Security using Elliptic Curve Cryptography (ECC) in Cloud

Now-a-days all organizations such as Facebook, Whatsapp, Healthcare, banking and many more applications are using cloud services to store and manage their business data as this cloud services provides heavy computation resources and storage spaces with cheaper cost but this advantage leads to data security issues as user’s data stored at third party cloud server which is completely away from user’s hand and cloud server’s internal employees or hackers may misuse this data and to protect data from such issues, data encryption algorithms such as AES, RSA, DES, Triple DES and many more was introduced which will encrypt data before outsource to cloud. Internal employees or hackers may access data but they can’t able to read or understand it.

All existing algorithms require large size of keys generation and management which took heavy computation time and resources which may increase cloud usage cost and to overcome from this problem ECC (elliptic curve cryptography) algorithm is introduce which is lighter to generate keys and take less computation time and resources to encrypt or decrypt data.

So in propose paper we are using ECC algorithm to encrypt data before outsource to cloud and then comparing its encryption time performance with AES algorithm and the experiment with AES and ECC proves that ECC is lighter and faster than AES.

To implement this project we have designed two different applications

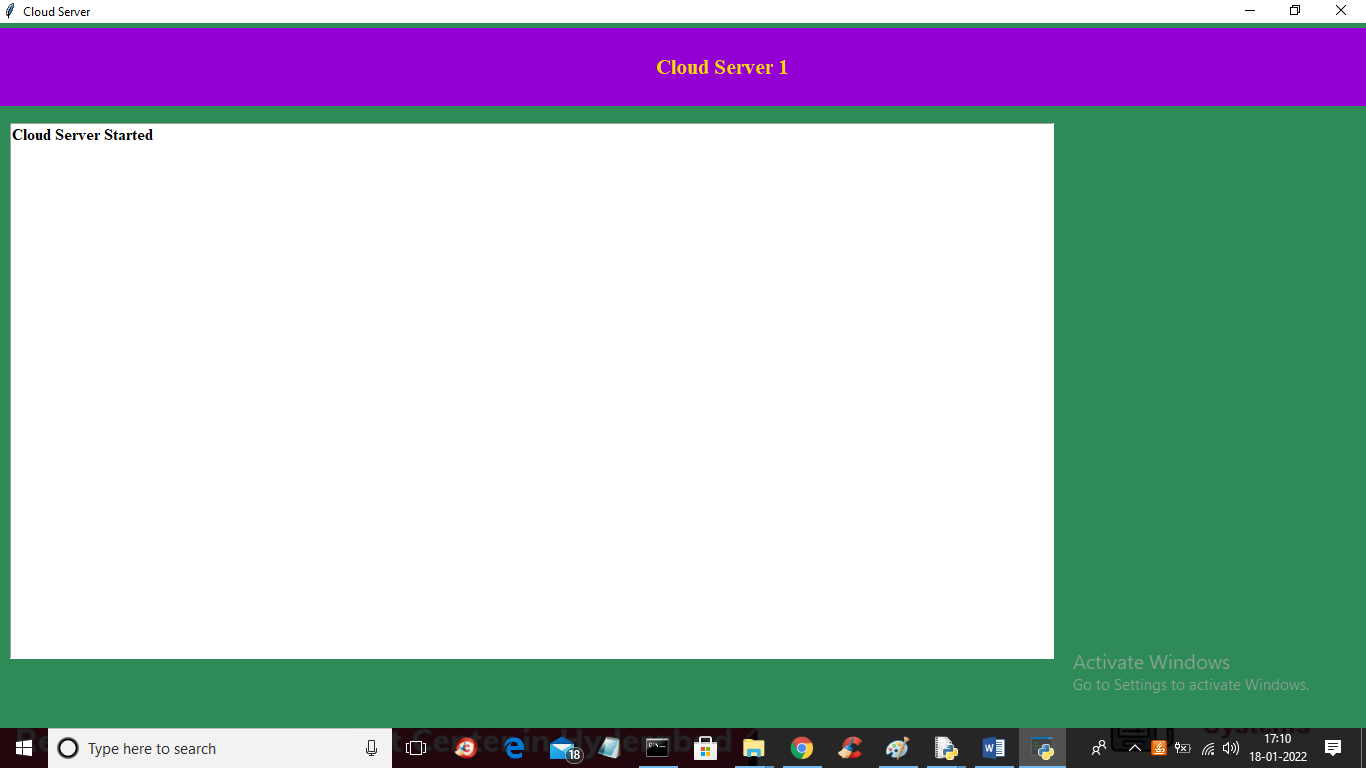
1. Cloud Server: This is a python based cloud server which accept input file from user and then save in its storage space. Any time user can send request to download particular file and cloud will respond to user with that file. All files send to this cloud will be encrypted using ECC.
2. Cloud User: cloud user will upload file and then encrypt using ECC and then send or outsource to cloud for storage. Any time user can send request to cloud for file download and then decrypt it.

To implement this project we have designed following modules

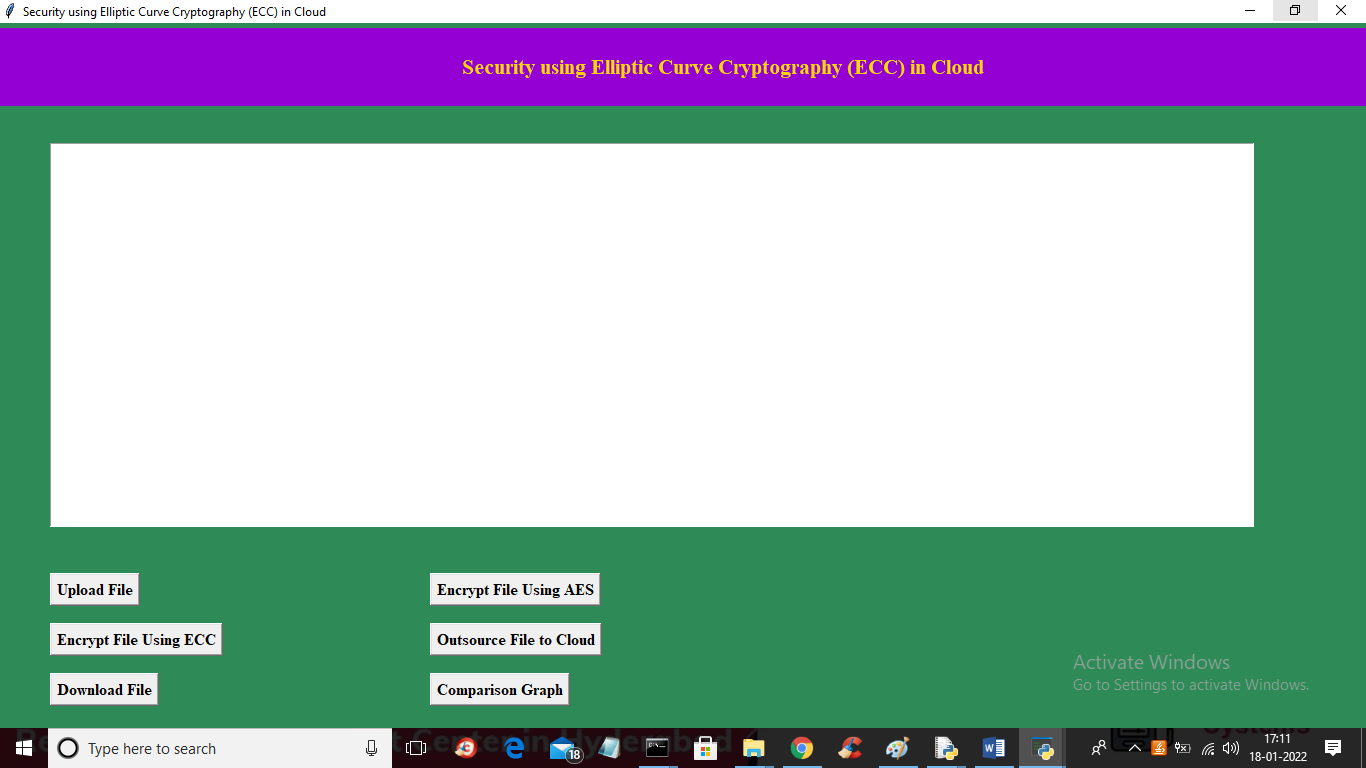
1. Upload File: using this module we will upload any file to application
2. Encrypt File Using AES: using this module we will read file data and then encrypt it using AES algorithm and then compute encryption time
3. Encrypt File Using ECC: using this module we will encrypt file using ECC algorithm and then calculate encryption time
4. Outsource File to Cloud: using this module we will outsource file to cloud server for storage
5. Download File: using this module we will send file request to cloud and then download and decrypt the file
6. Comparison Graph: using this module we will plot encryption time graph between AES and ECC algorithm

SCREEN SHOT

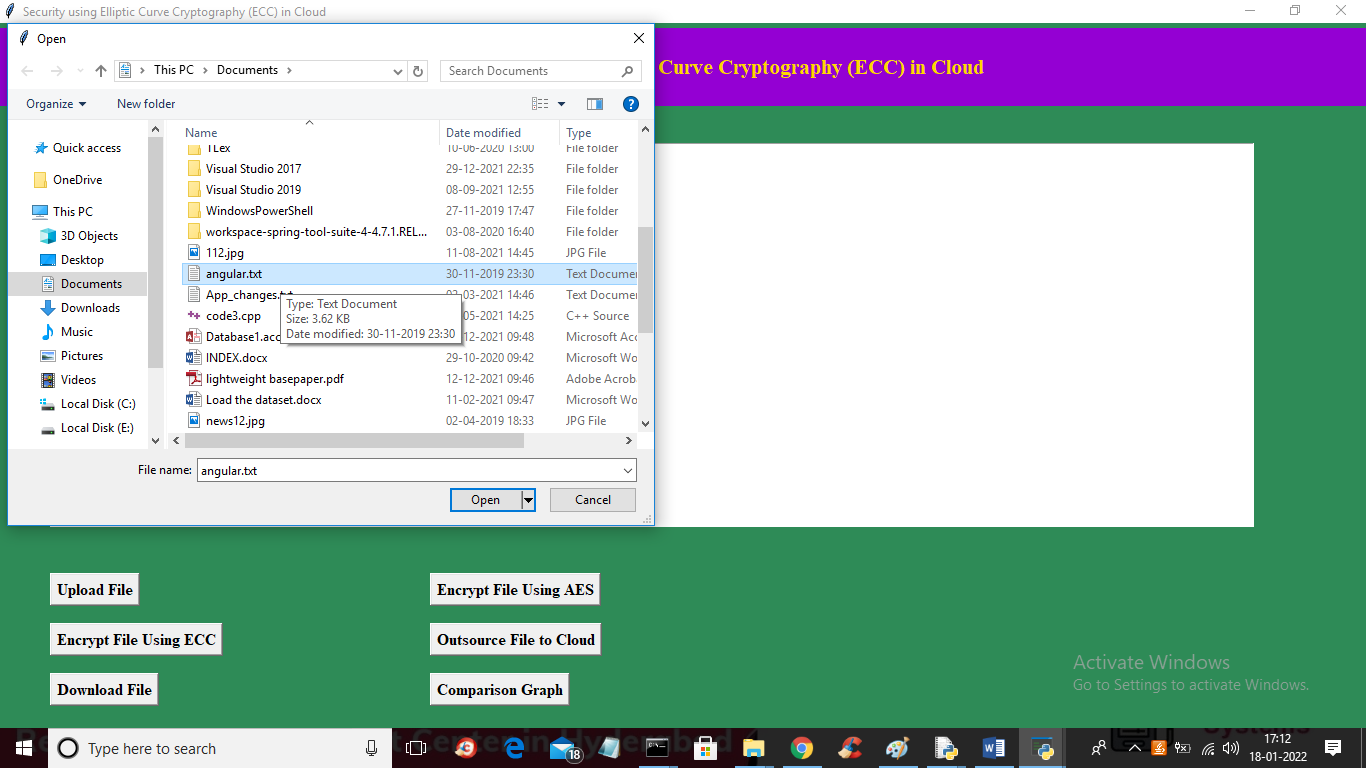
To run project first double click on ‘run.bat’ file from ‘CloudServer’ folder to start cloud application and to get below screen



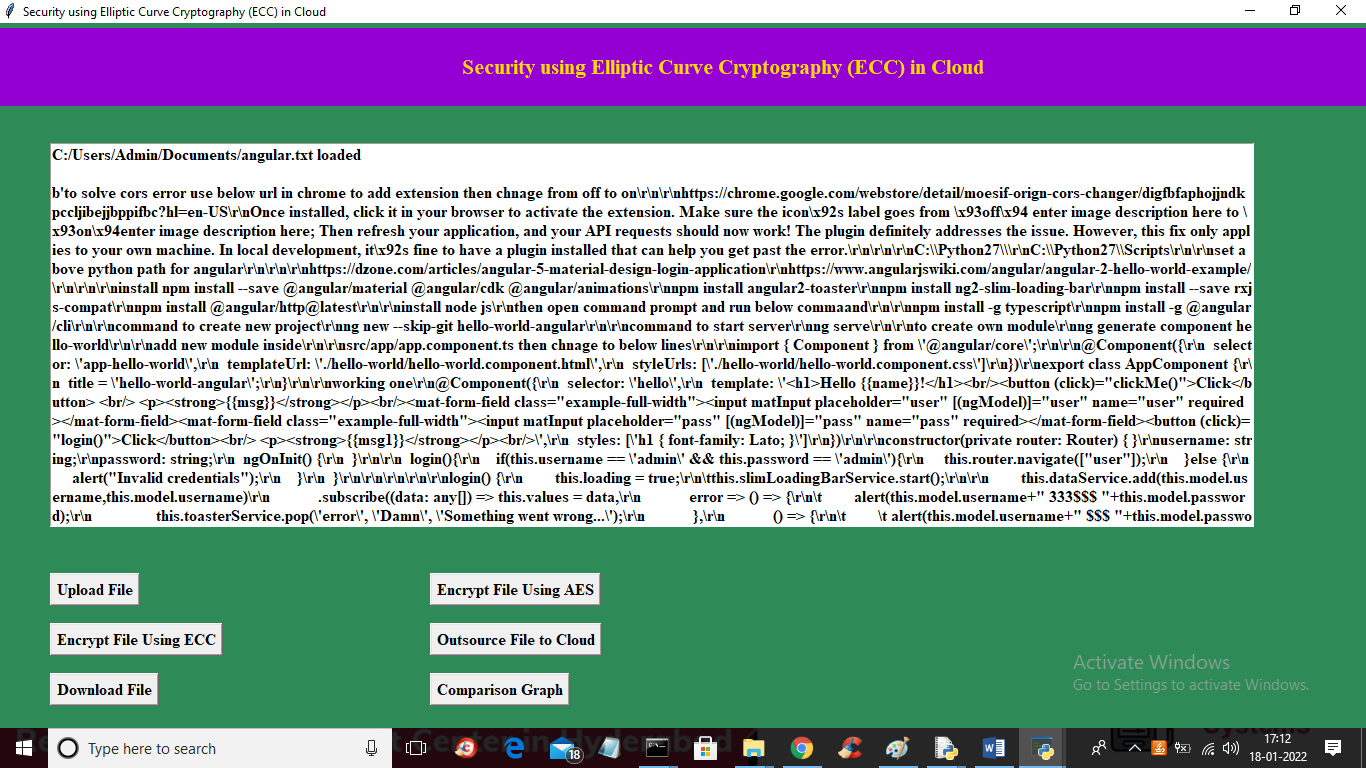
In above screen cloud server started and now double click on ‘run.bat’ file from ‘CloudUser’ folder to start cloud user application and to get below screen



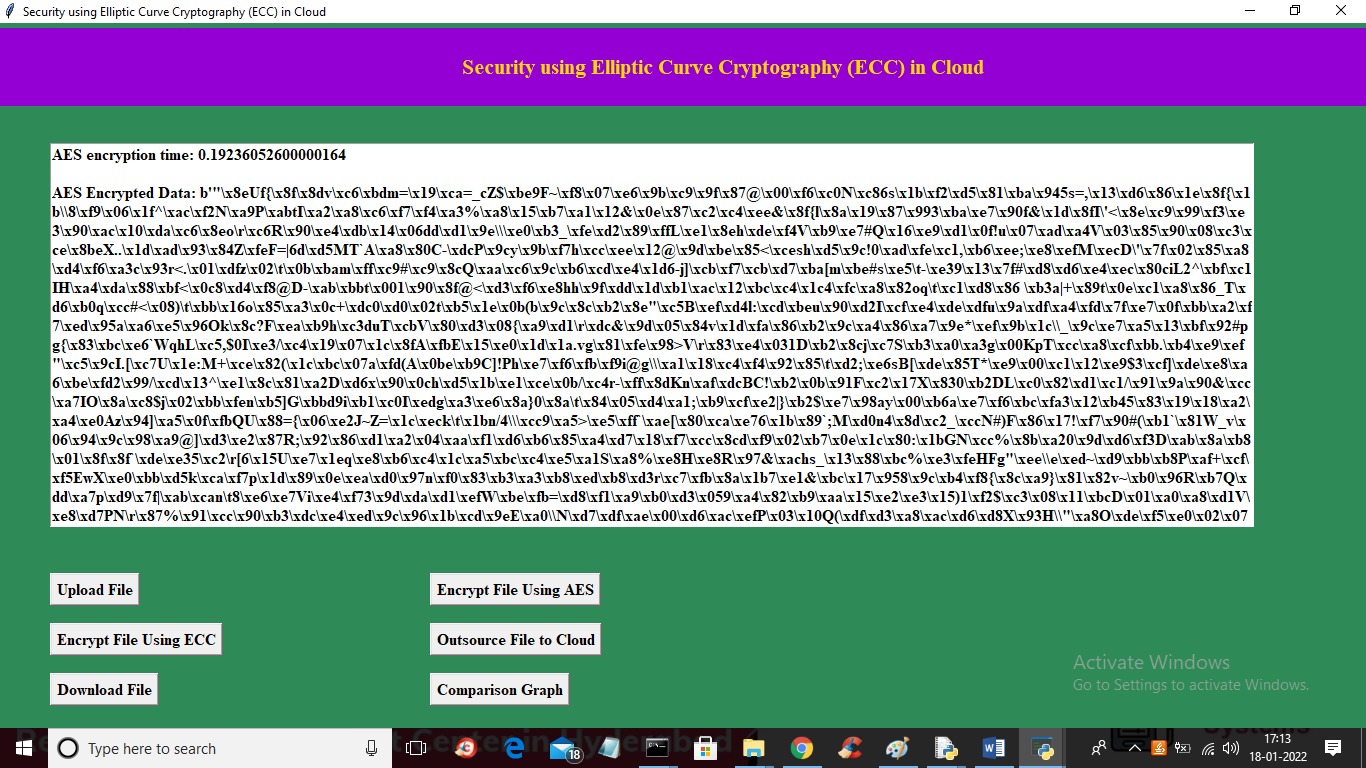
In above screen click on ‘Upload File’ button to upload any file to application like below screen



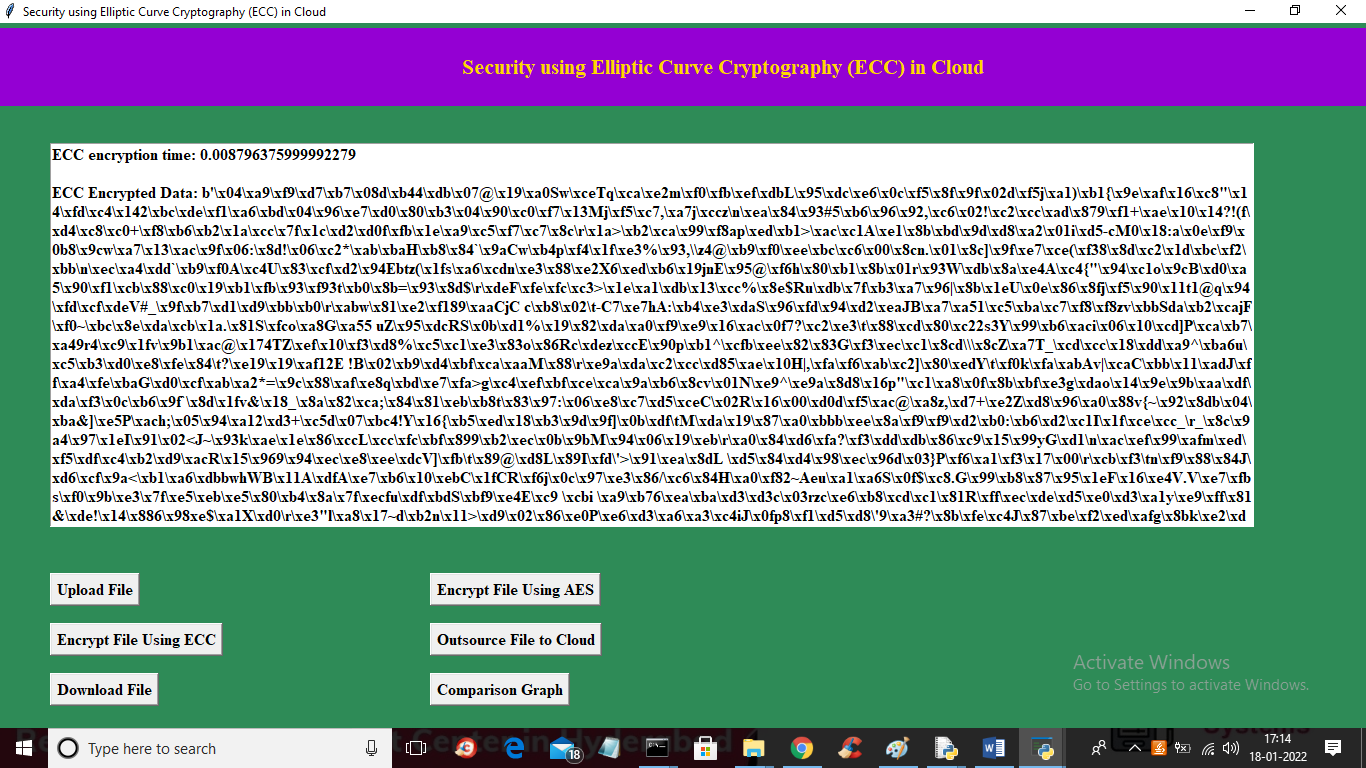
In above screen selecting and uploading ‘angular.txt’ file and then click on ‘Open’ button to load file and to get below screen



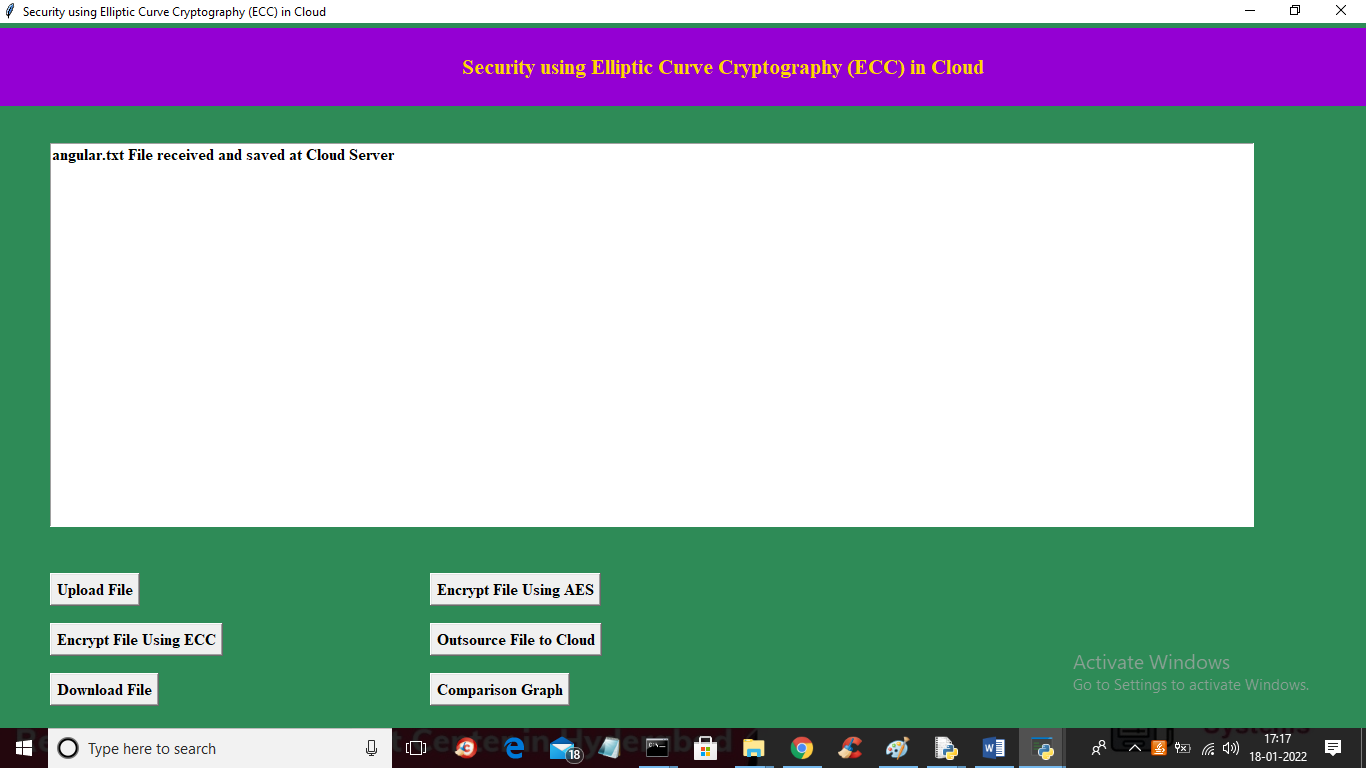
In above screen file is loaded and now click on ‘Encrypt File Using AES’ algorithm button to encrypt file and to get below screen



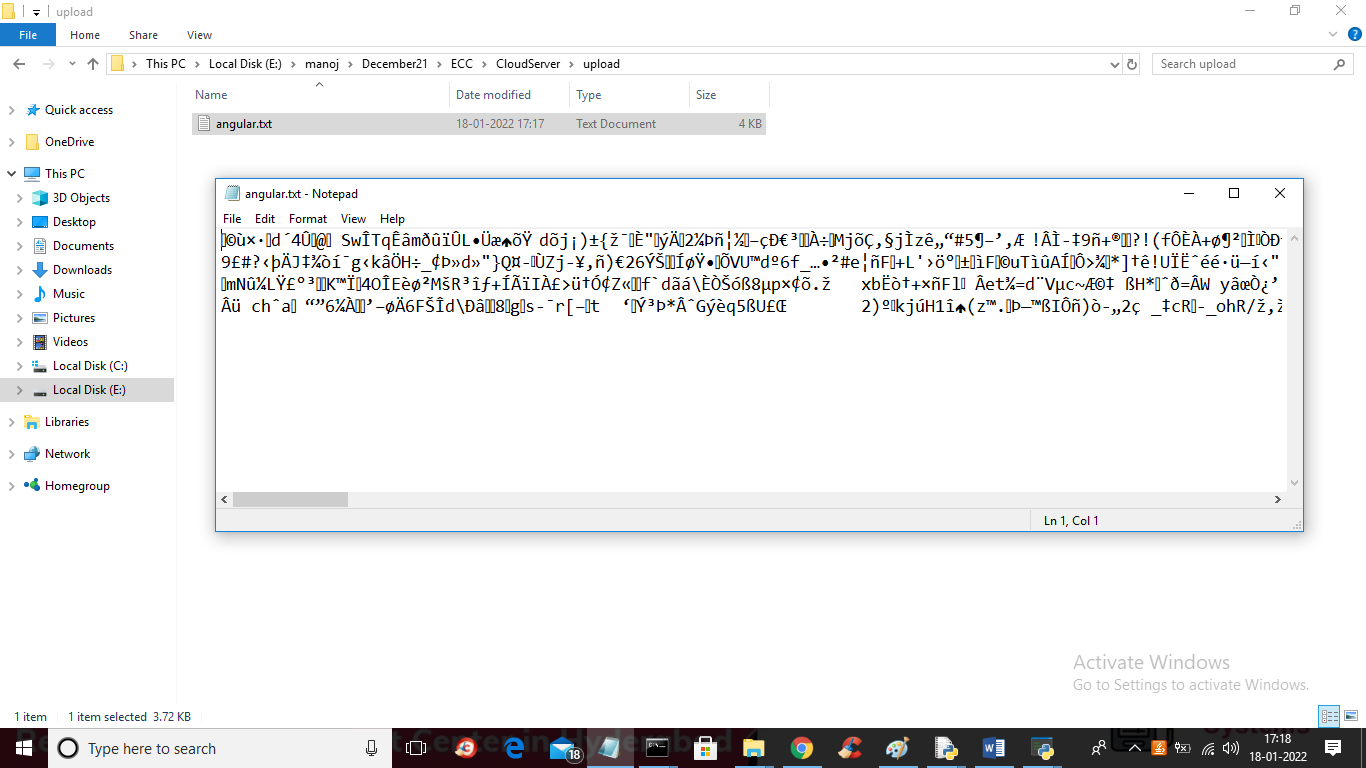
In above screen we can see plain data is encrypted and in first line AES encryption time is 0.192 milli seconds. Now click on ‘Encrypt File using ECC” button to encrypt same file using ECC and calculate time



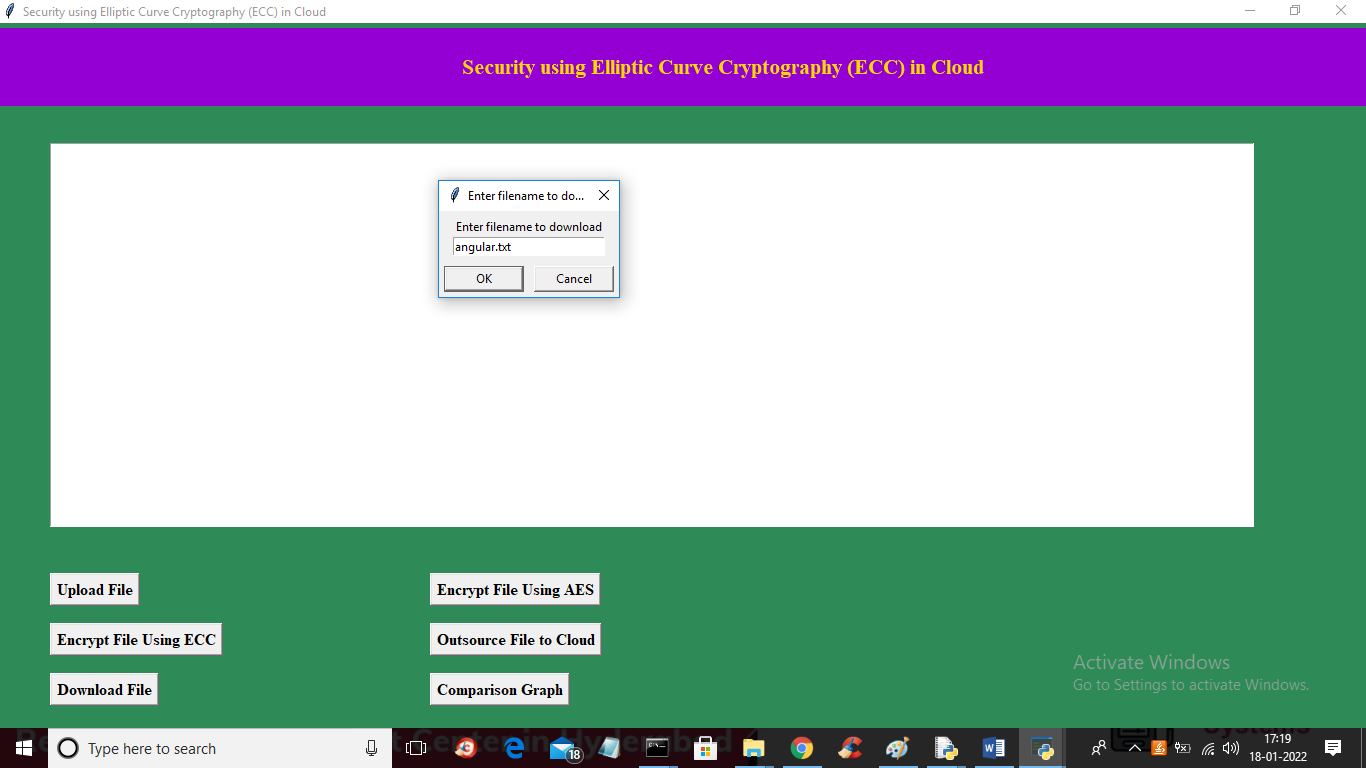
In above screen same file data encrypted using ECC and its took only 0.008 milli second to encrypt same data. Now click on ‘Outsource File to Cloud’ button to send file to cloud



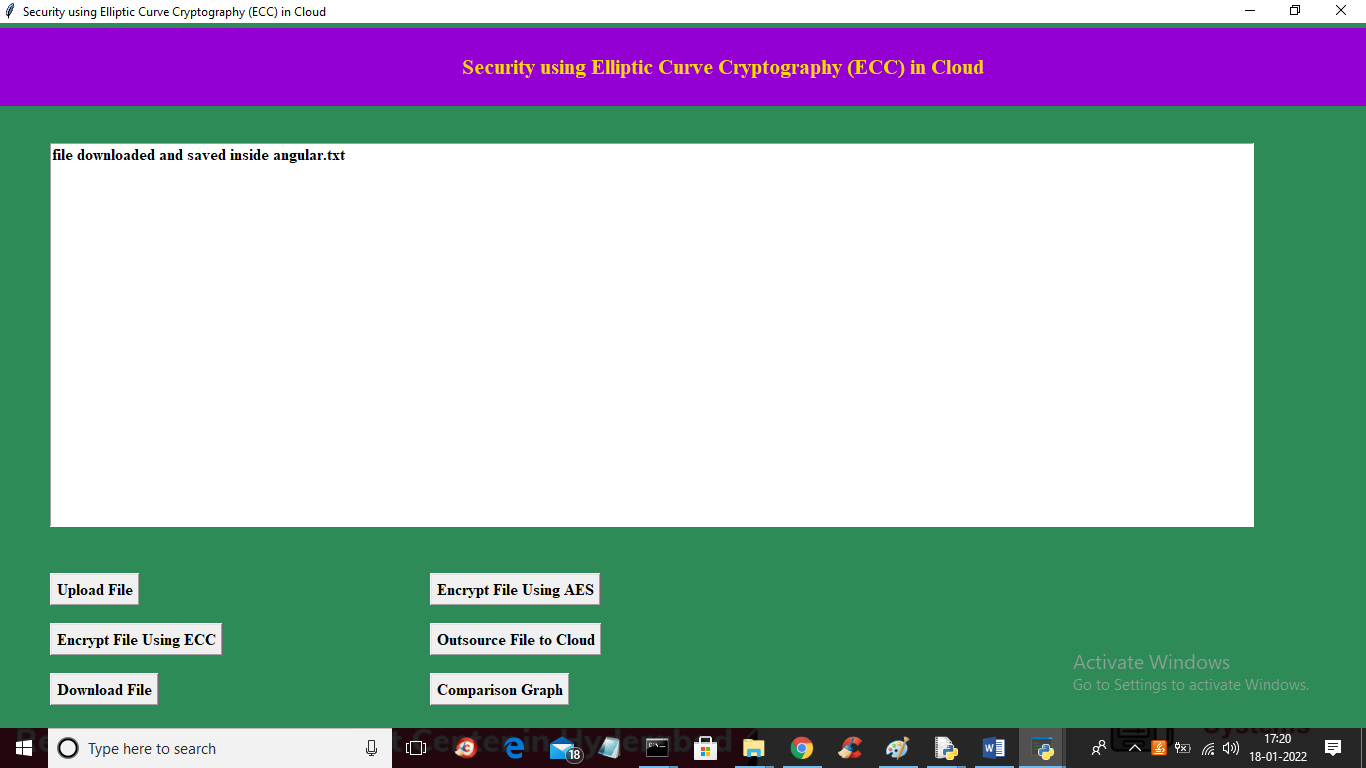
In above screen we can see file sent to cloud server and in ‘CloudServer/upload’ folder we can see same file stored in encrypted format



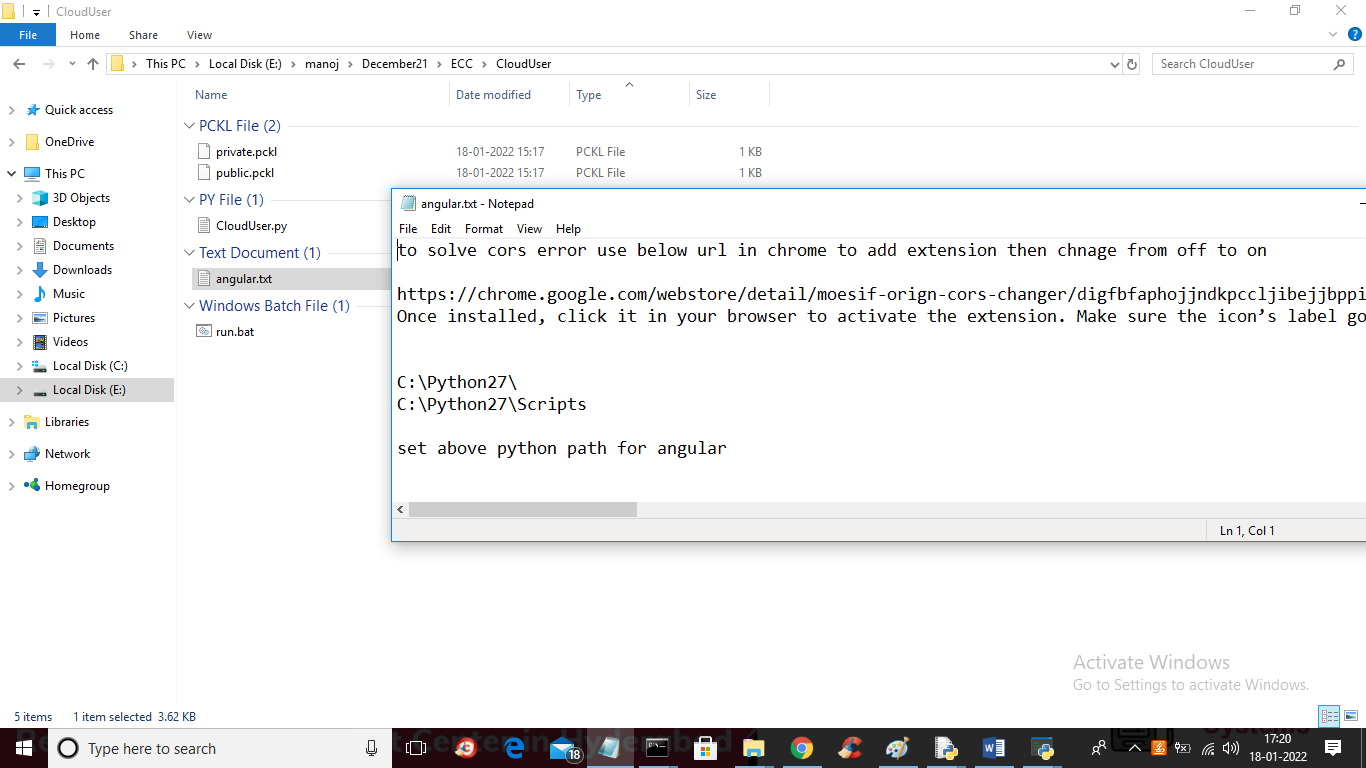
In above screen we can see that files saved in encrypted mode in CloudServer folder. Now click on ‘Download File’ button to download file



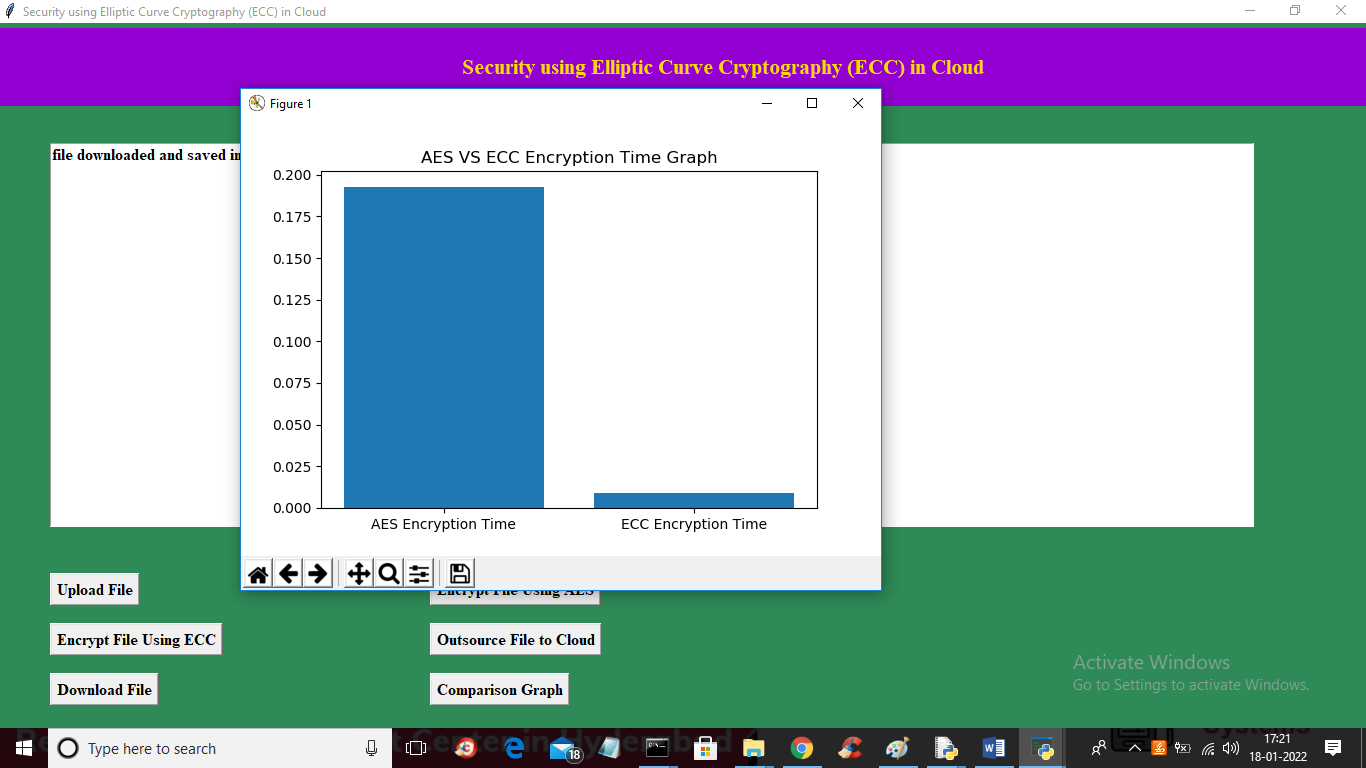
In above screen I entered file name to download and then click on ‘OK’ button to download file and to get below screen



In above screen we can see in text area that file is downloaded in CloudUser folder and now we can see that file in decrypted mode

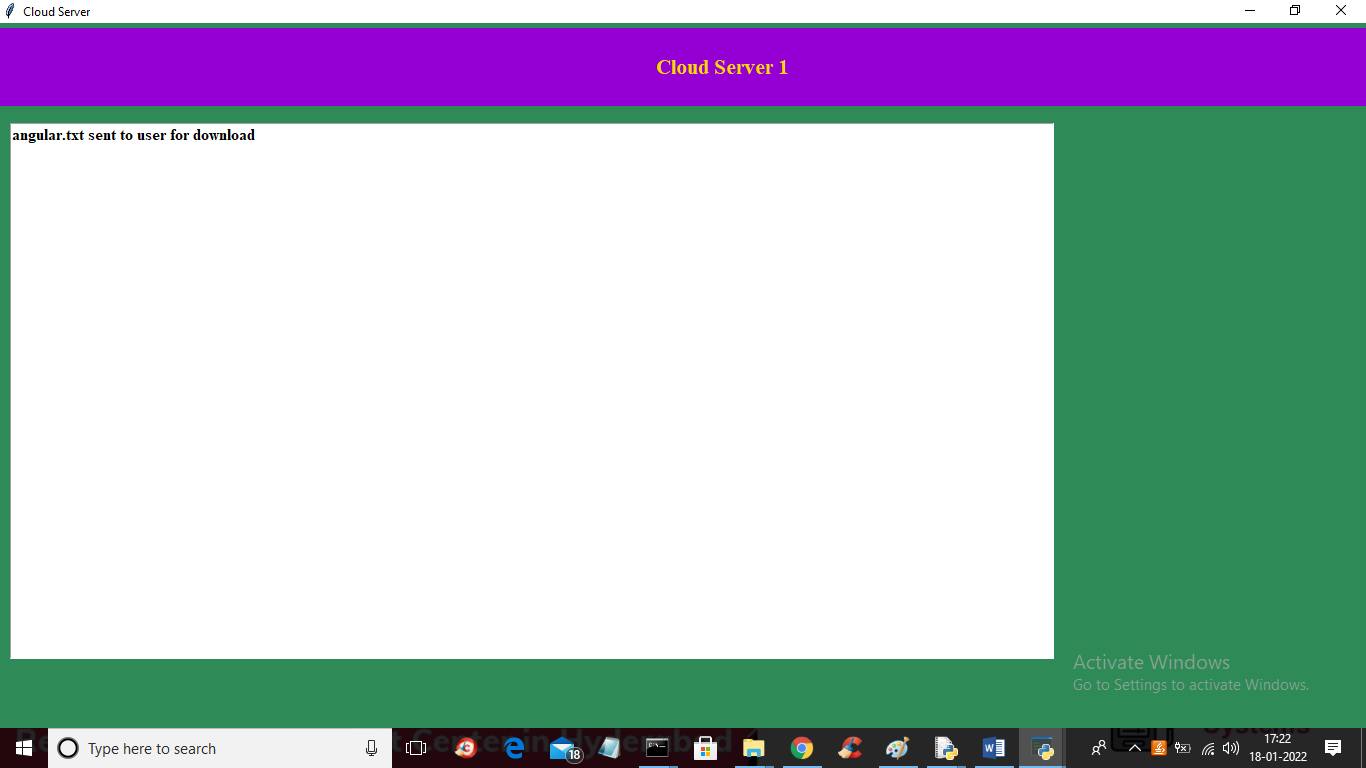


In above screen same file decrypted and showing in plain text mode and now click on ‘Comparison Graph’ button to get below graph



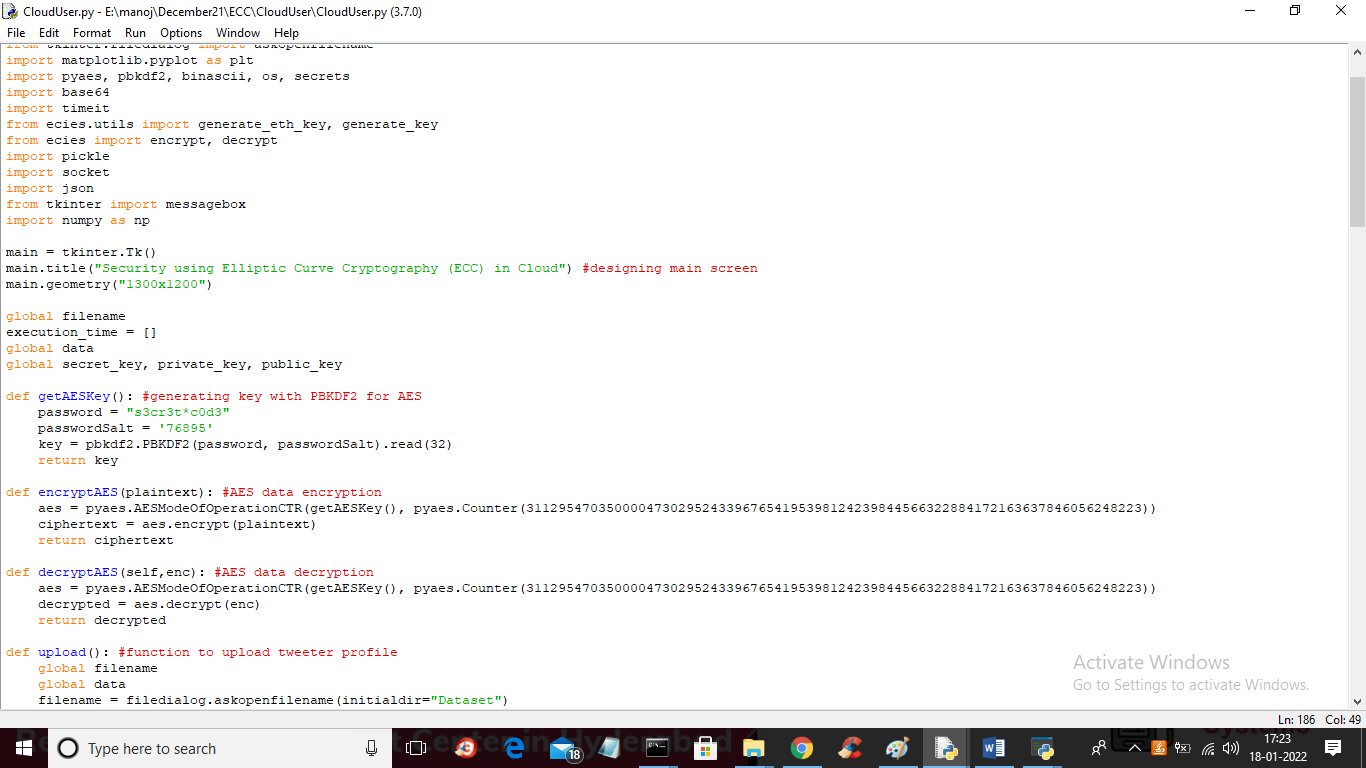
In above screen x-axis represents algorithm names and y-axis represents encryption time and in both algorithm ECC took less encryption time compare to AES.

In below cloud screen we can see all operations



Similarly you can upload and download any number of files from cloud and compare execution time between AES and ECC.

Below screen showing code to generate AES keys and encrypt and decrypt function



In above screen read red colour comments to know about AES and in below screen showing code from ECC

