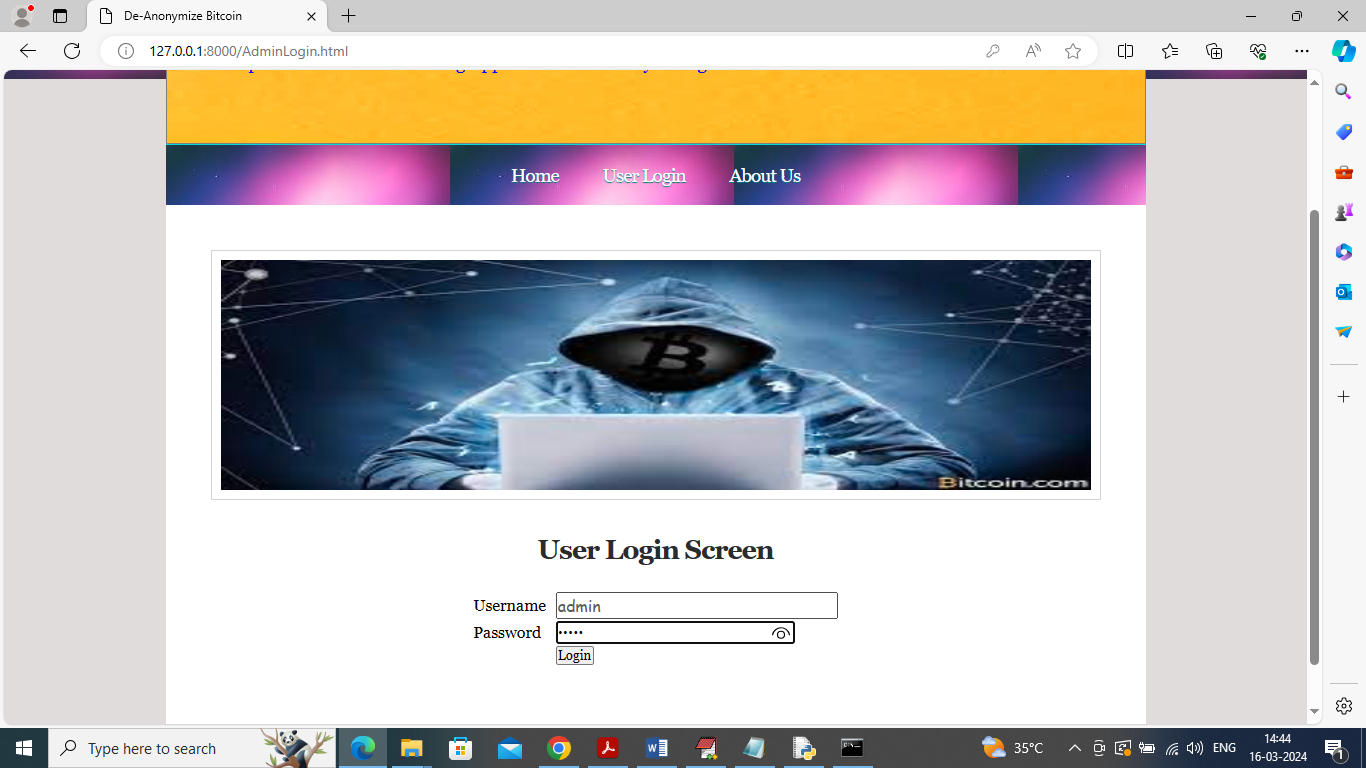
To run project double click on run.bat file to get below screen



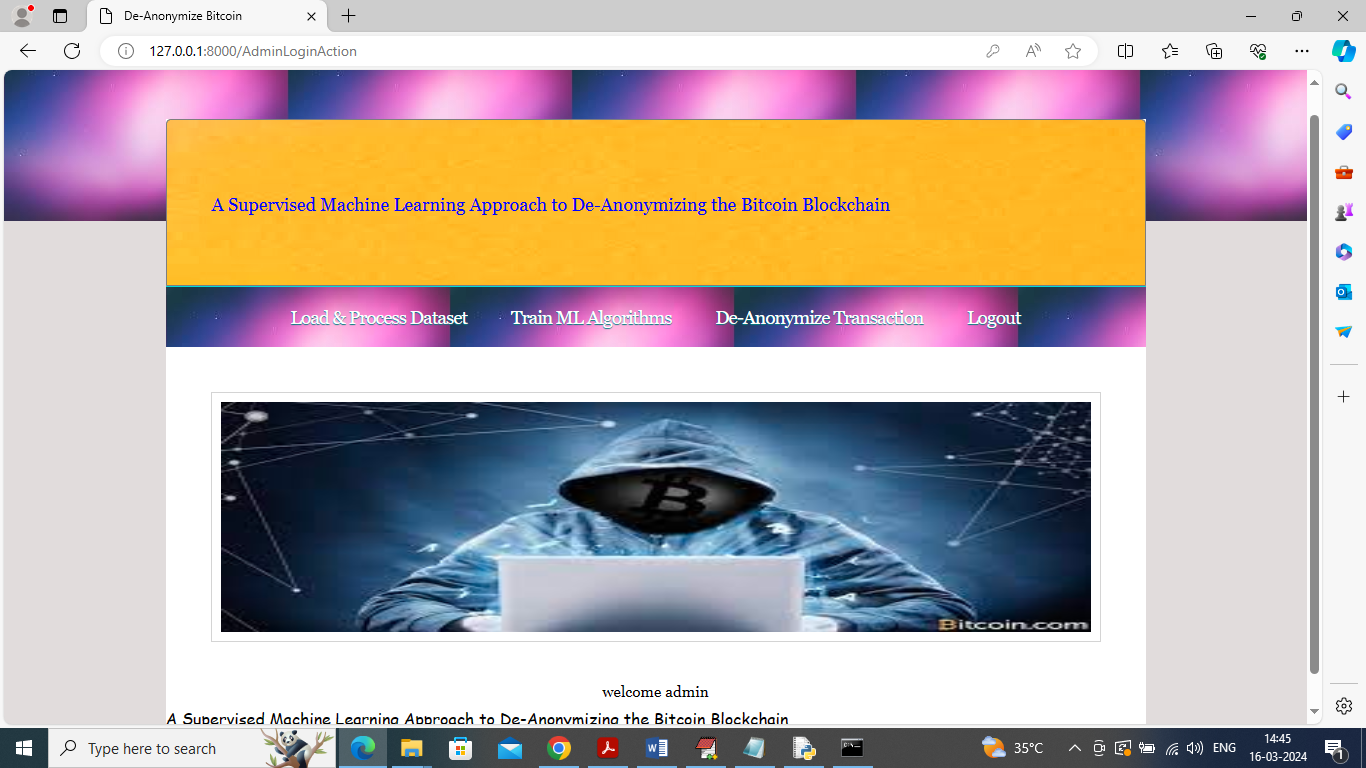
In above screen python server started and now open browser and enter URL as <http://127.0.0.1:8000/index.html> and press enter key to get below page



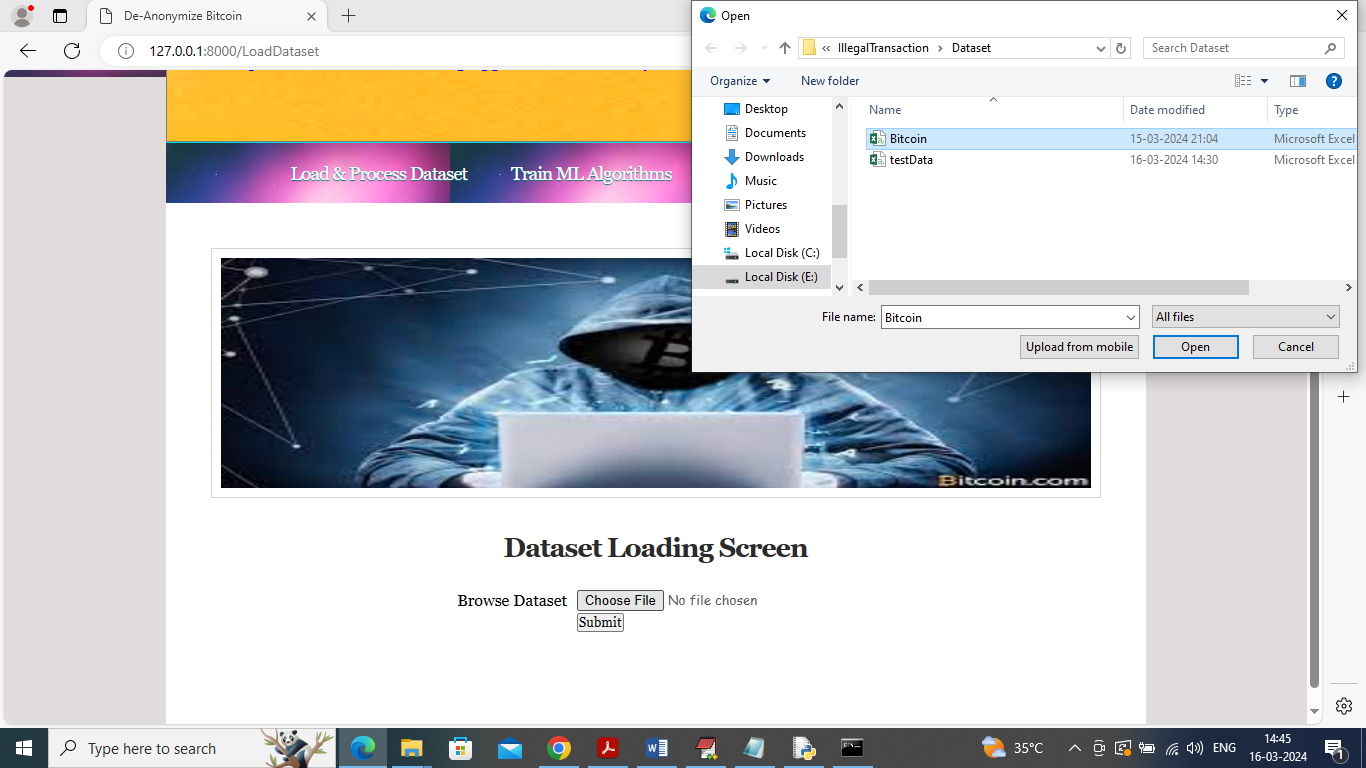
In above screen click on ‘User Login’ link to get below page



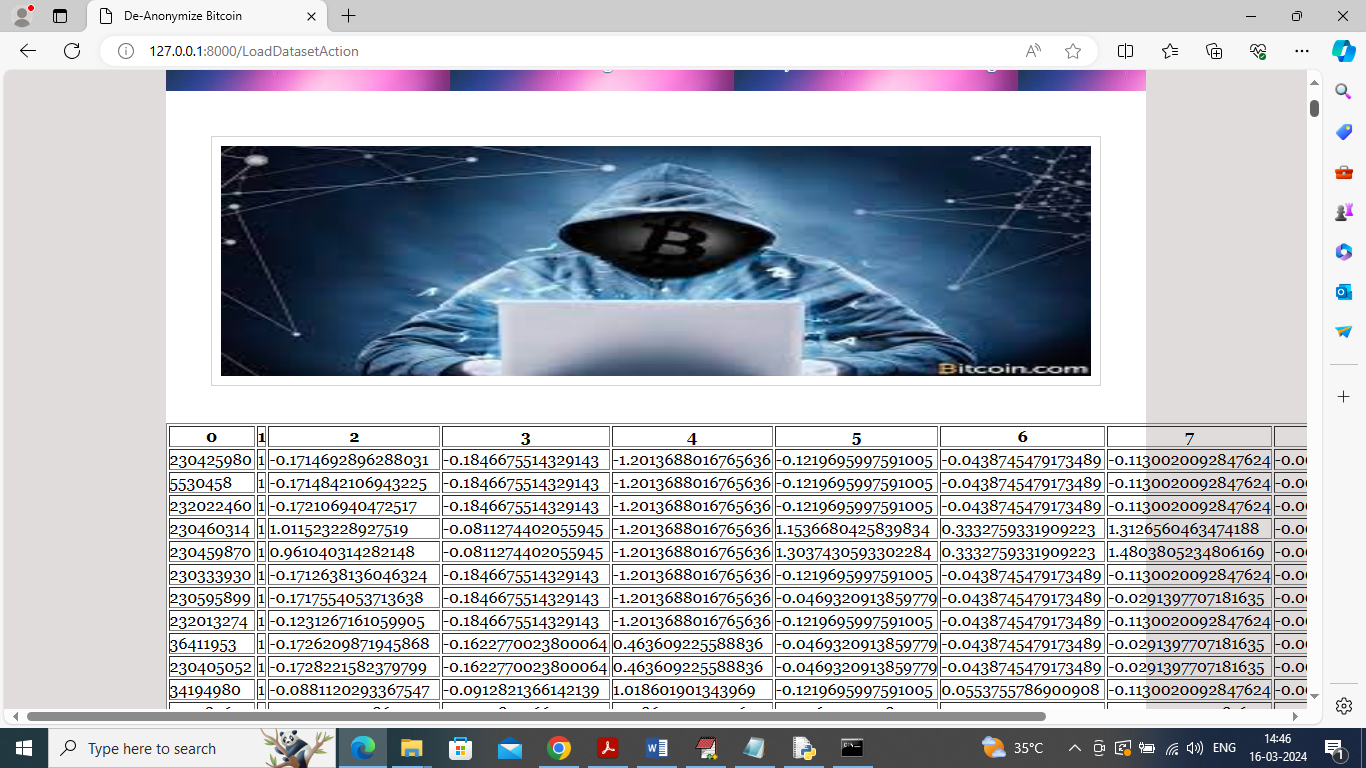
In above screen user is login and after login will get below page



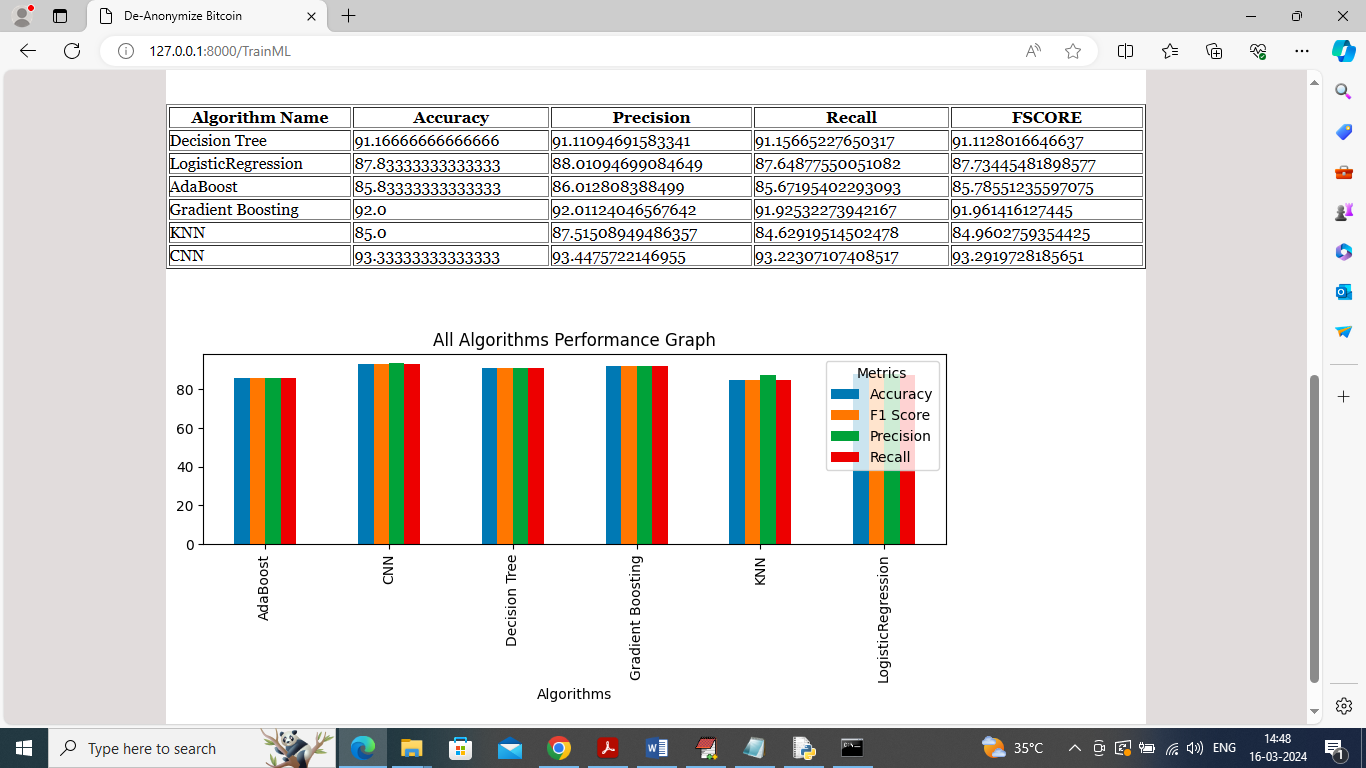
In above screen click on ‘Load & Process Dataset’ link to upload dataset and get below page



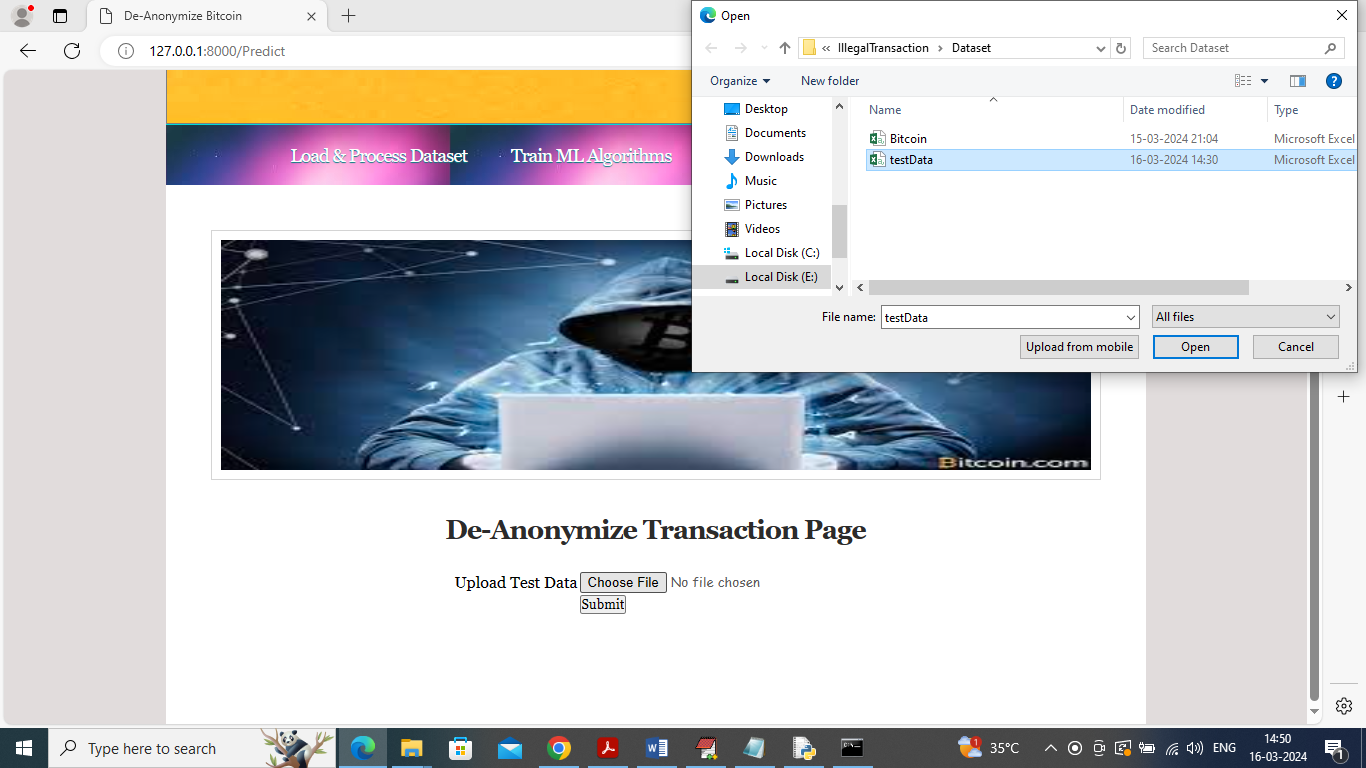
In above screen selecting and uploading dataset file and then click on ‘Open’ button to load and process dataset and get below page



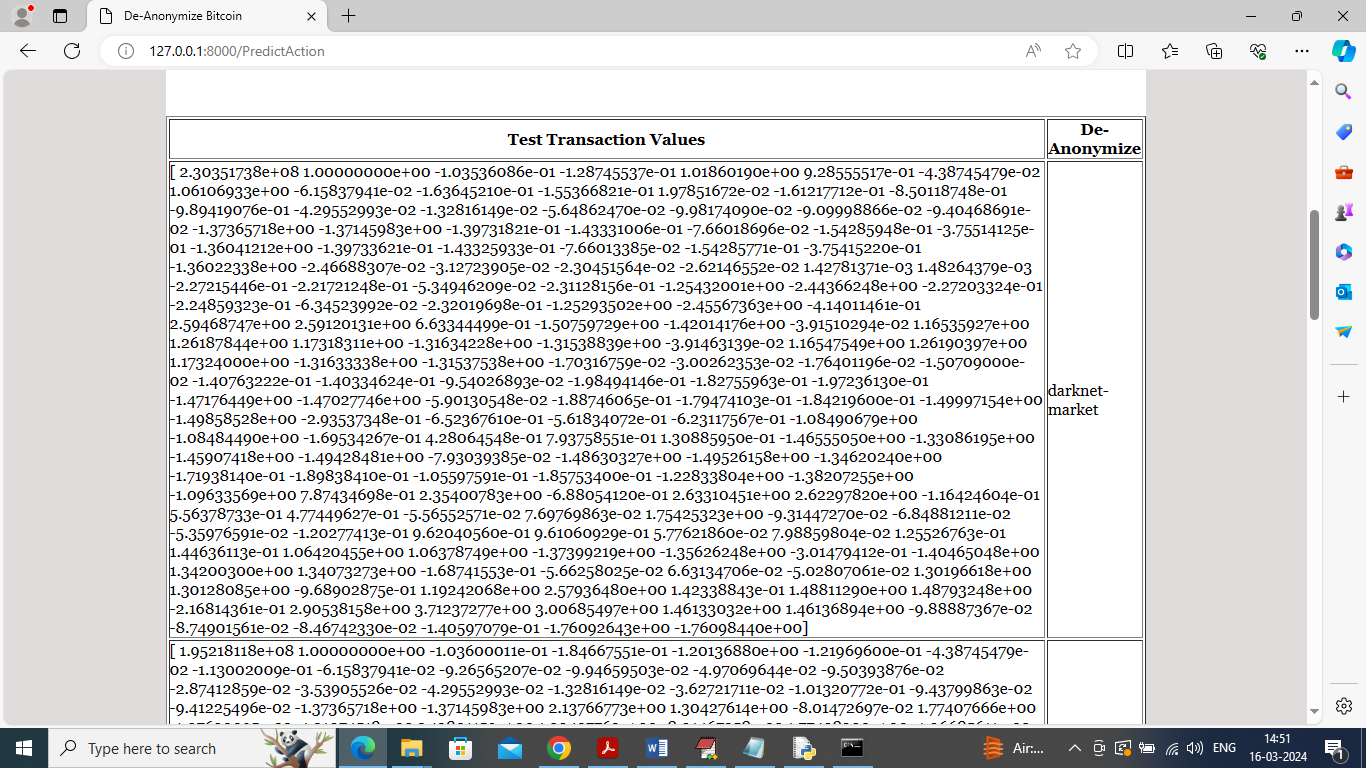
In above screen dataset loading and processing completed and now click on ‘Train ML Algorithm’ link to train all algorithms and get below page



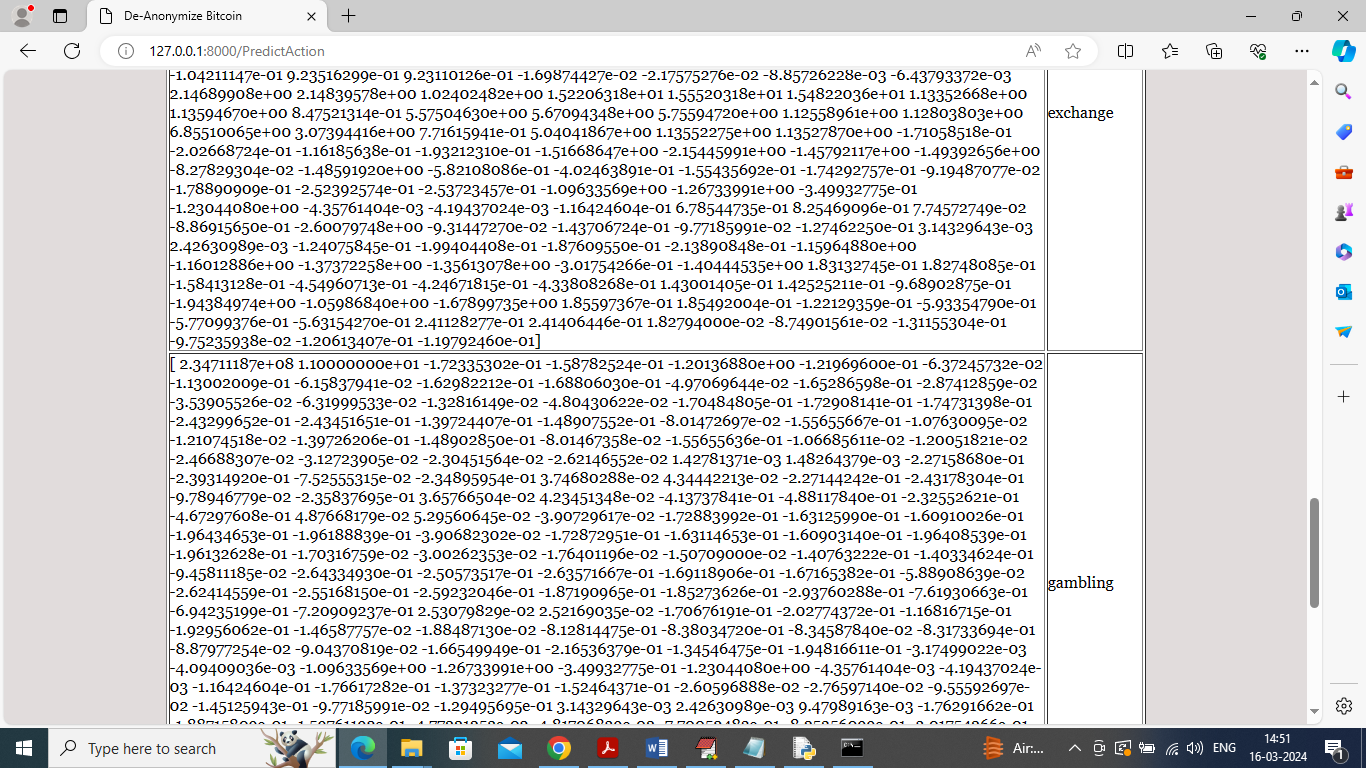
In above screen can see propose CNN and existing algorithms results in table and graph format and in all algorithms propose CNN got high accuracy and now click on ‘De-Anonymize Transaction’ link to get below page



In above screen selecting and uploading ‘test data’ file and then click on ‘Open’ button to get below transaction type predicted page



In above screen in first column can see ‘Transaction Test Data values’ and in second column can see De-Anonymize transaction type as ‘Darknet’



In above screen other transactions predicted as “Exchange and Gambling’.

So by following above screen you can add test data to predict or de-anonymize Blockchain transaction type