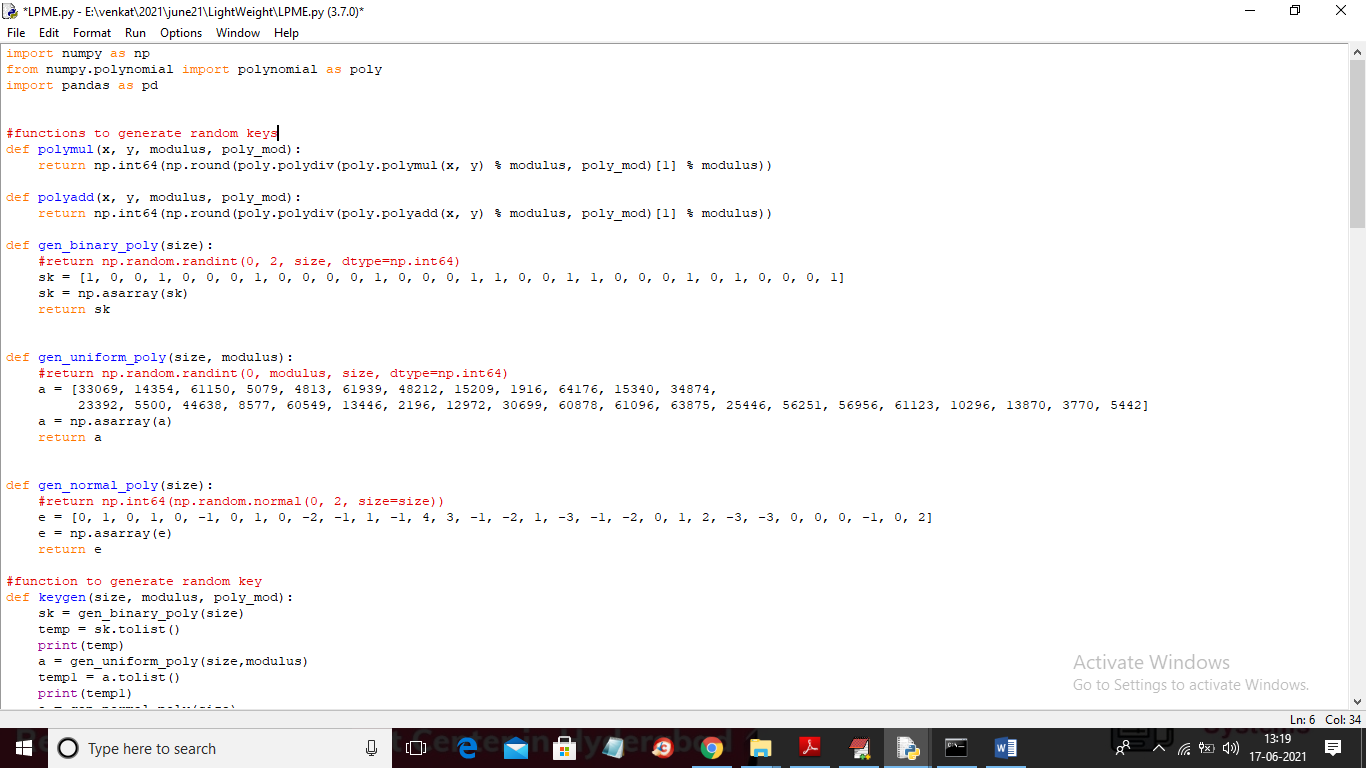
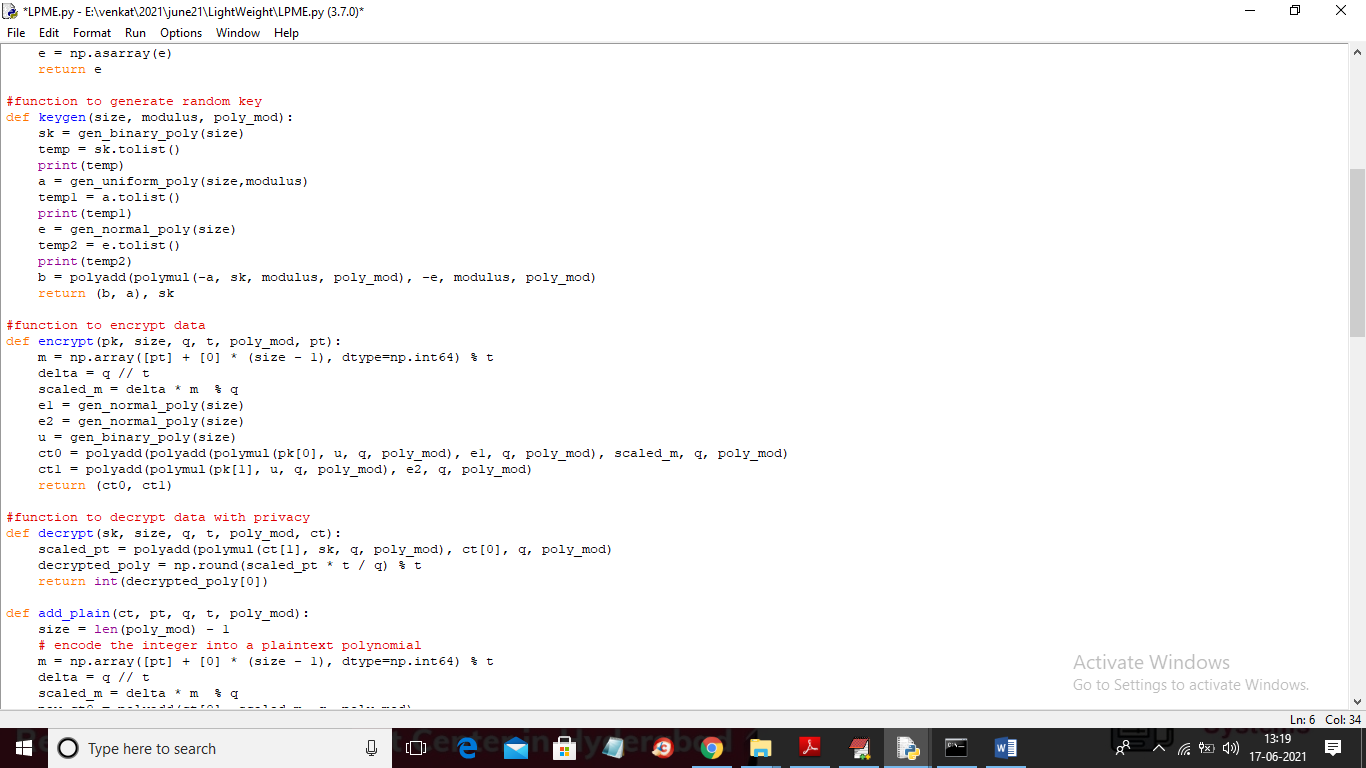
Lightweight Privacy-preserving Medical Diagnosis in Edge Computing

Now-a-days from mobile user can do anything and they can enter their health symptoms to mobile and mobile will send request to hospital cloud and this cloud will apply machine learning algorithm on user data to predict disease and while using such application many drawbacks can be encounter

1. User request has to process faster and if cloud taking too much time for response then this will be severe problem when patient has to diagnose with heart disease. In propose paper this problem is solving by using Edge Node where mobile will choose nearest and free available Edge Node to process request so response time can be minimize. Each cloud can be connected with multiple EDGE NODES and mobile will choose nearest Edge Node to get response.
2. To predict disease using machine learning algorithms we need to train the algorithm with existing dataset and if this dataset exposed then patient privacy will be leak. To overcome from this problem author is encrypted patient data for training using Light Weight Homomorphic algorithm and this algorithm not require any decryption process and we can directly operate on encrypted data without performing decryption. So machine learning XGBOOST algorithm will get trained on Homomorphic encrypted data and this trained model parameters will be shared between multiple EDGE nodes. Edge node will used XGBOOST model to predict or diagnose disease from new patient data.
3. In propose work author providing privacy to patient data by applying Light Weight Privacy Preserving Medical Diagnosis (LPME) and XGBOOST classifier. LPME will encrypt patient train and test data and XGBOOST will predict disease from that encrypted data.

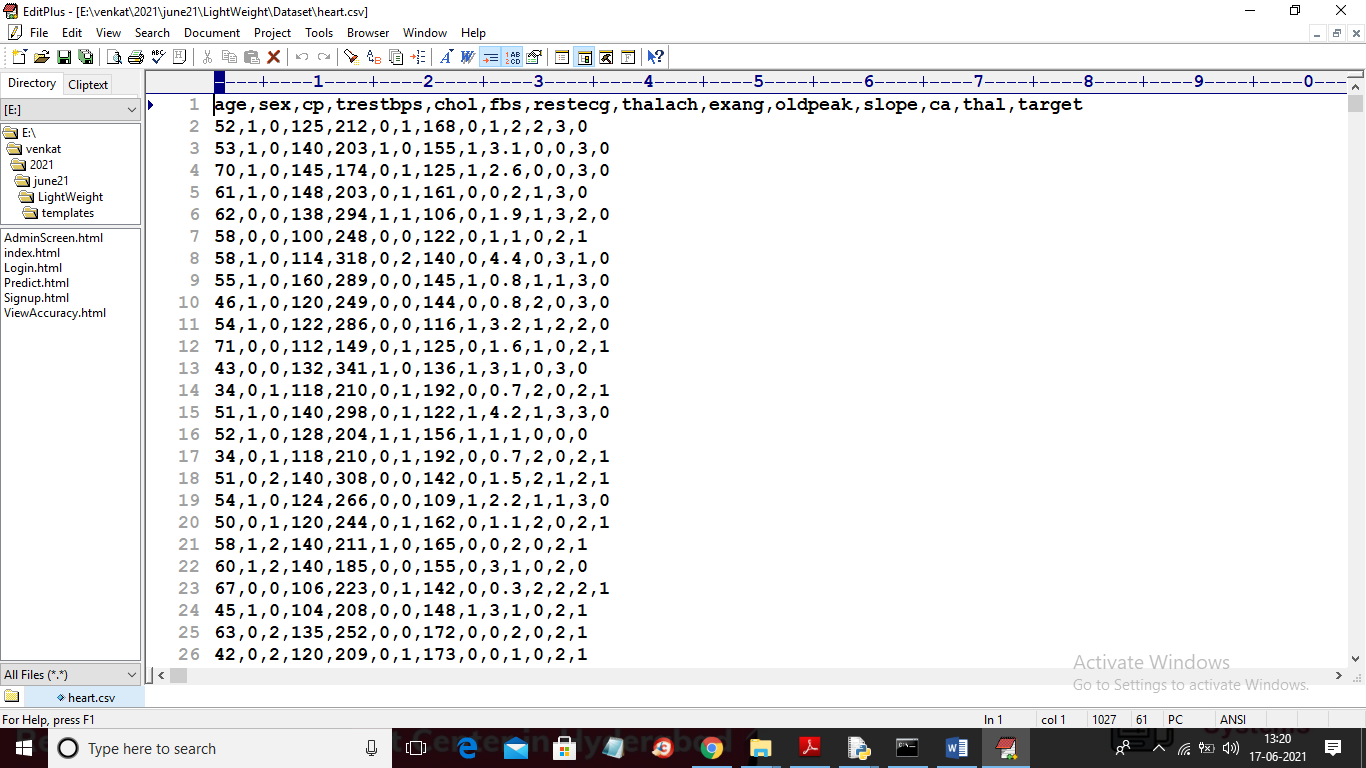
Below code screen showing steps to generate keys, data encryption and decryption process of LPME technique



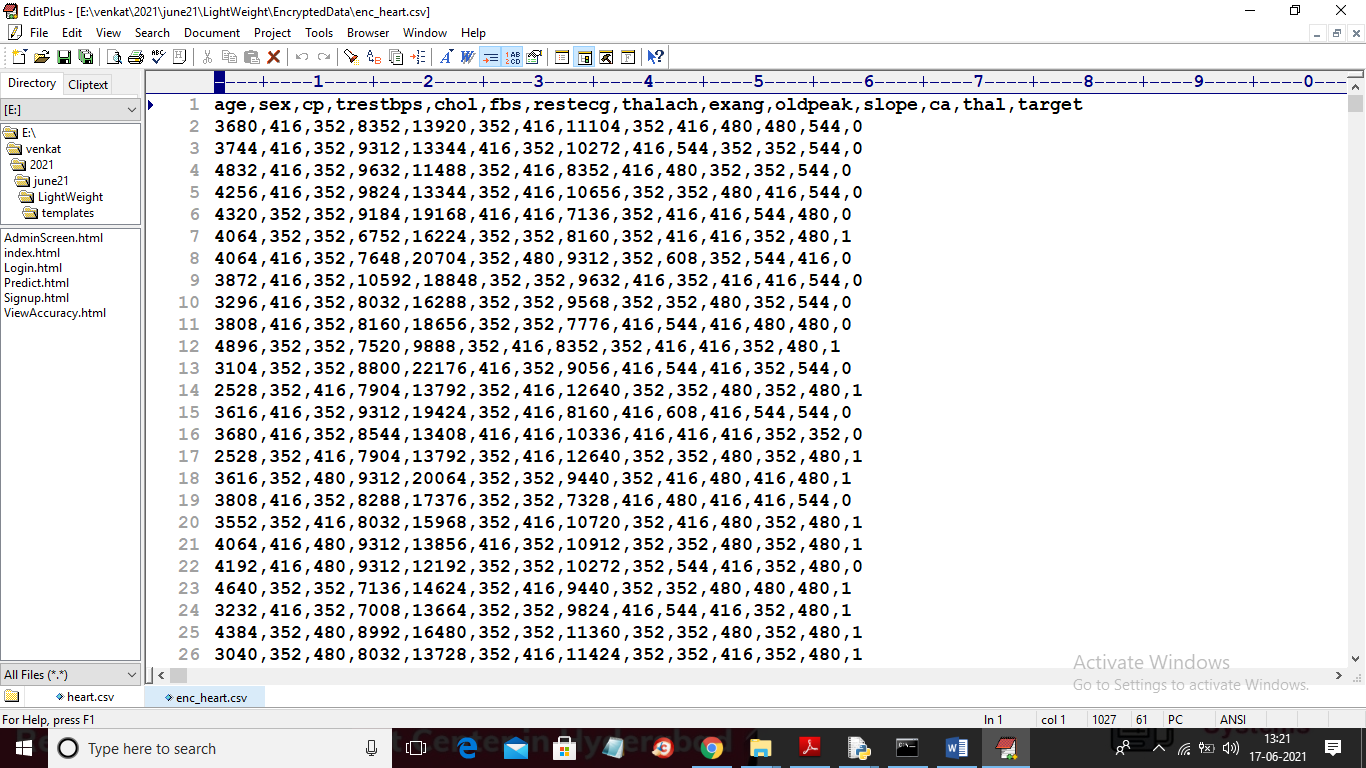


In above two screens read red colour comments to know about LPME encryption using Homomorphic algorithm.

To implement this project we are using Heart Disease Dataset and below screen shot showing some records from dataset

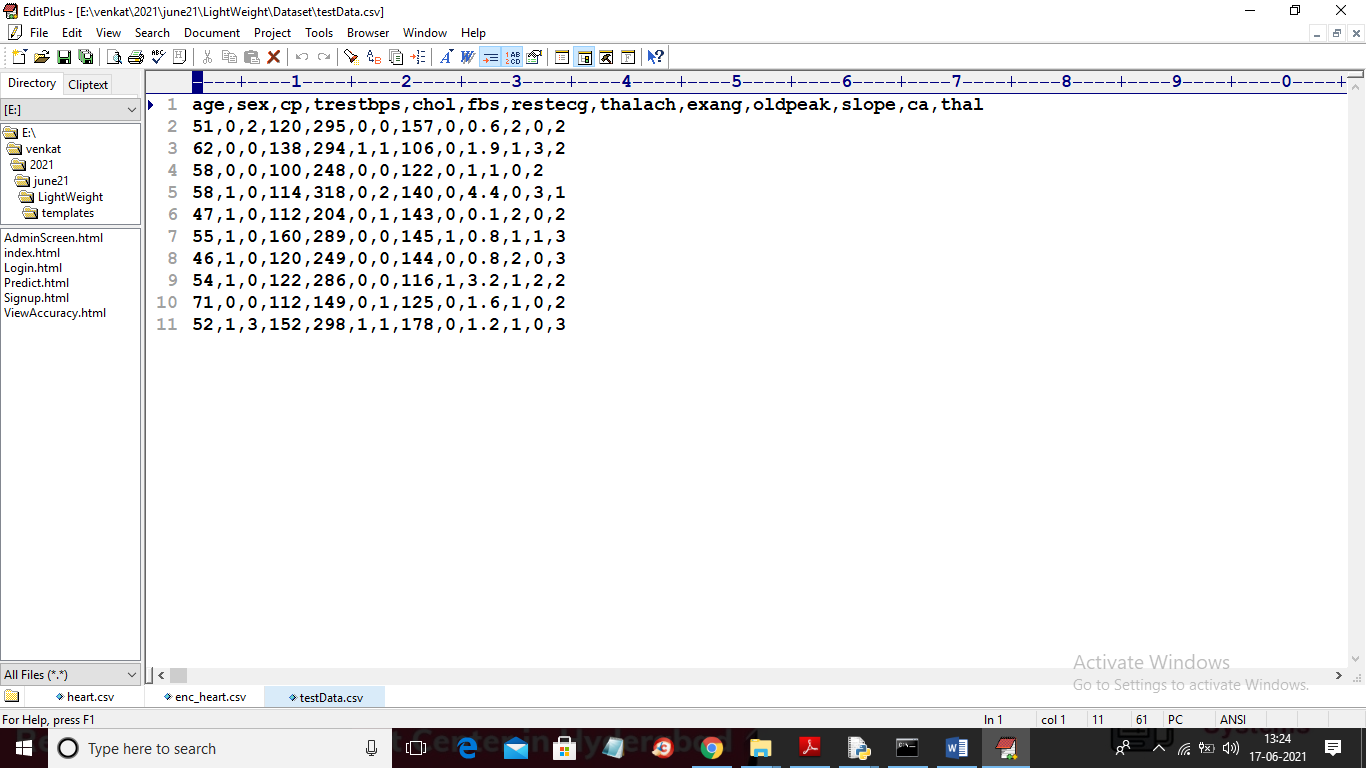


In above screen first row contains dataset column names and remaining rows contains dataset values and after applying LPME encryption then above dataset will be changed to below encrypted values



In above encrypted dataset first column contains AGE value and after applying encryption then age value completely changed and no one will figure out exact age from above encrypted data. In both plain and encrypted dataset in last column we can see class label as 0 or 1 where 0 means that row values are NORMAL and 1 means that row values contains HEART disease.

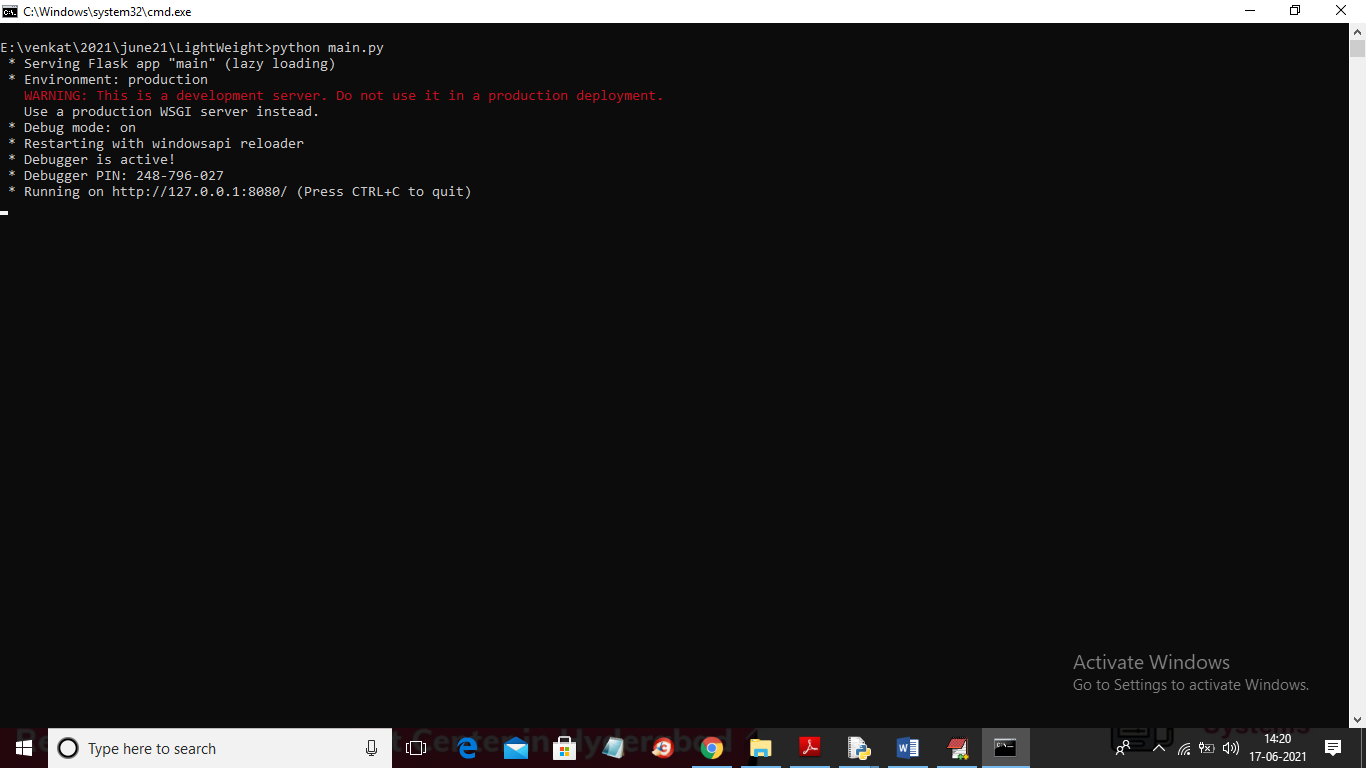
We will use above dataset to train XGBOOST classifier and then we will upload below test data in encrypted format to allow XGBOOST to predict disease



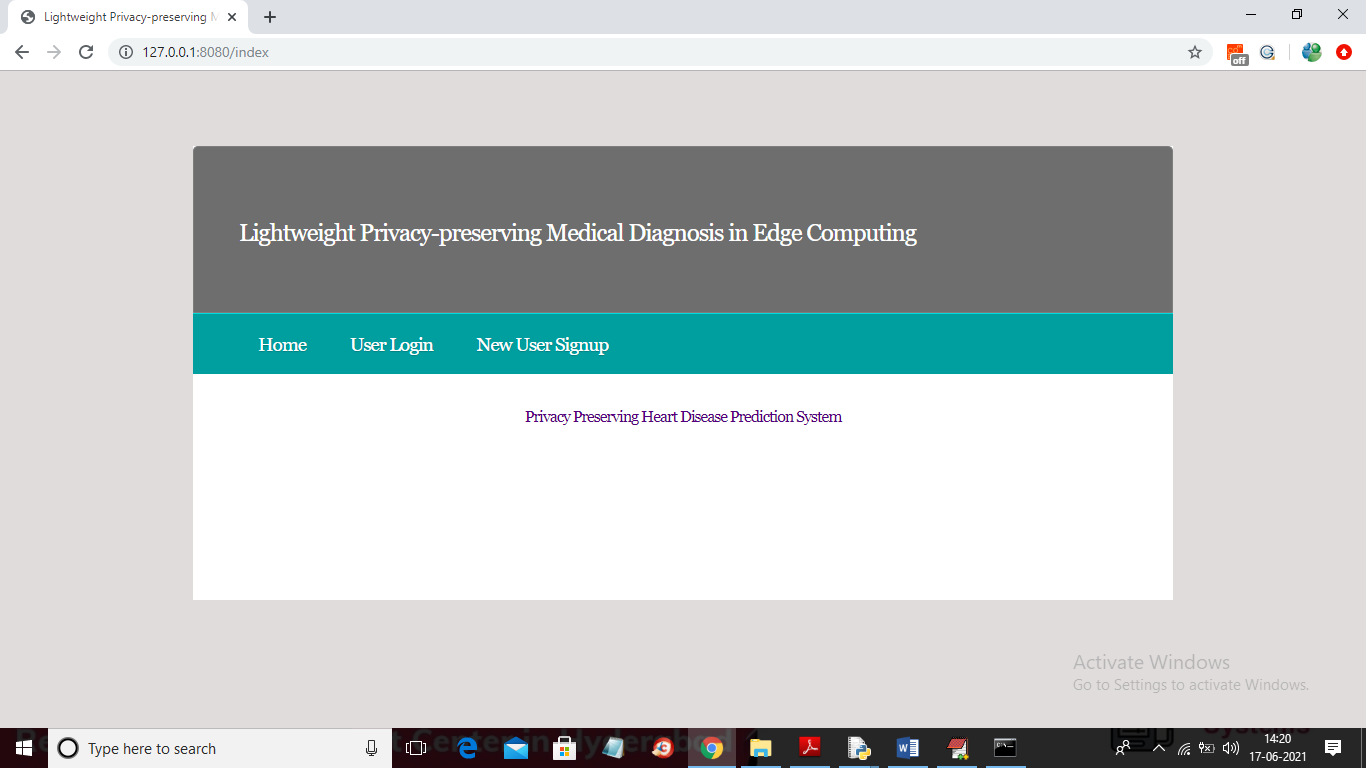
In above test data we can see there is no 0 or 1 values in last column an when we convert above dataset to encrypted format then XGBOOST will predict those 0 and 1 values.

SCREEN SHOTS

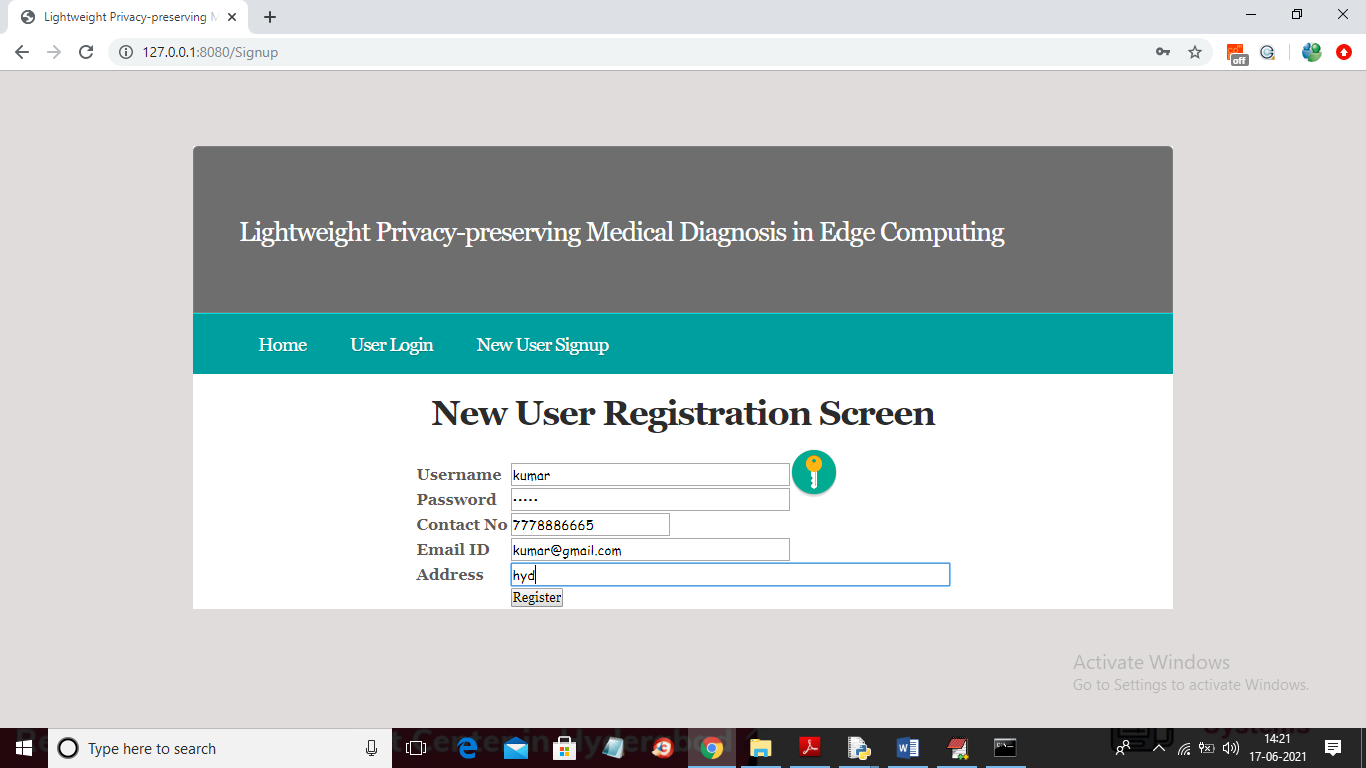
To run project double click on ‘run.bat’ file to start FLASK server like below screen



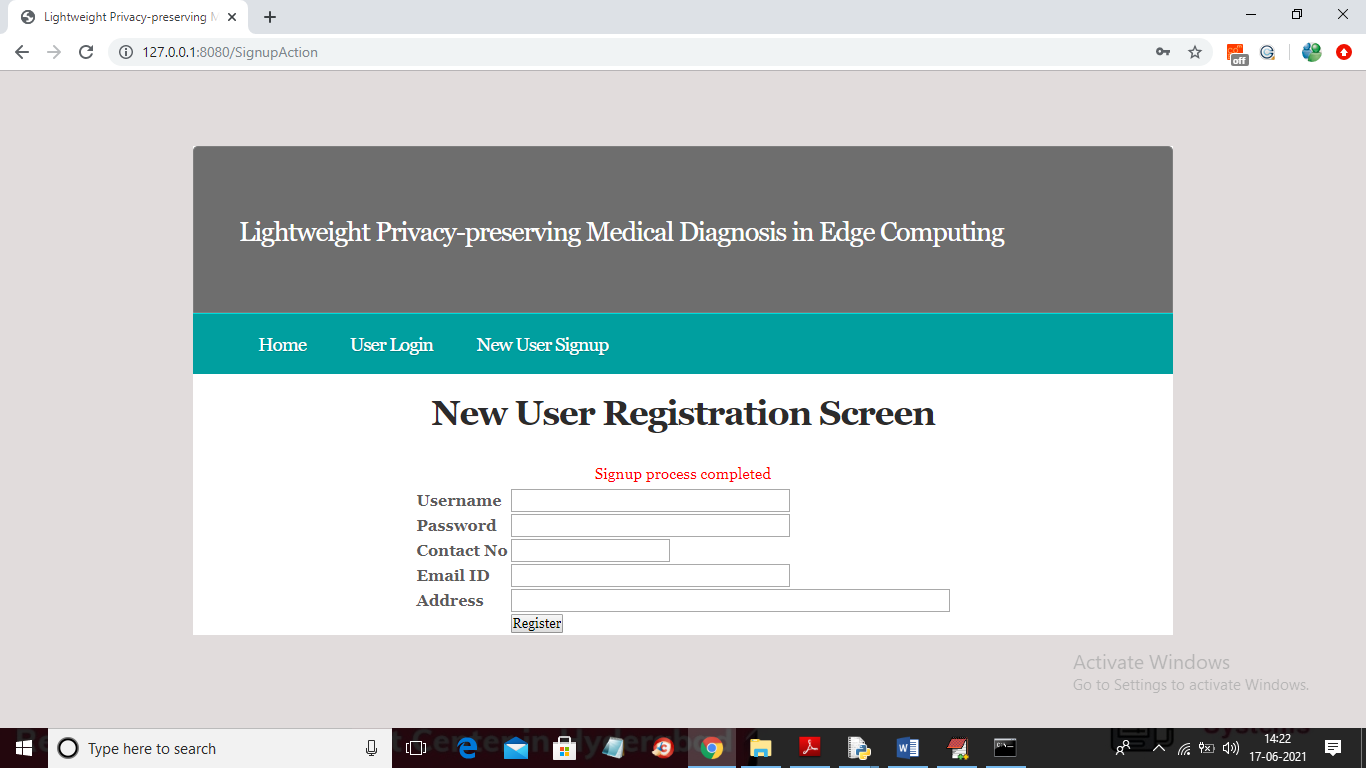
In above screen FLASK server started and now open browser and enter URL as ‘http://127.0.0.1:8080/index’ and press enter key to get below screen



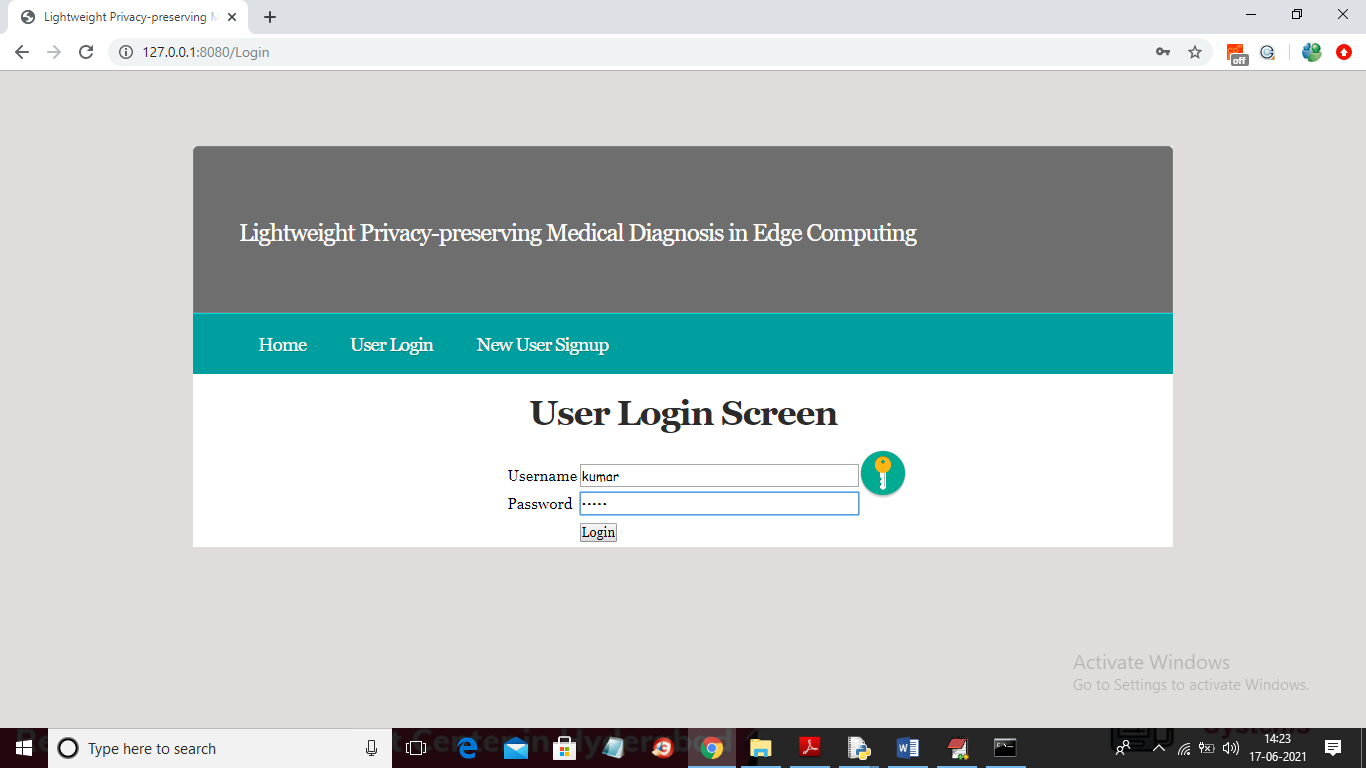
In above screen click on ‘New User Signup’ link to get below signup screen



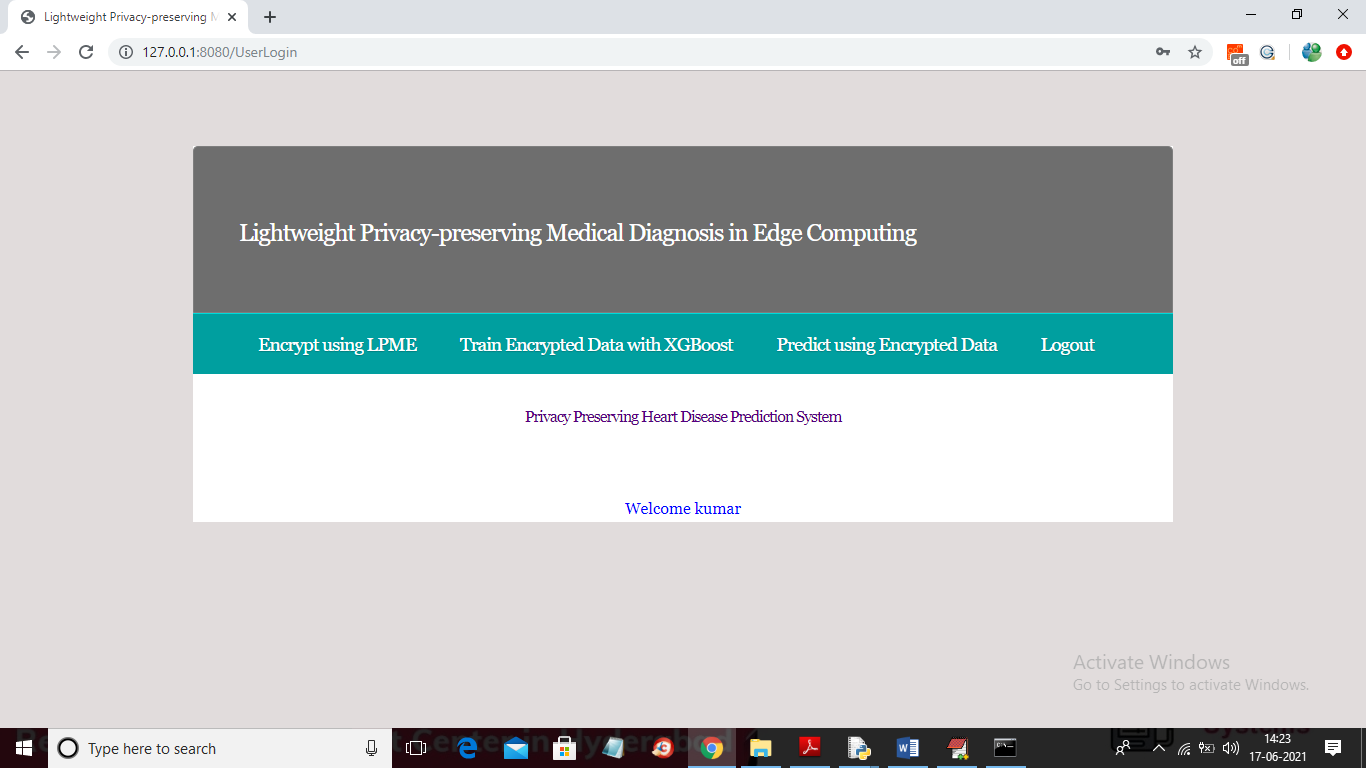
In above screen registering one user and then click on ‘Register’ button to get below screen



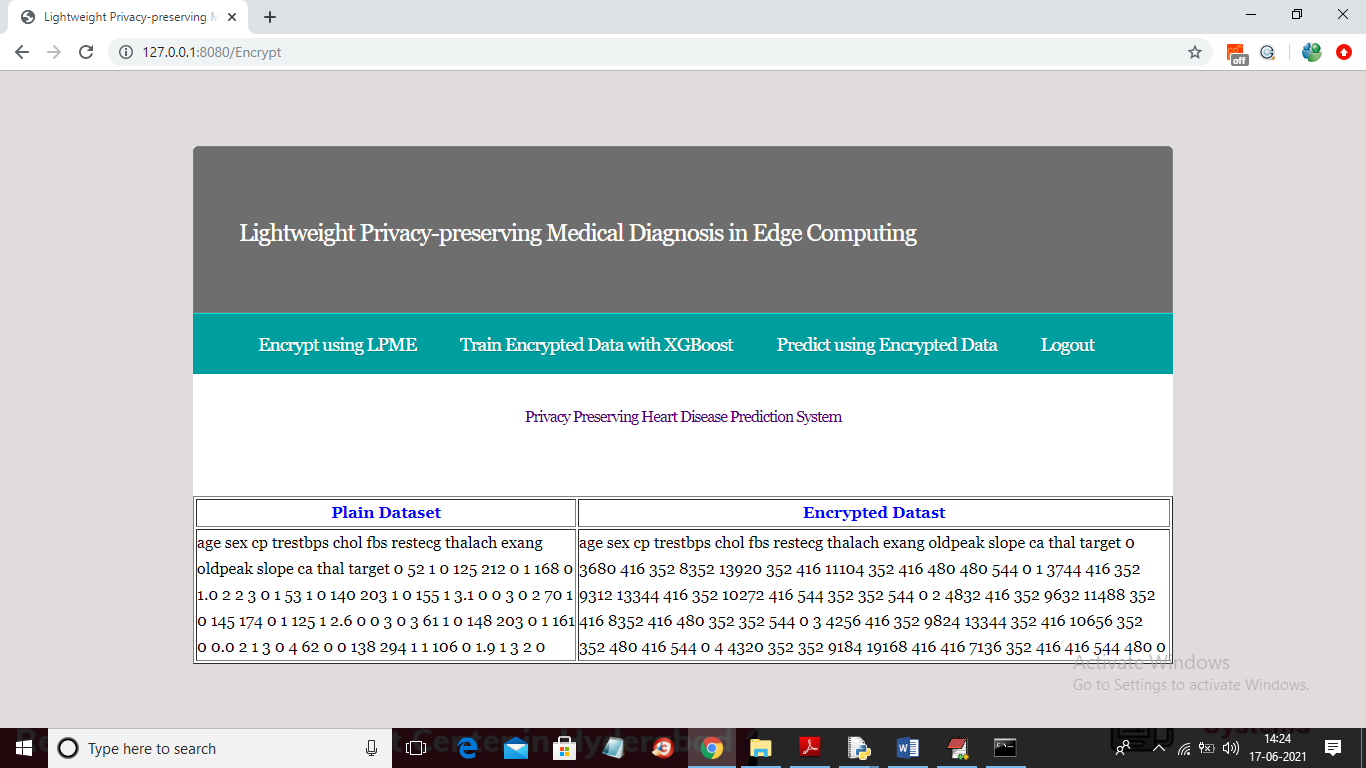
In above screen user signup process completed and now click on ‘User Login’ link to get below screen



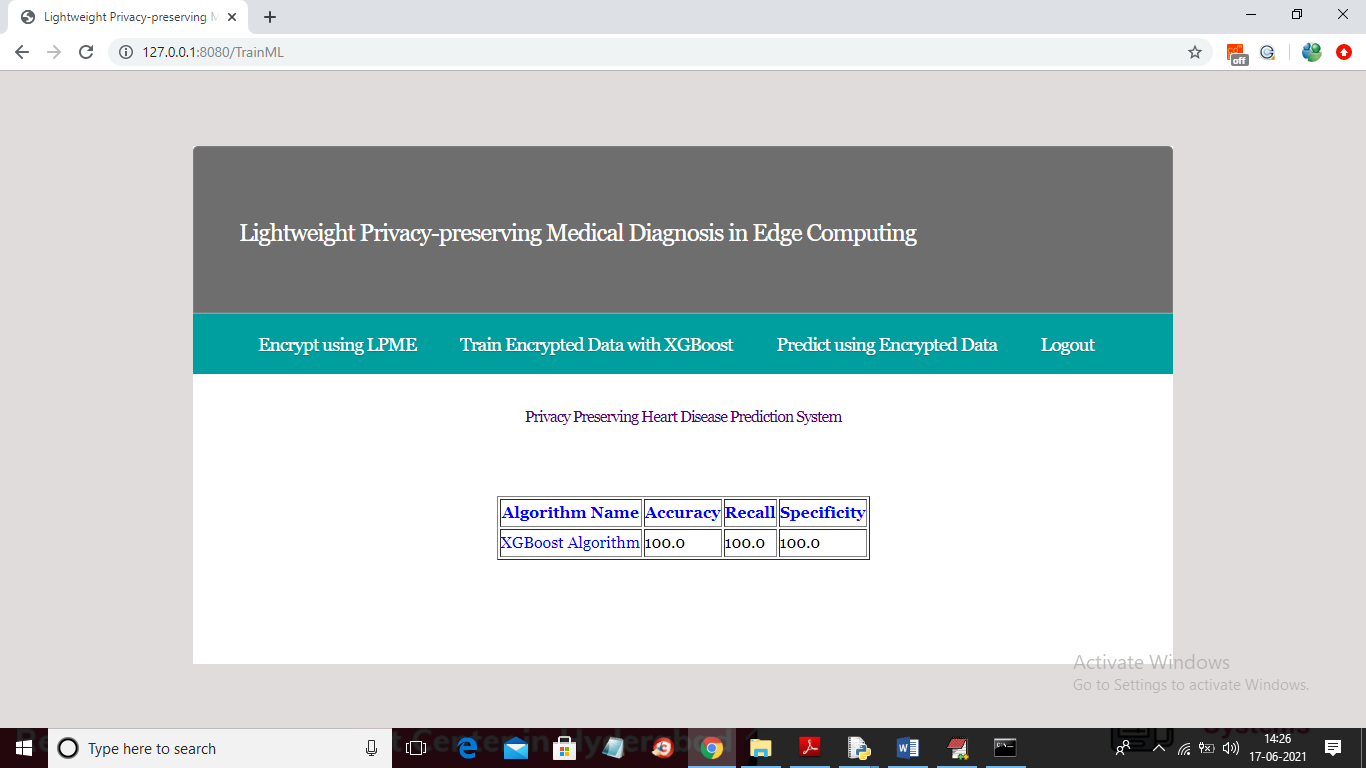
In above screen user is login and after login will get below screen



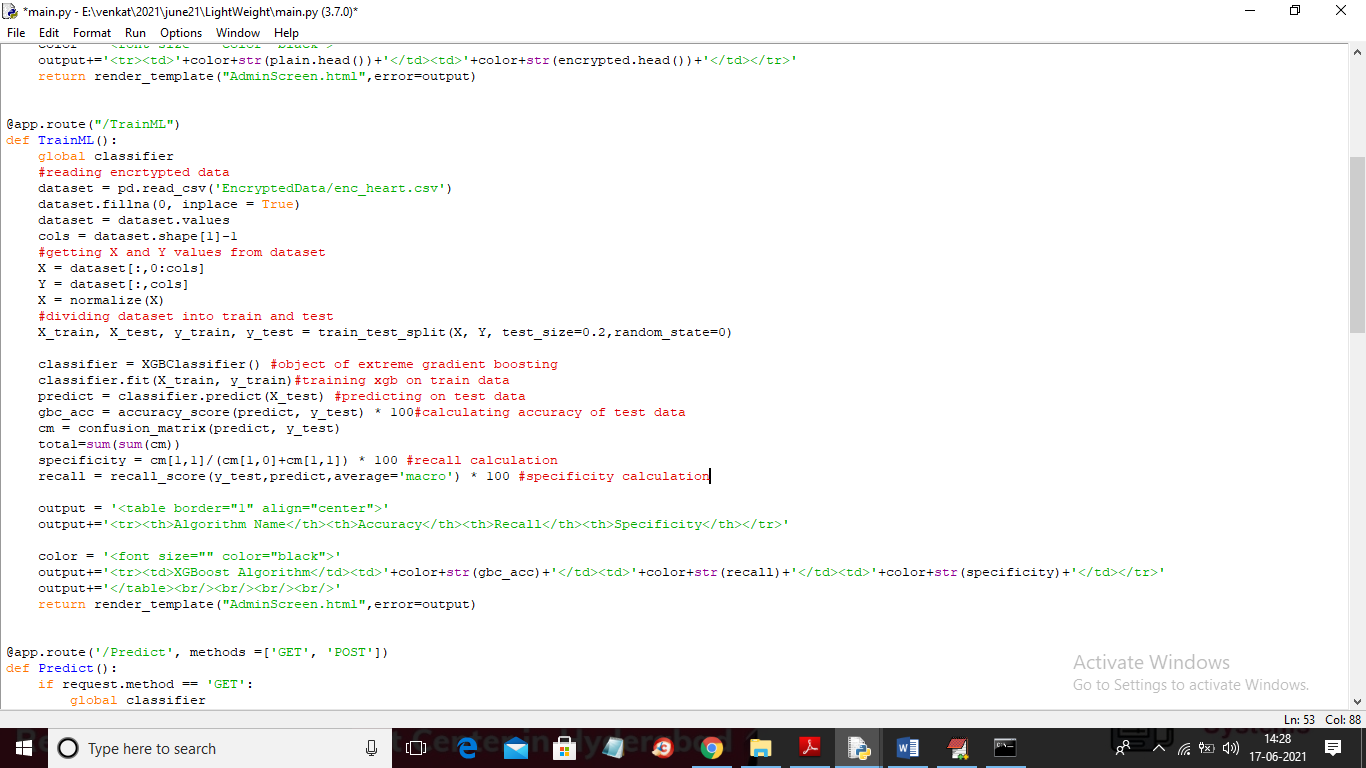
In above screen you can click on ‘Encrypt using LPME’ link to encrypt dataset with LPME technique



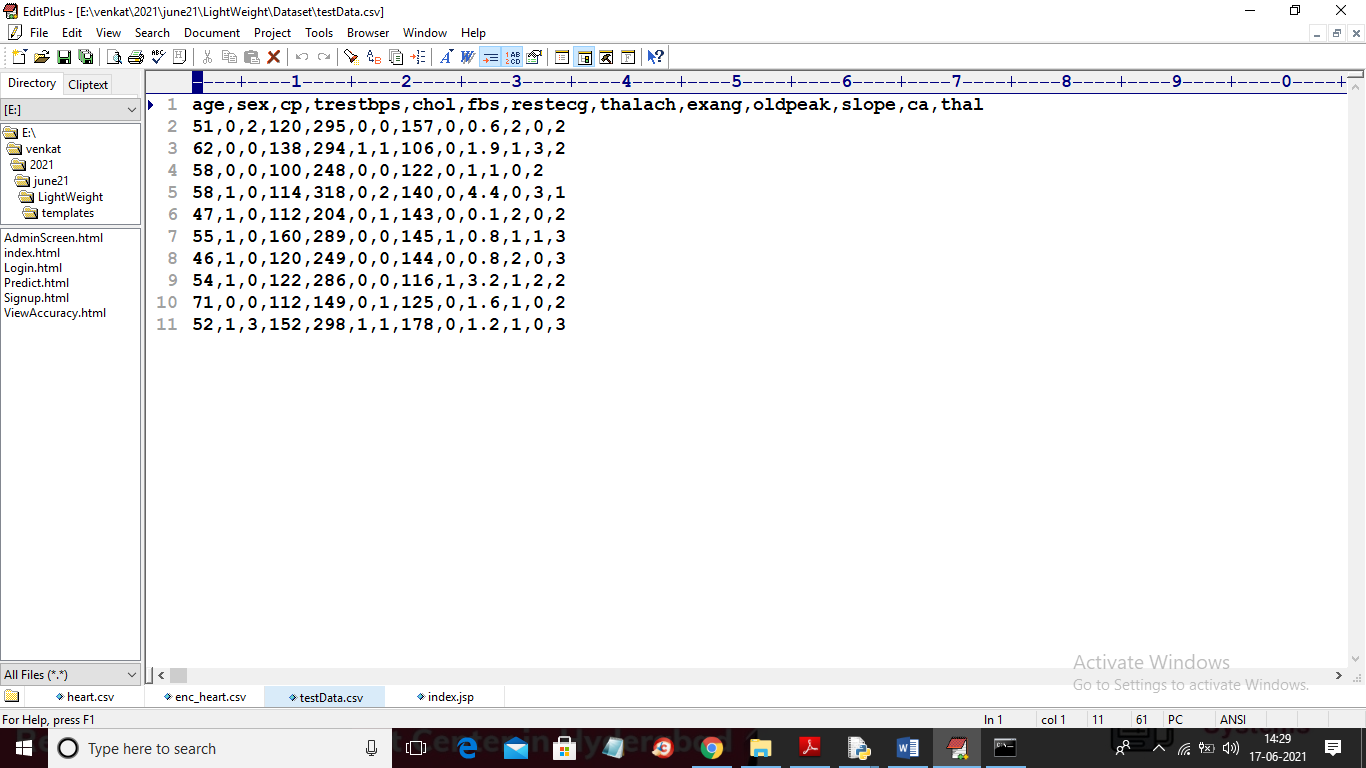
In above screen first column showing original dataset and second column showing encrypted format of that original plain data and now dataset is encrypted and now click on ‘Train Encrypted Data with XGBoost’ link to train dataset and to build XGBOOST secure disease prediction model



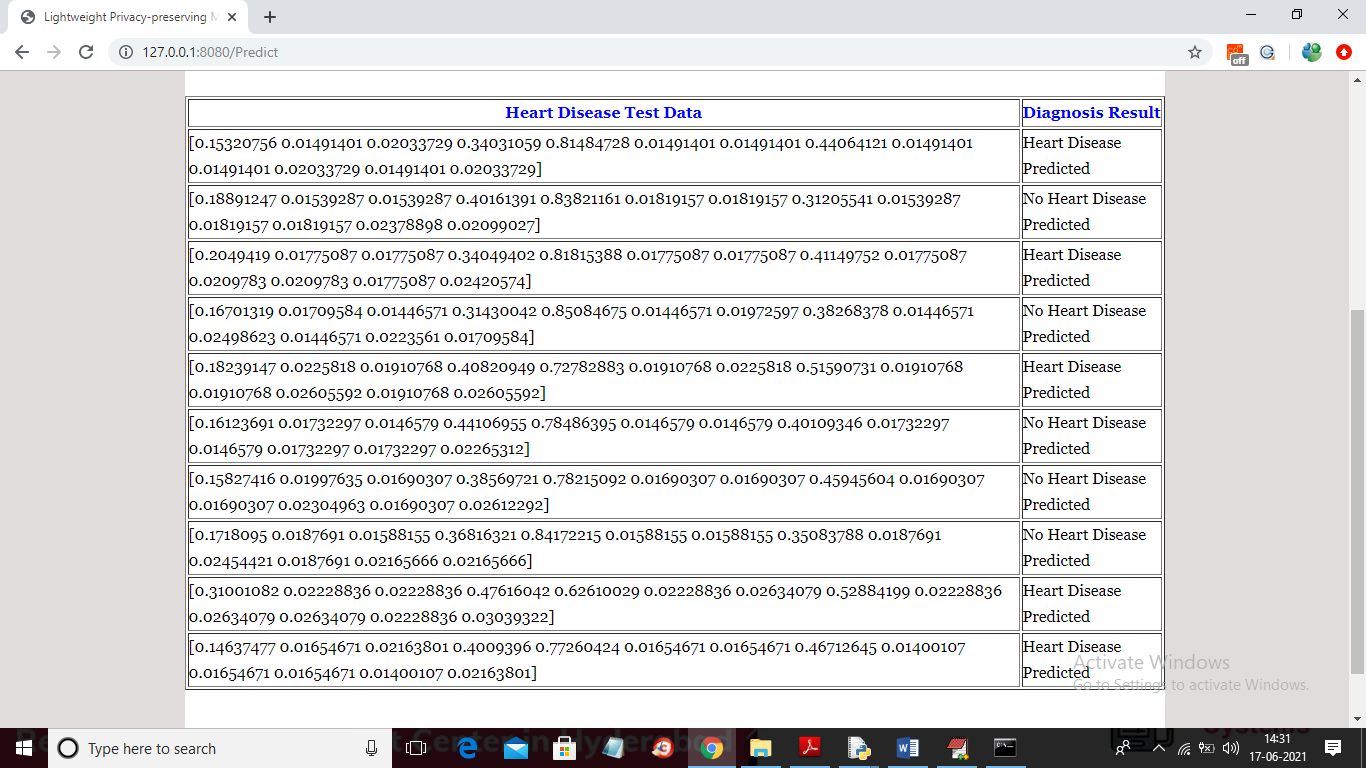
In above screen XGBOOST training completed and we got accuracy of the model on test data is 100% and in below screen u can training and testing of XGBOOST



In above screen read red colour comments to know about XGBOOST training on encrypted data and now go back to previous application and click on ‘Predict Using Encrypted Data’ link to predict disease from new test data and below is the test data screen



Above is the test data which XGBOOST will encrypt and perform prediction of disease and if you want u can add new records to above test data and this testData.csv file is available inside ‘Dataset’ folder



In above screen in first column you can see then encrypted test data and in second column you can see prediction result as ‘No Heart Disease Detected’ or ‘Heart Disease Detected’