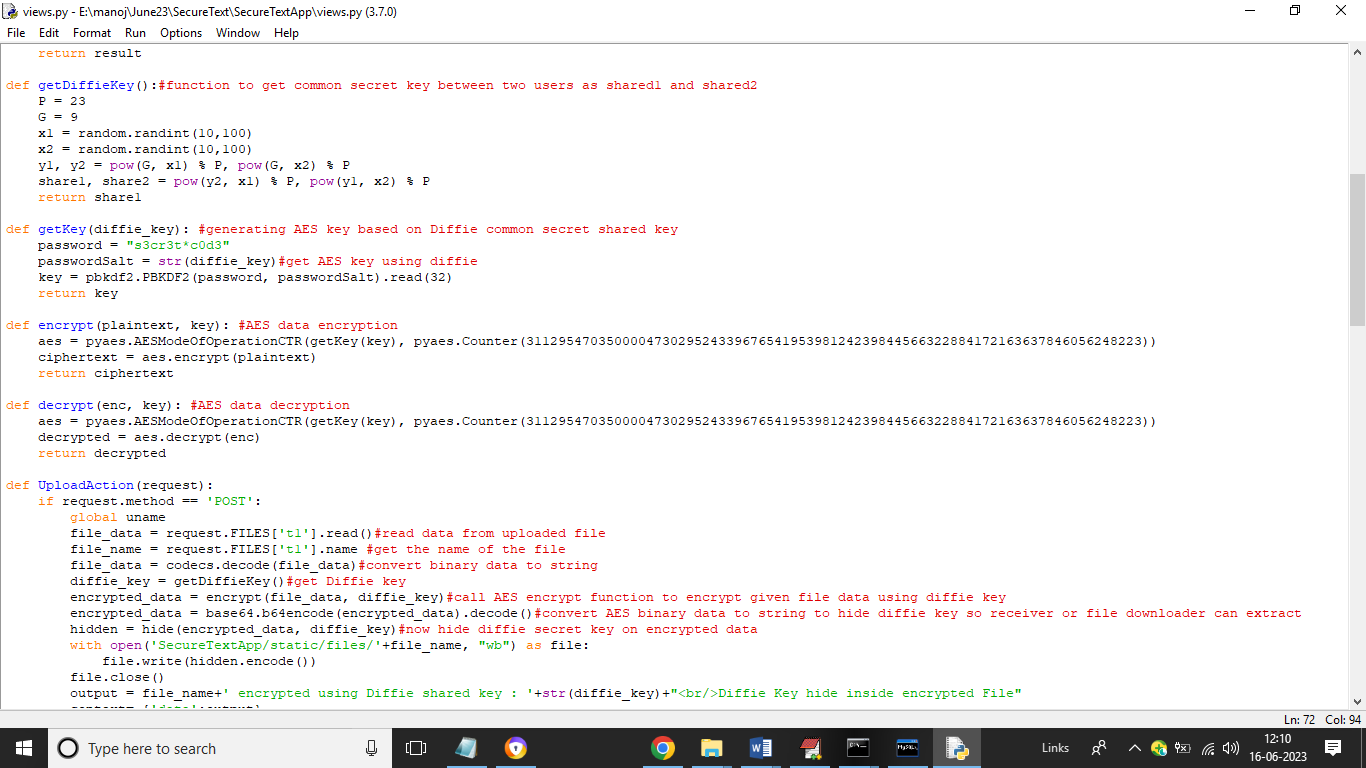
Secure Text Transfer Using Diffie-Hellman Key Exchange Based On Cloud

Cloud services offers heavy computation and storage server at cheaper cost so all companies or users are migrating their business data to cloud server but this clouds are away from user hands and their data store at 3rd party cloud servers. This cloud servers can view and misuse user’s data so to provide security to user data Encryption techniques are introduced which will provide security to user data.

In propose work we are using Diffie Hellman algorithm to generate common secret key between file uploader and downloader and then Diffie Key can be used to encrypt file and then user will hide Diffie key inside encrypted file as Secret Message. Recipient or downloader first extract key from encrypted file and then using that key will decrypt the file.

In encrypted file it’s not possible for cloud or hackers to know the hidden key from the encrypted file so he cannot decrypt and view the file so data will be fully secured.

In below screen we are showing code for Diffie Key Generation, AES file encryption using Diffie key and then hiding key to encrypted file.



In above screen read red colour comments to know about Diffie key generation, encryption and hiding key as secret message. Recipient will do reverse process to decrypt and download data.

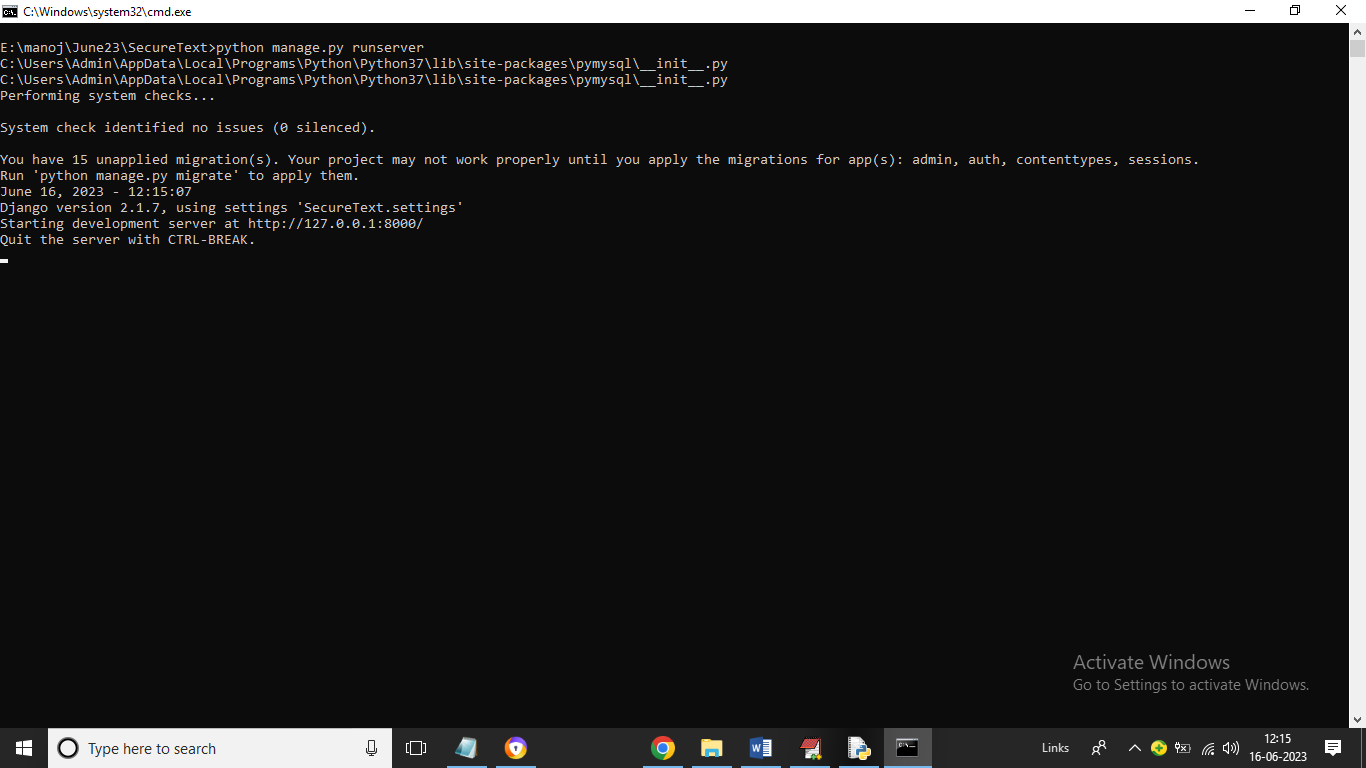
To implement this project we have designed following modules

1. New User Signup: using this module user can signup with the application
2. User Login: using this module user can login to application
3. File Upload: using this module user will upload file to cloud and then application will generate key, encrypt file and hide key to encrypted data as secret message
4. Download File: any genuine user can login to system and then browse list of files uploaded to cloud and then can select desired file to download and this file will get decrypted by extracting hidden keys and then download.

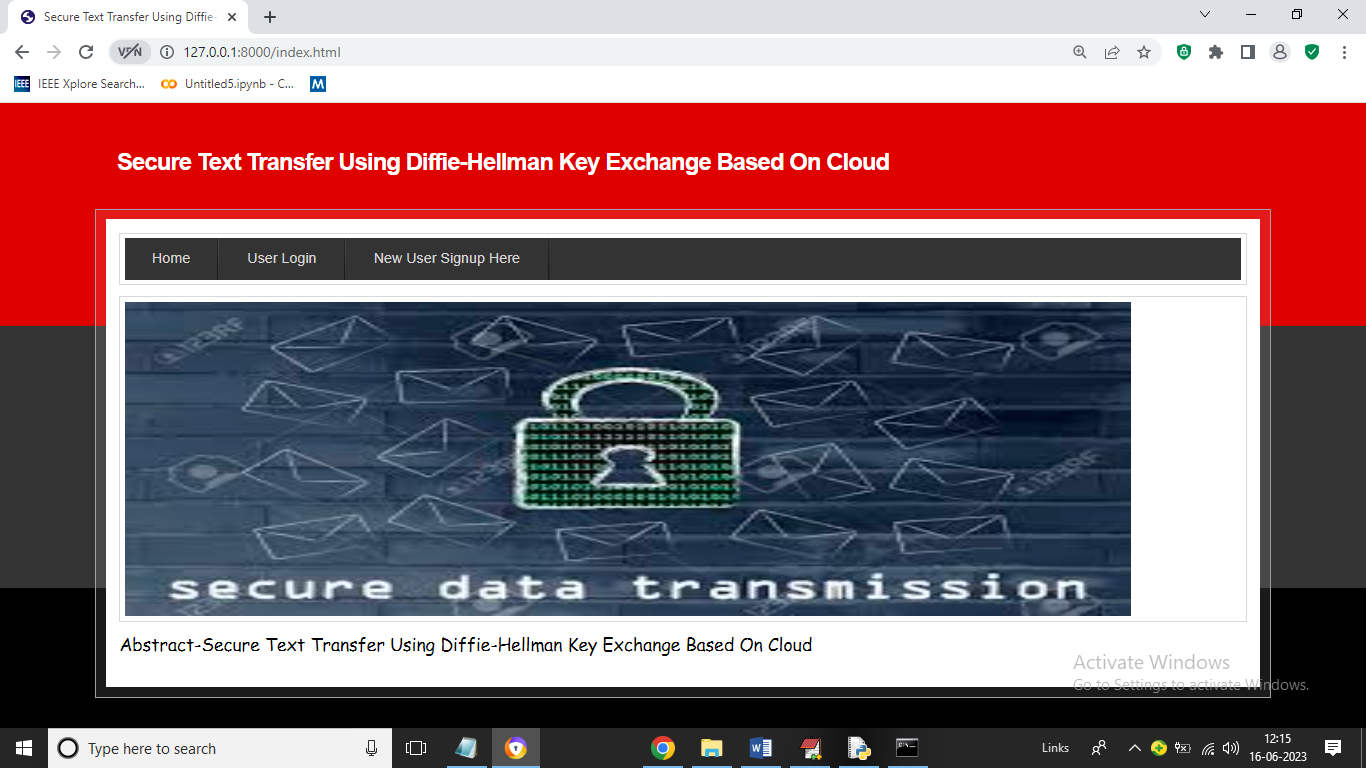
To run project install Python 3.7.0 and then install MYSQL database and then copy content from DB.txt file and paste in MYSQL to create database.

SCREEN SHOTS

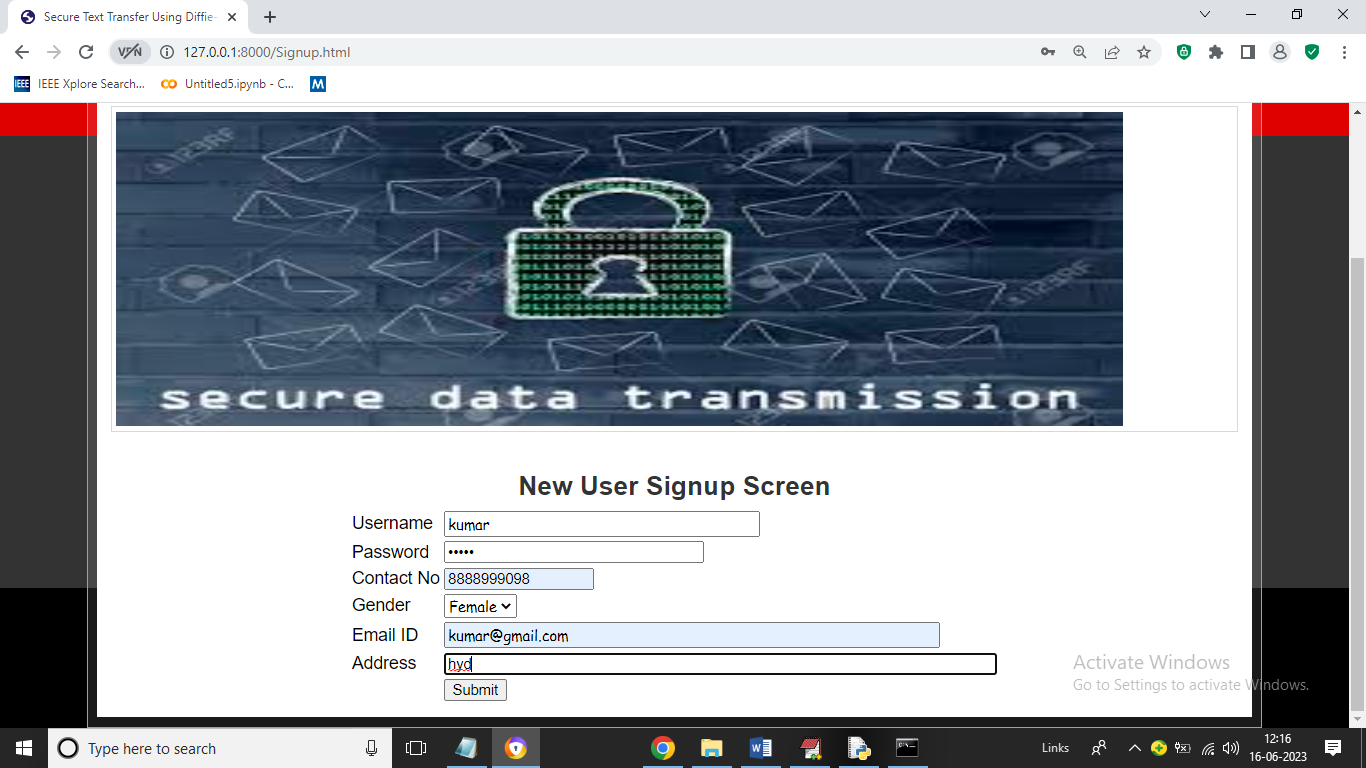
To run project double click on ‘run.bat’ file to get python web server and get below page



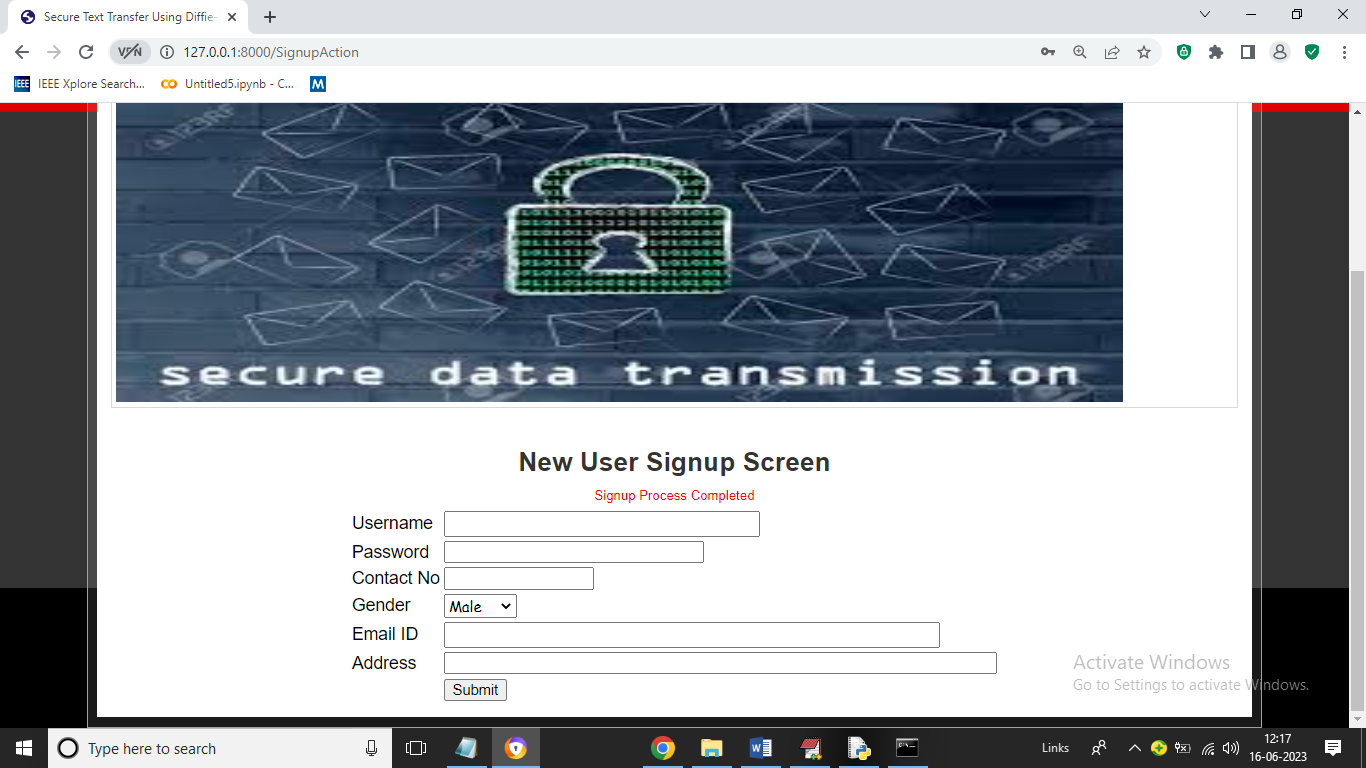
In above screen python server started and now open browser and enter URL as <http://127.0.0.1:8000/index.html> and press enter key to get below page



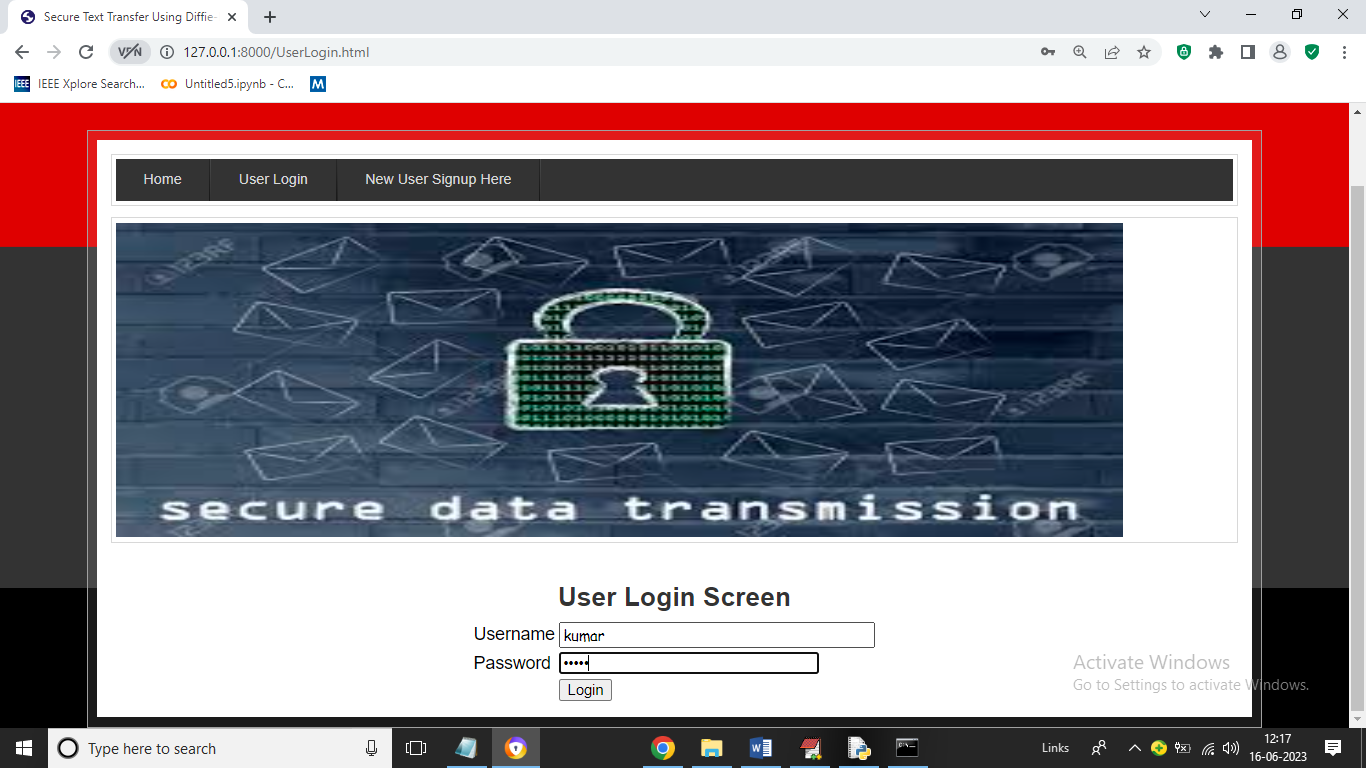
In above screen click on ‘New User Signup Here’ link to register new user



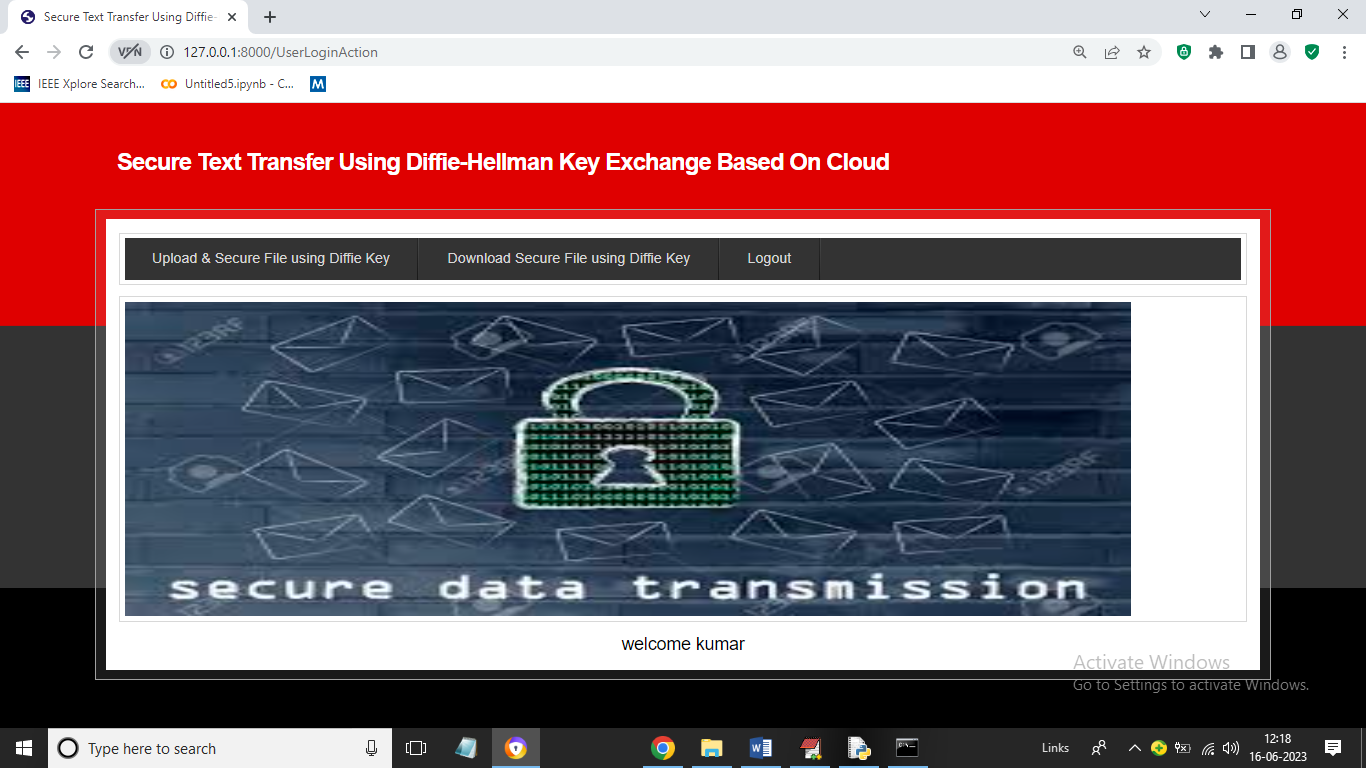
In above screen user is entering signup details and then press button to get below page



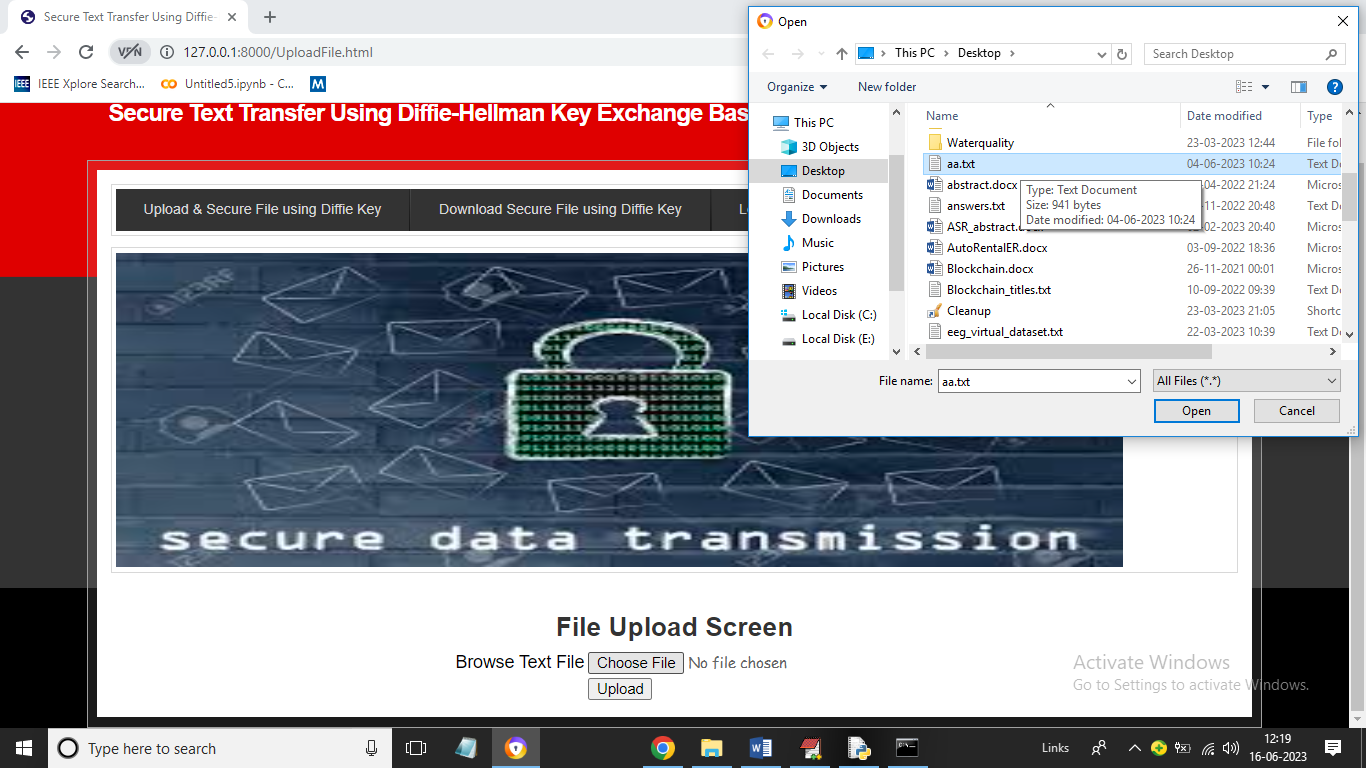
In above screen signup task completed and now click on ‘User Login’ link to get below login page



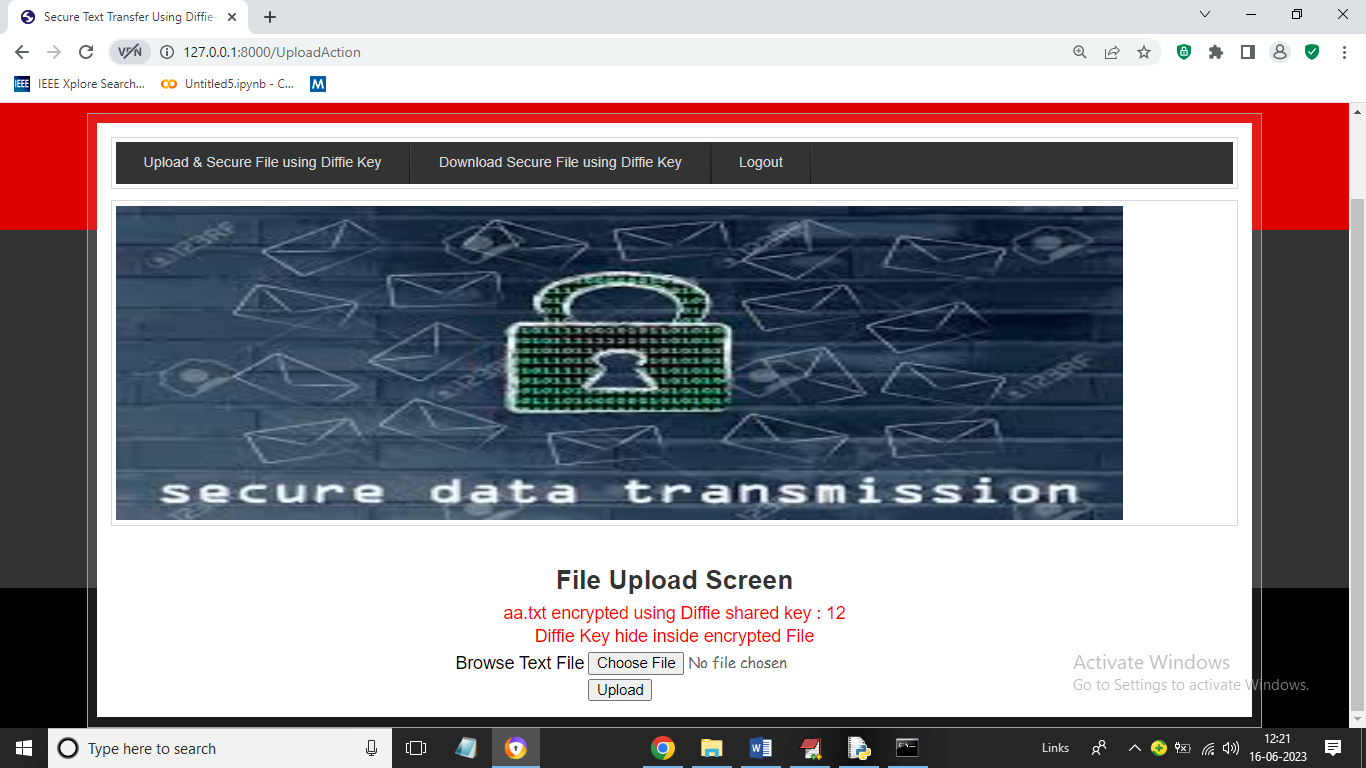
In above screen user is login and after login will get below page



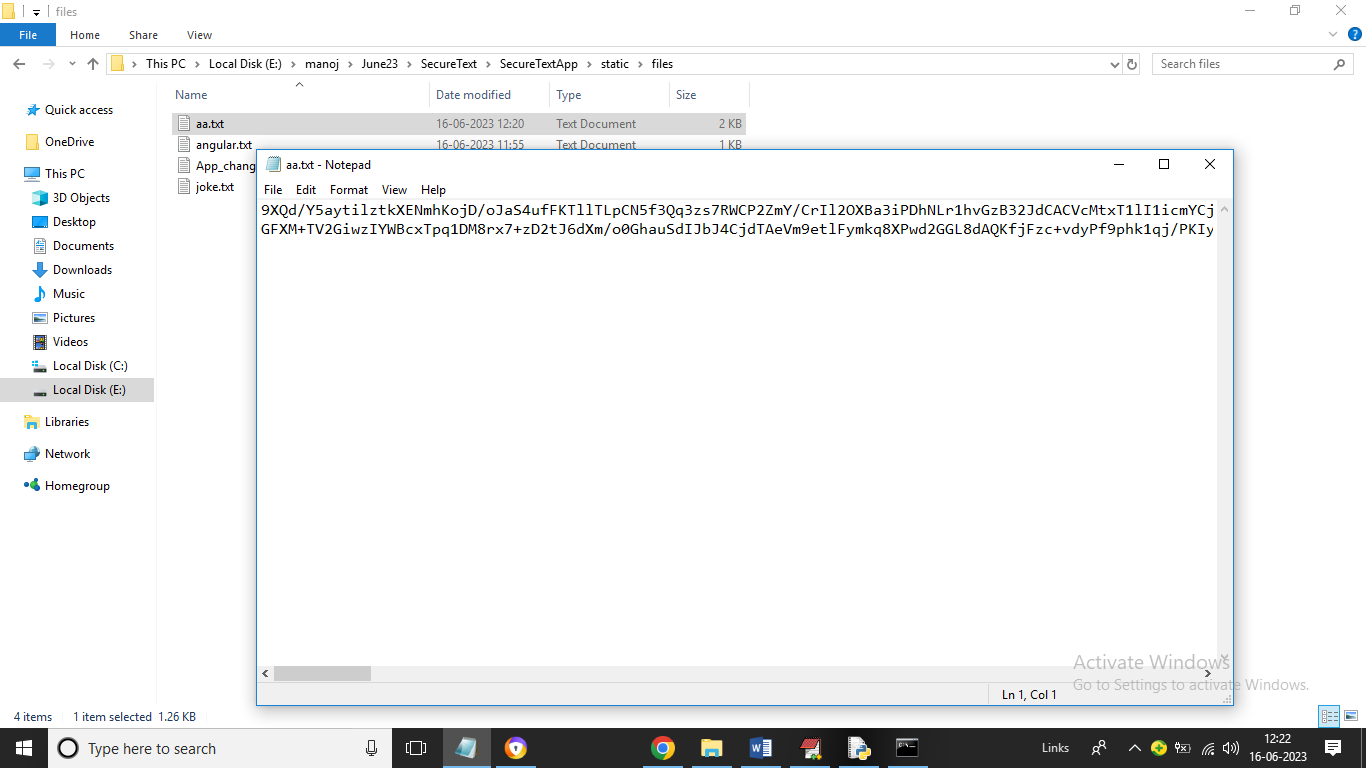
In above screen user can click on ‘Upload & Secure File using Diffie Key’ link to upload file which get encrypted and saved at cloud



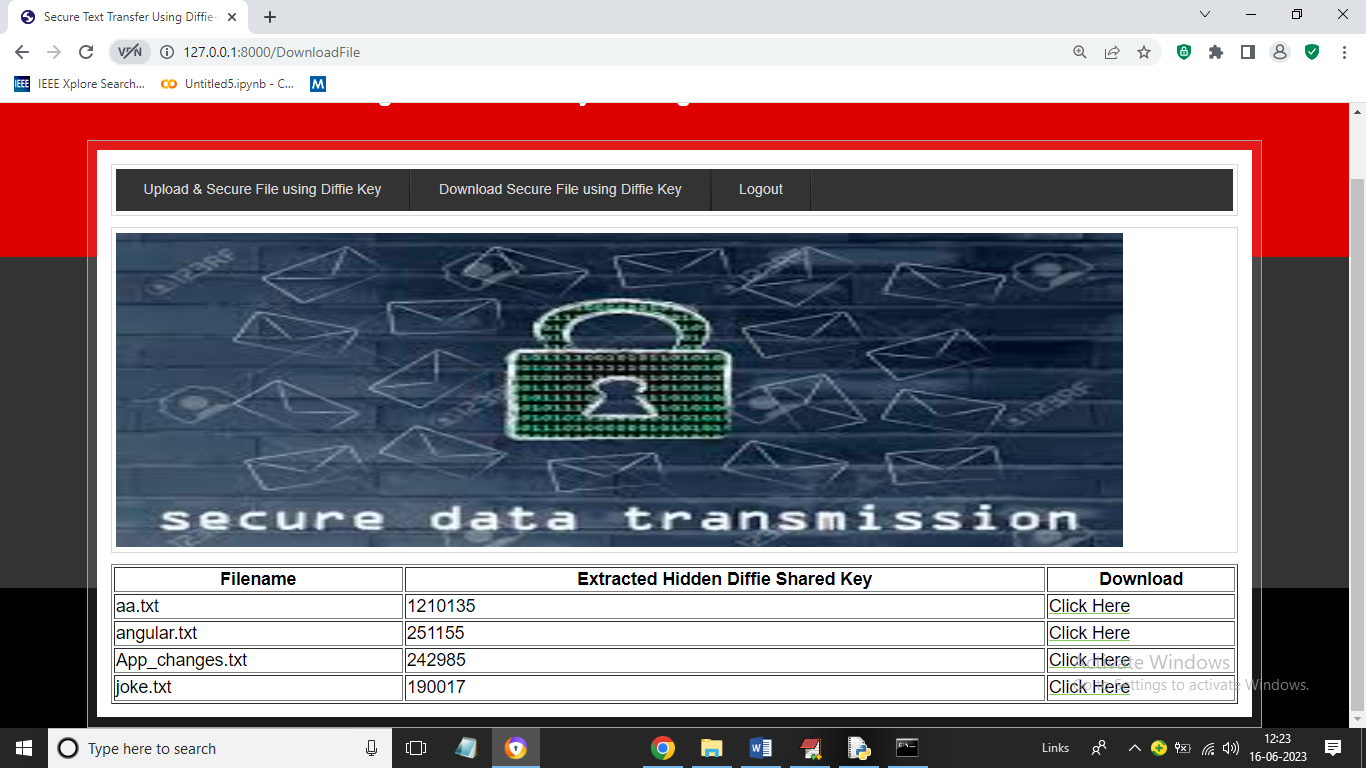
In above screen I am selecting and uploading ‘aa.txt’ file and then click on ‘Open’ and ‘Upload’ button to save above file in cloud server and get below page



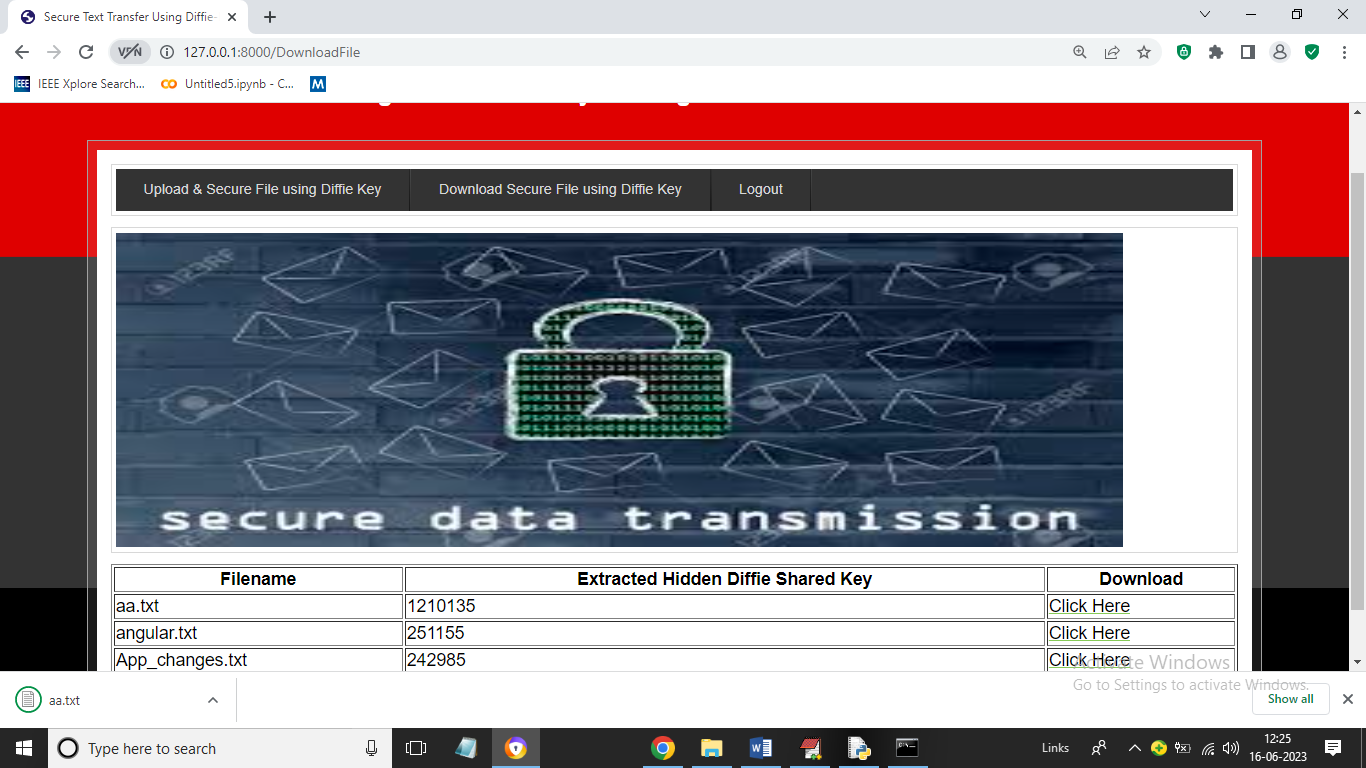
In above screen file is encrypted using Diffie key as 12 and we can see this file on server location such as ‘SecureTextApp/static/files’ folder and in below screen we can see uploaded ‘aa.txt’ file data



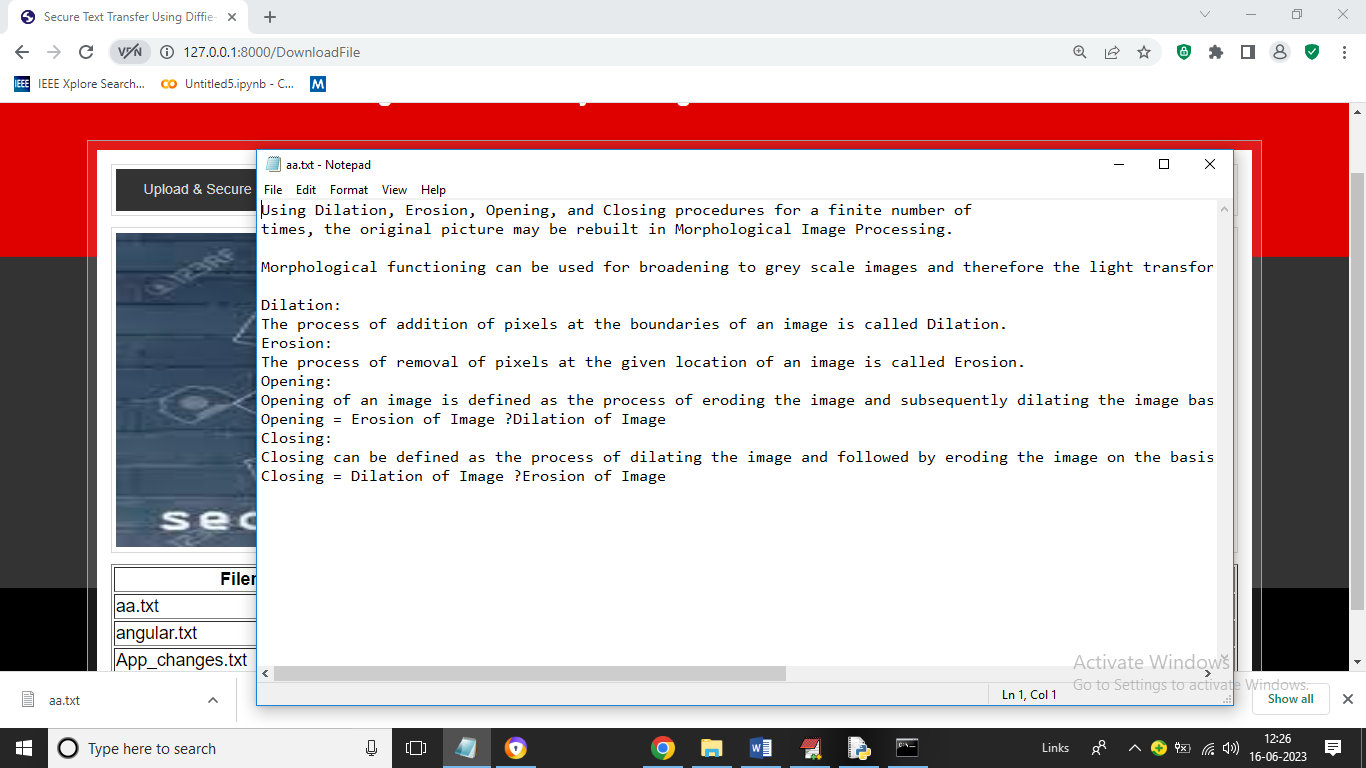
In above encrypted data hacker don’t know here Diffie key is hidden so he cannot decrypt data and now click on ‘Download Secure File using Diffie Key’ link to view list of uploaded and shared files like below screen



In above screen user can see the uploaded file with hidden and extracted Diffie keys and user can click on ‘Click Here’ link in any file row to download that file in decrypted format and now I am downloading ‘aa.txt’ and showing in below screen downloading status



In above screen in browser status bar we can see file is downloading and now we can open and view file content in below screen



In above screen ‘aa.txt’ file is showing as decrypted data.

Similarly by following above screens you can upload and secure files