Cybersecurity: Data Protection using Hybrid Encryption & Steganography

Growing technologies making user data to be float in network universe with the help of centralized servers like Clouds and Decentralized servers like P2P or Blockchain. All servers providing heavy encryption for user data security but data store away from user hands always vulnerable to 3rd party malicious server employees who can easily get database keys and can decrypt user data.

To avoid above data leakage we are employing Hybrid and steganography based self-data protection algorithms to provide more security to user’s data. In propose work as Hybrid encryption we are encrypting file with symmetric (AES) and asymmetric (ECC) algorithms and this Hybrid Encryption will not allow Server employees to know keys of both algorithms and file will not be decrypted.

In Steganography process user can hide messages in images and upload to network like plain image and malicious users aware of hidden message and user data will be secured. Note: you ask for video and audio steganography also but this required heavy computation so we are employing Image based Steganography.

To further check file integrity we are generating hashcode on uploaded file so file content will be verify anytime with the help of hashcode.

To allow only genuine user to access account we are employing Multi Factor based authentication where user has to authenticate with normal login and then must be authenticated via EMAIL OTP. So give valid Email ID during registration.

To aware user about Cybersecurity issues we are allowing user to know about latest tools and learning materials by accessing modules like ‘Learning Material and News Updates’.

To implement this project we have designed following modules

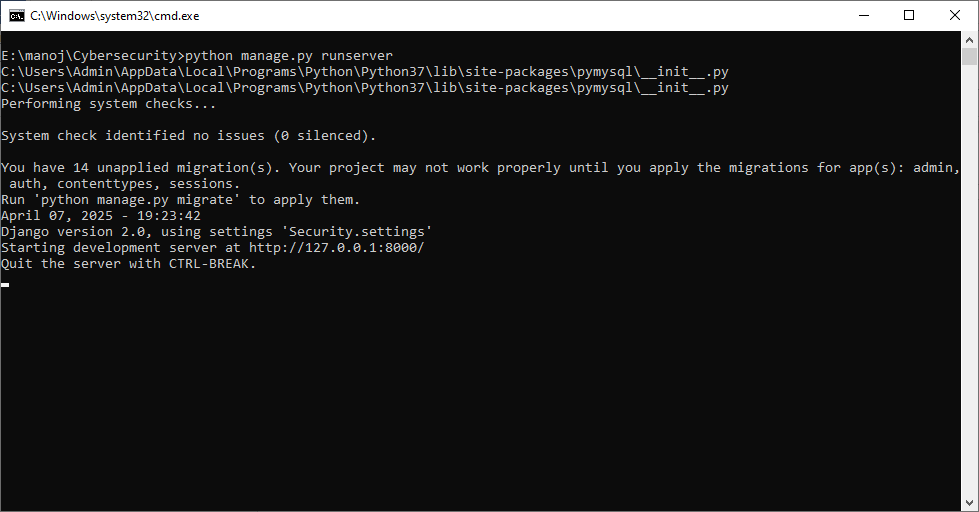
1. New User Sign up: user can sign up with the application
2. User Login: user can login to system and then authenticate via OTP process
3. Hybrid Encryption: using this module user can upload any file which will get encrypted using Hybrid Encryption process and file integrity process will be done with hashcode.
4. Image Steganography: using this module user can enter some message and then upload image and then system will hide encrypted message in image
5. Access Data: using this module user can access data anytime and normal file can be downloaded in decrypted process and steganography images will be extracted and display to user
6. Learning Tools: using this module user can learn about new tools on Cybersecurity
7. News Updates: using this module user can get latest modules

Note: all possible modules we have added in this project

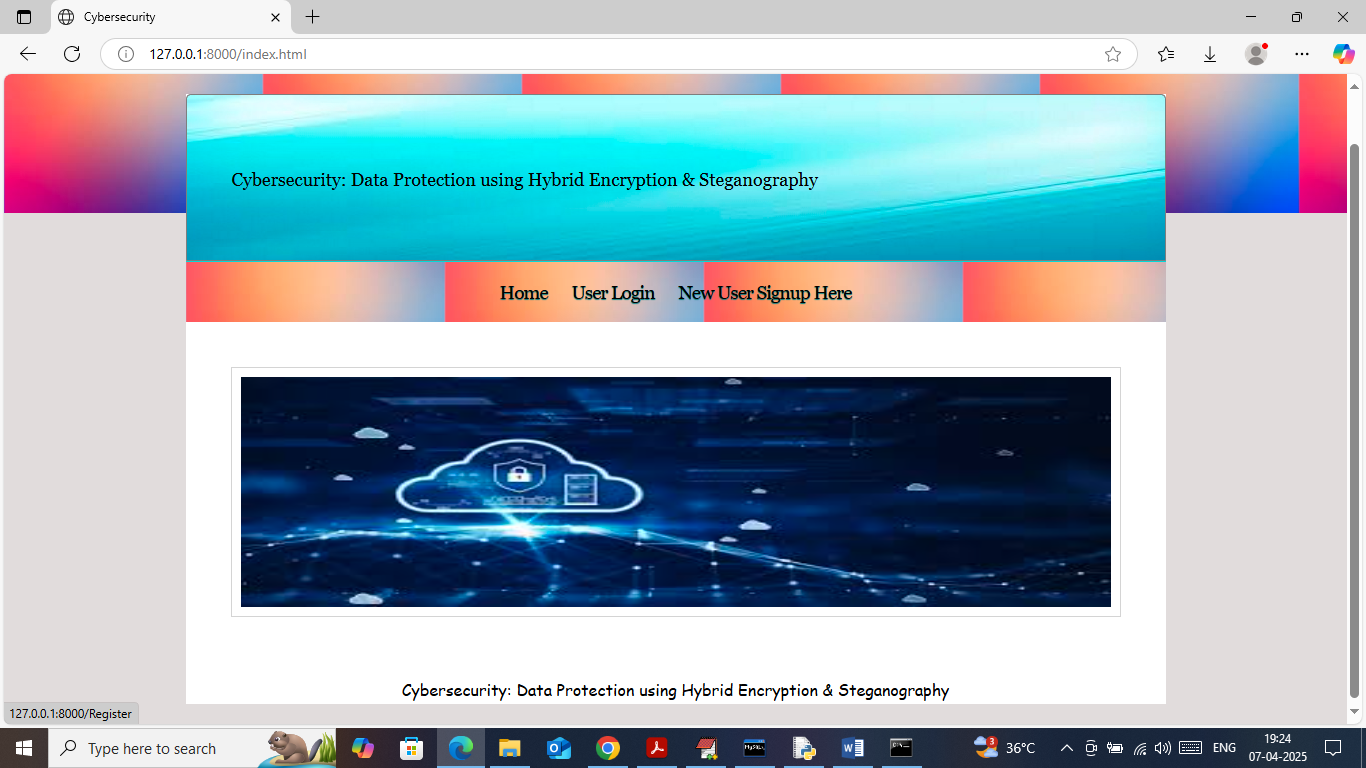
SCREEN SHOTS

To run project install python 3.7.2 and then install all packages given in requirements.txt file. Install MYSQL and then copy content from ‘database.txt’ file and paste in MYSQL console to create database.

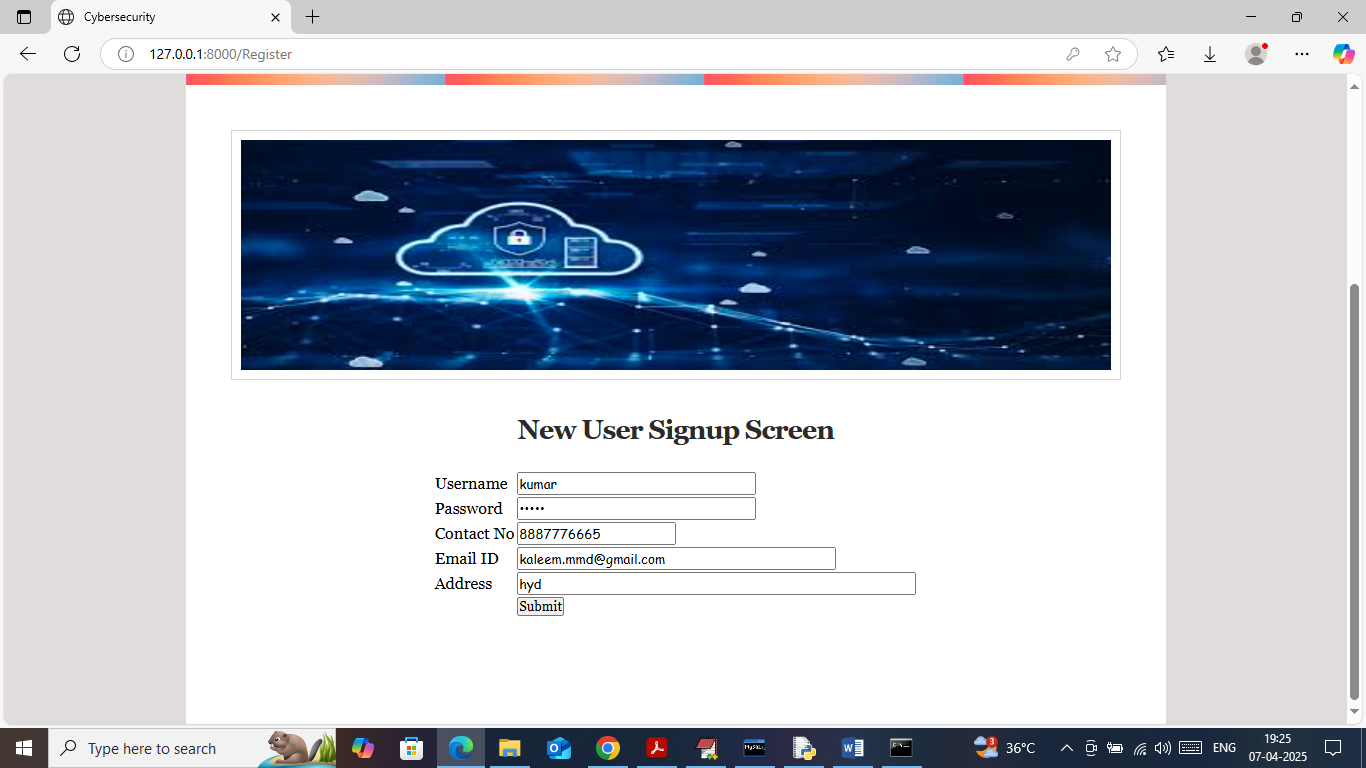
Now double click on ‘run.bat’ file to start python web server and then will get below page



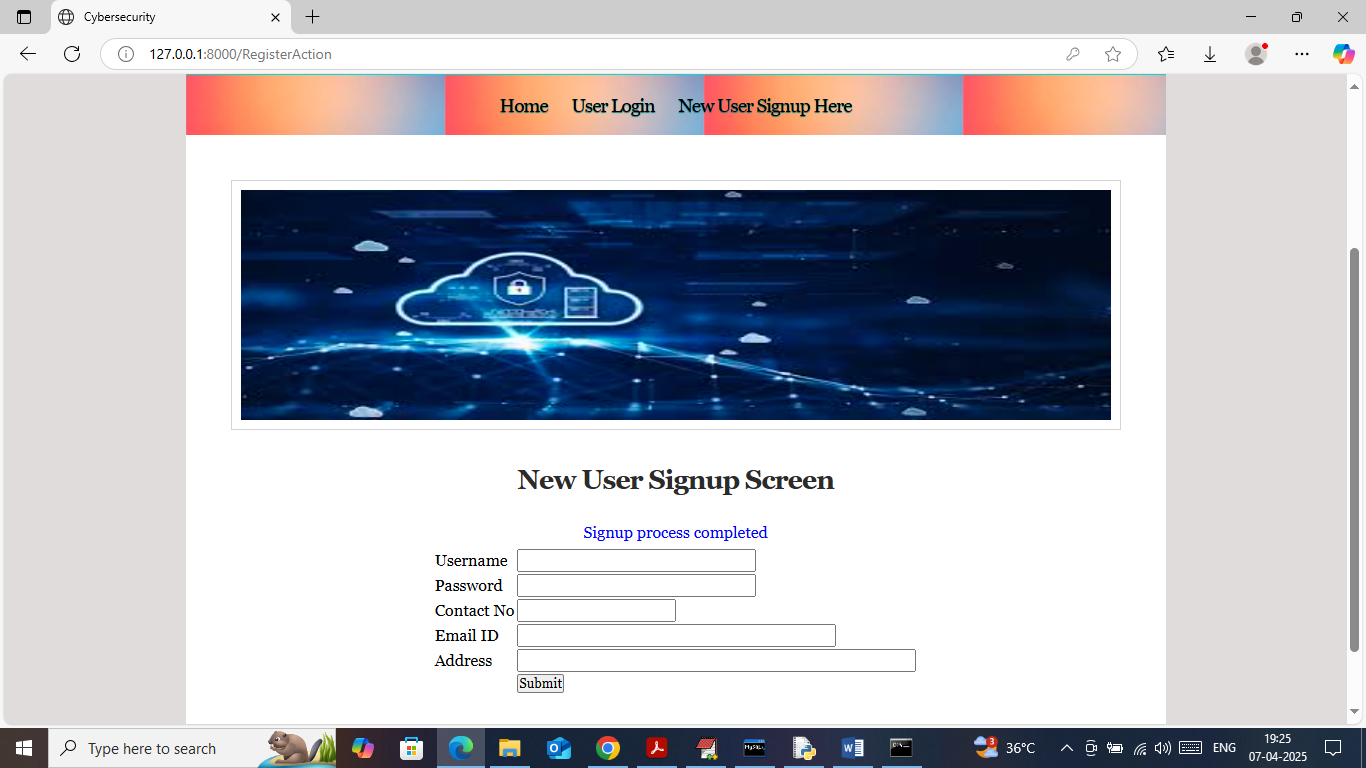
In above screen python server started and now open browser and enter URL as <http://127.0.0.1:8000/index.html> and then press enter key to get below page



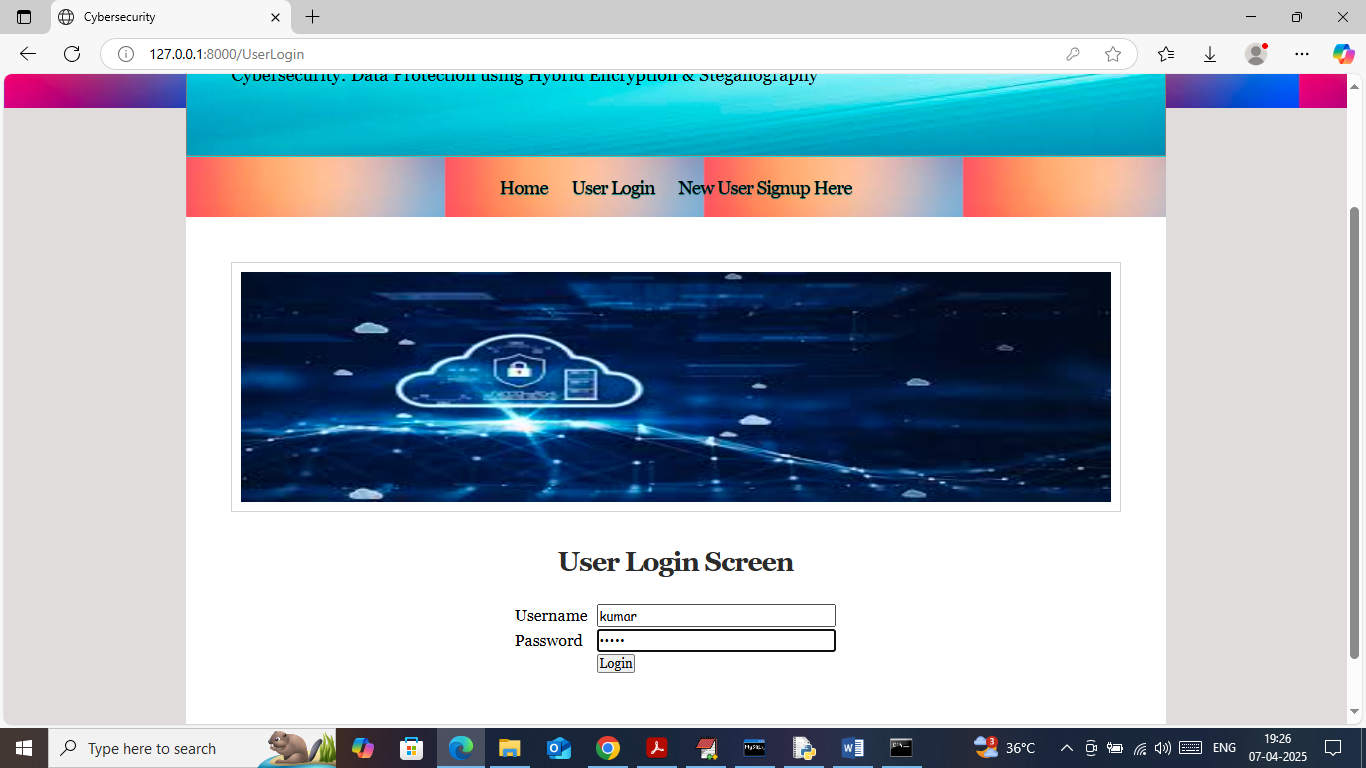
In above screen click on ‘New User Sign up’ link to get below page



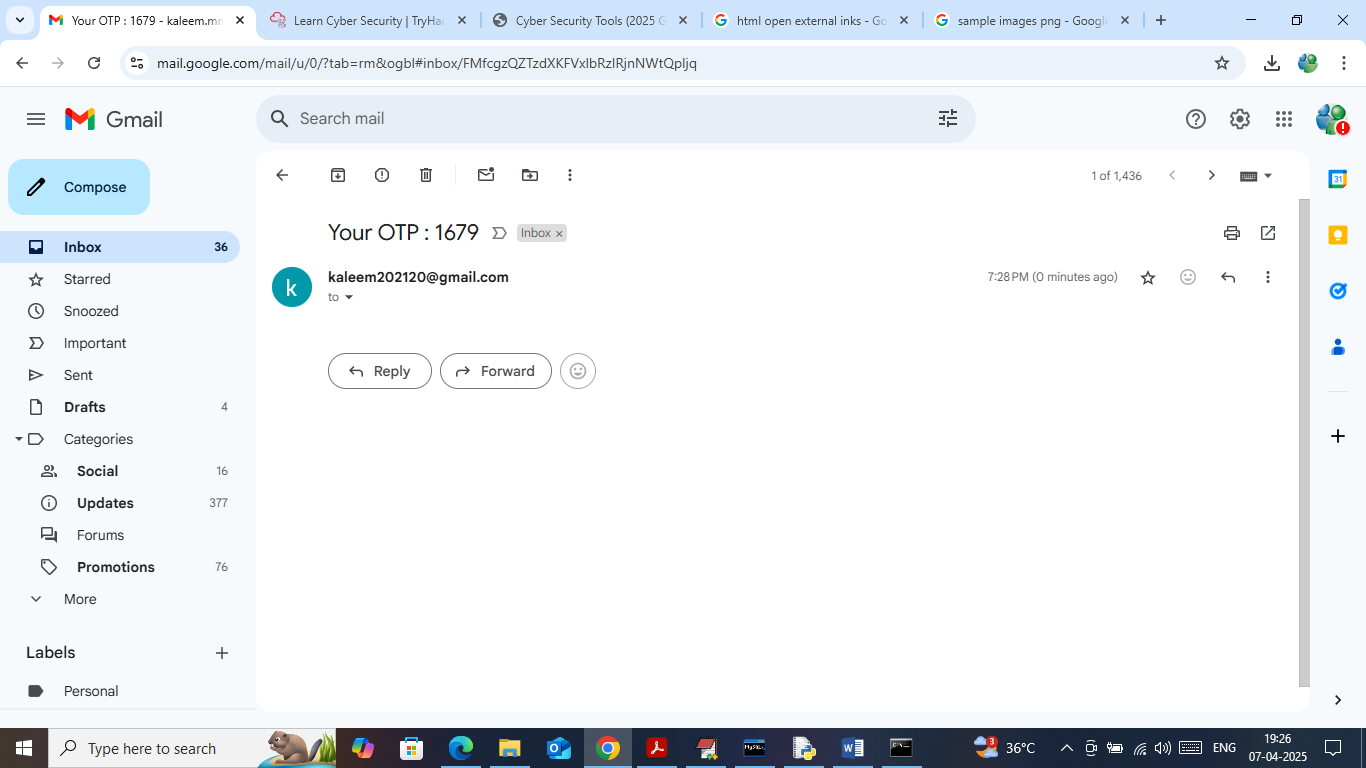
In above screen user is entering sign up details and then press button to get below page



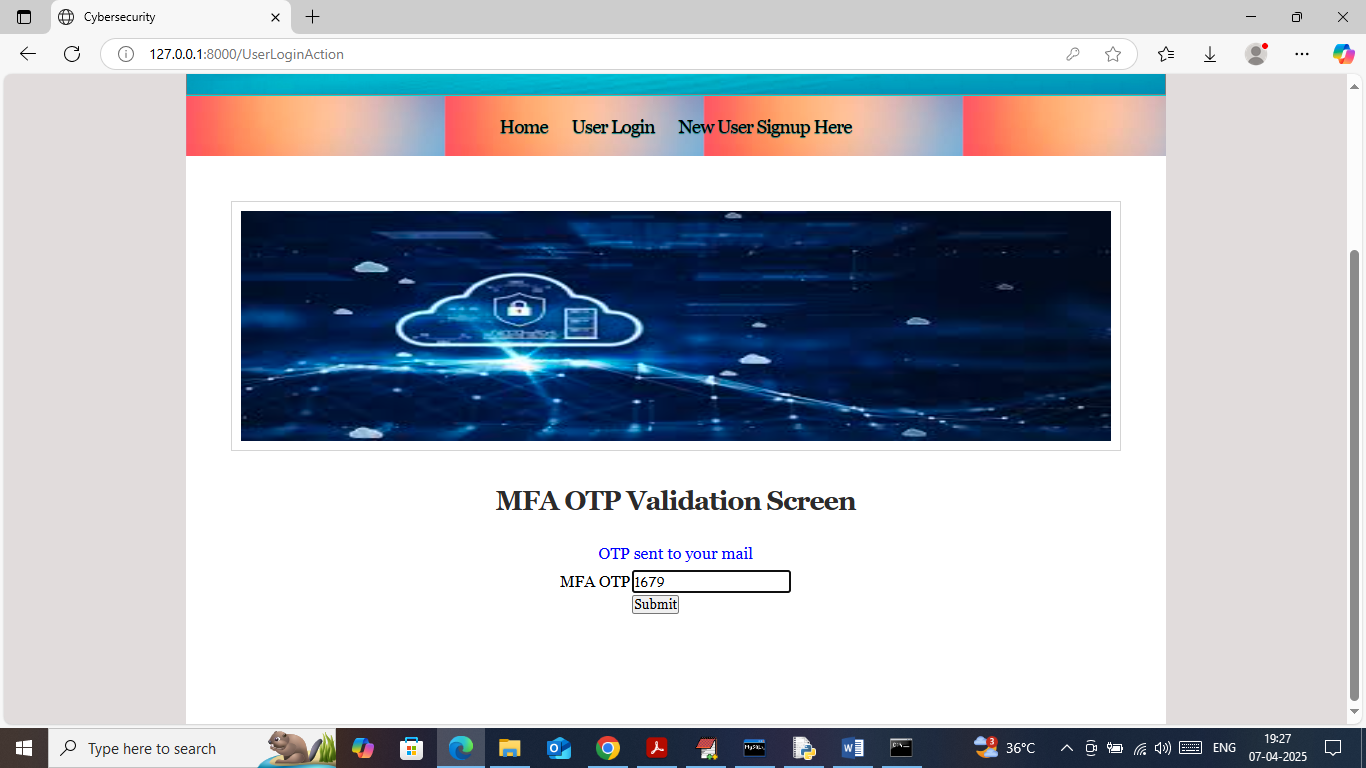
In above screen sign up process completed and now click on ‘User Login’ link to get below page



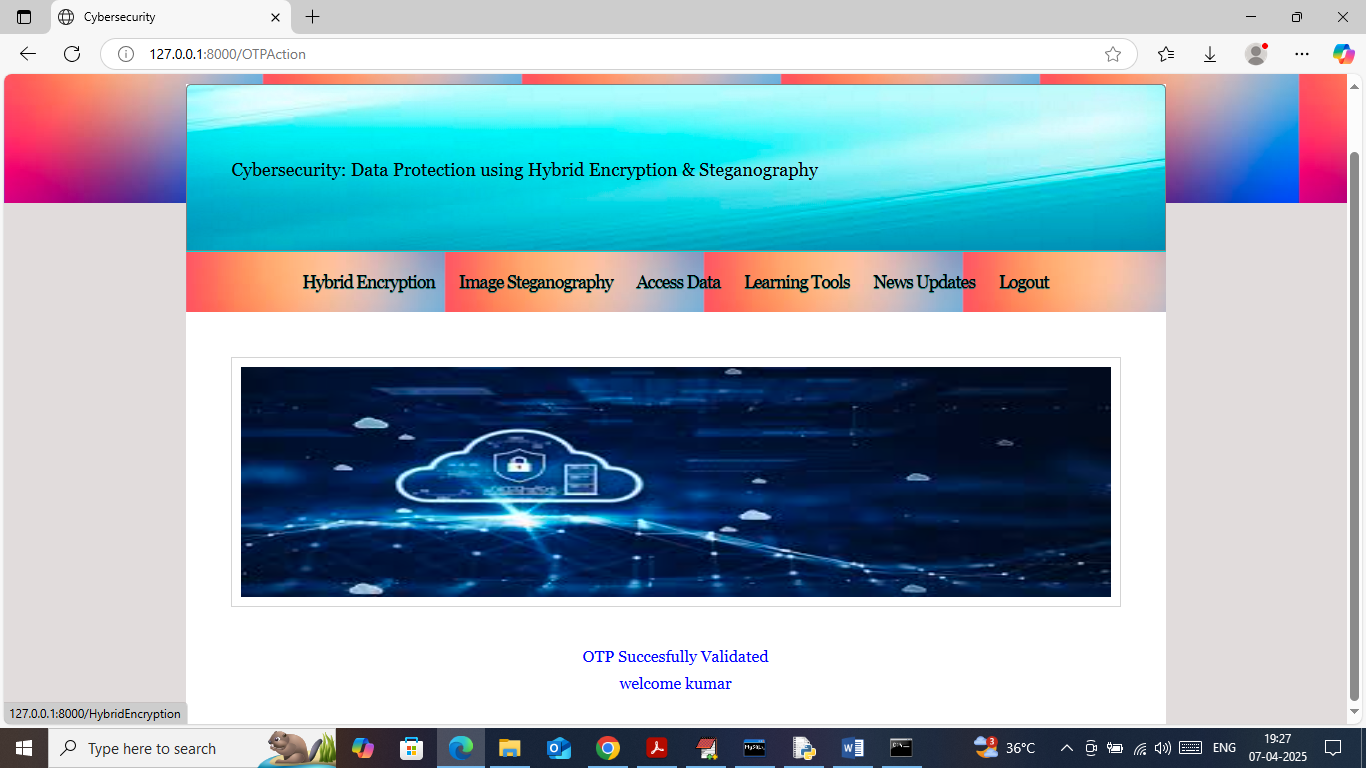
In above screen user is login and after login will get OTP in email like below page



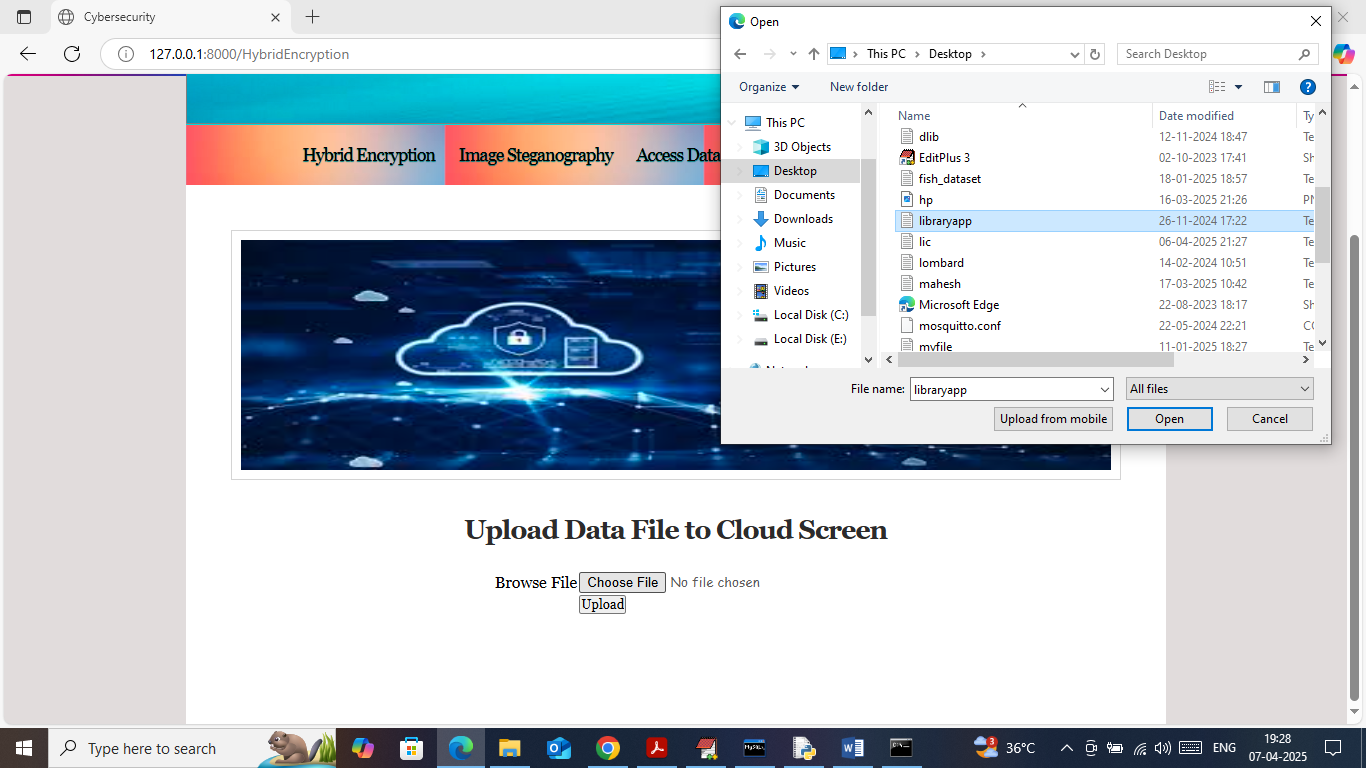
In above screen OTP received to email and enter to application to continue authentication process



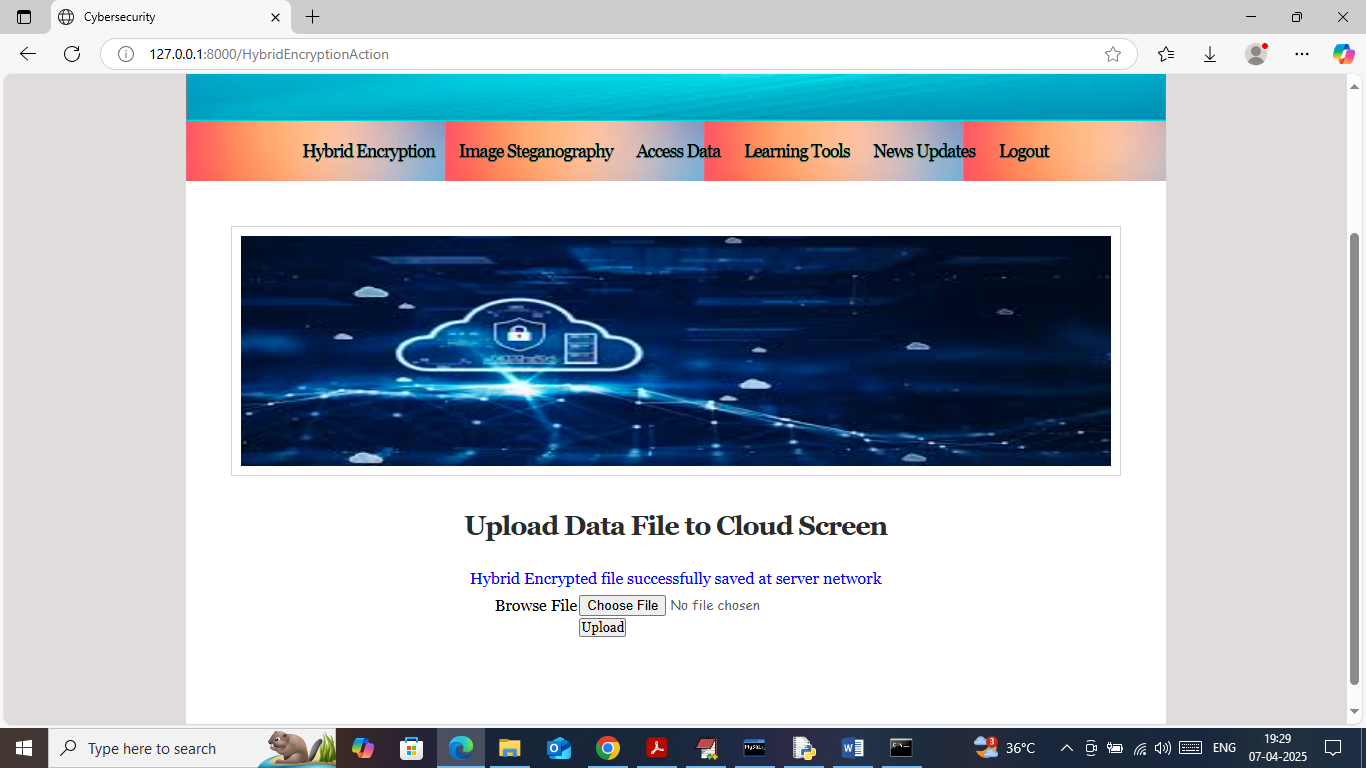
In above screen enter OTP and then press button to get below page



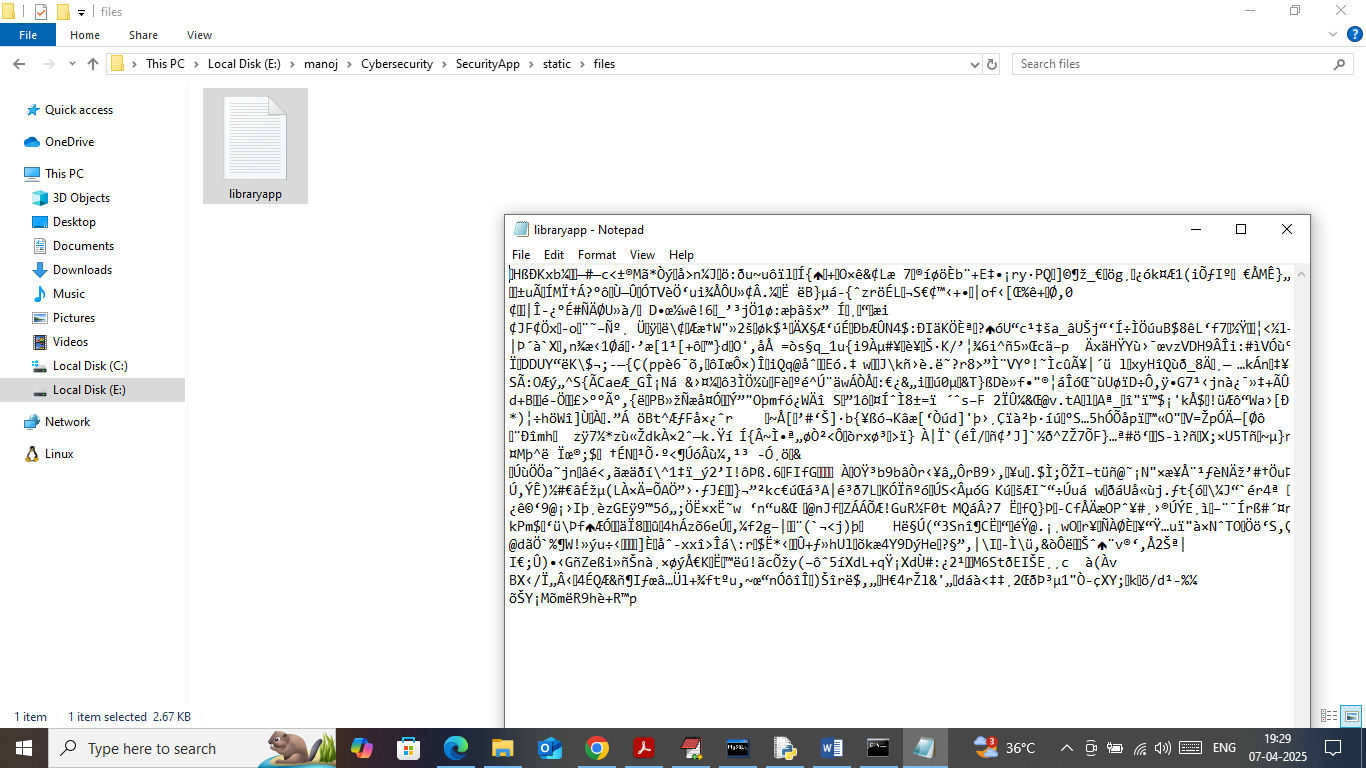
In above screen user can click on ‘Hybrid Encryption’ link to get below page



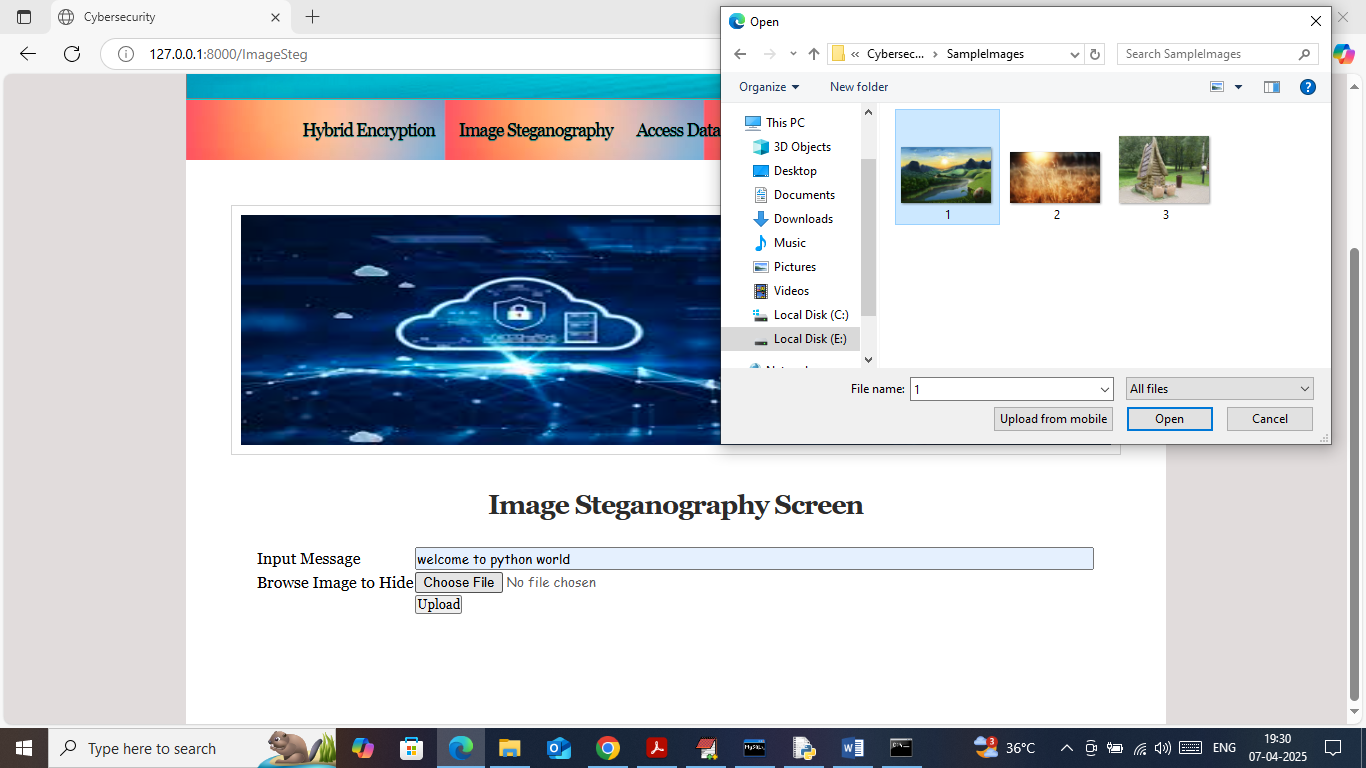
In above screen select and upload any file and then click on ‘Open and upload’ buttons to saved file in encrypted format and then will get below page



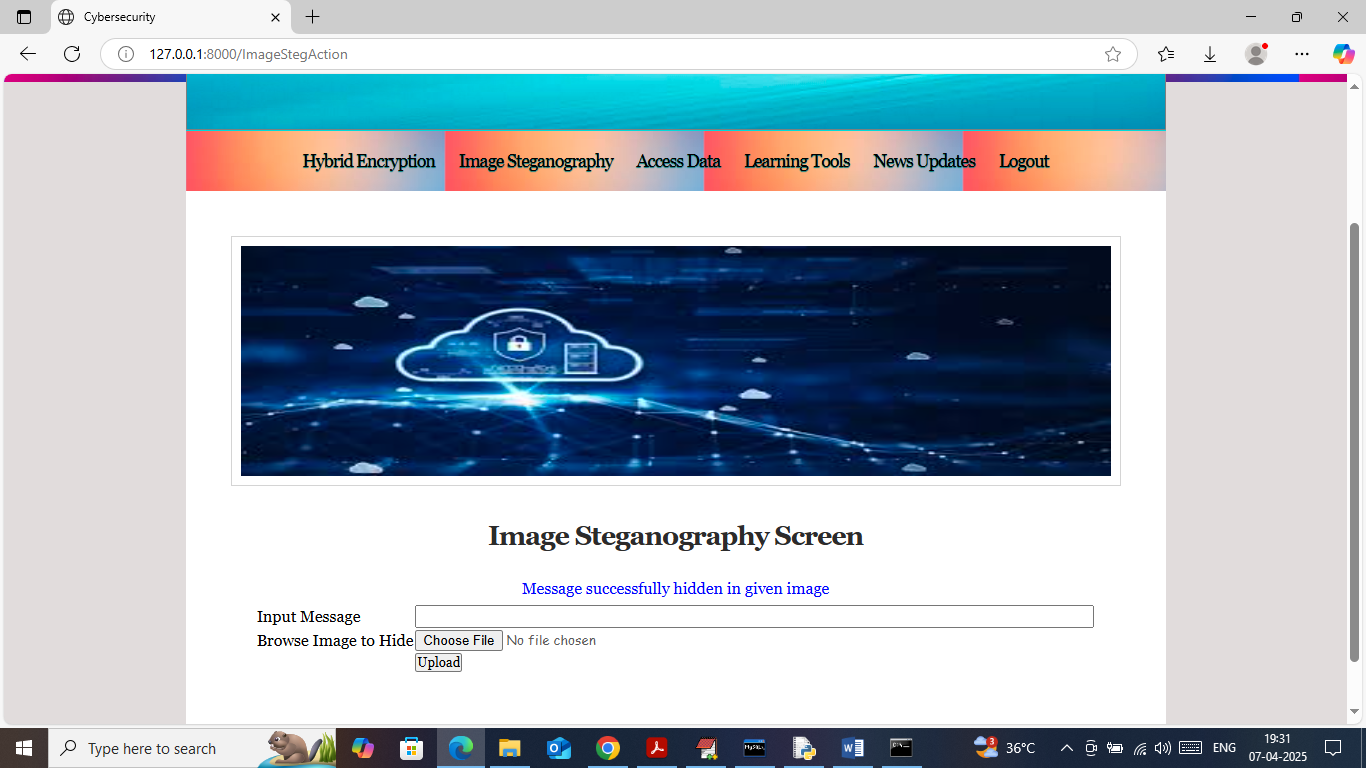
In above screen can see file saved at server and in below screen can see file content in encrypted format



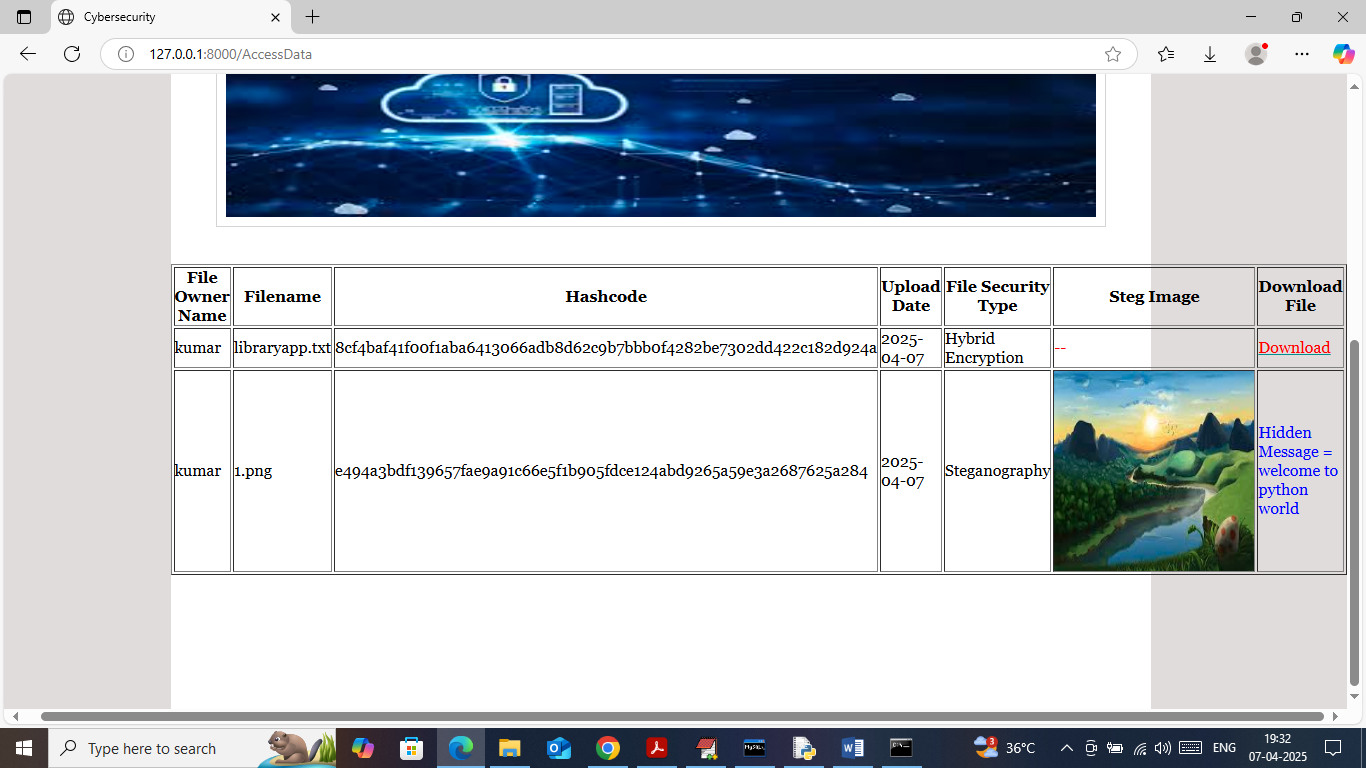
In above screen can see file content is in very heavy encrypted format and now go back and click on ‘Image Steganography’ link to hide message



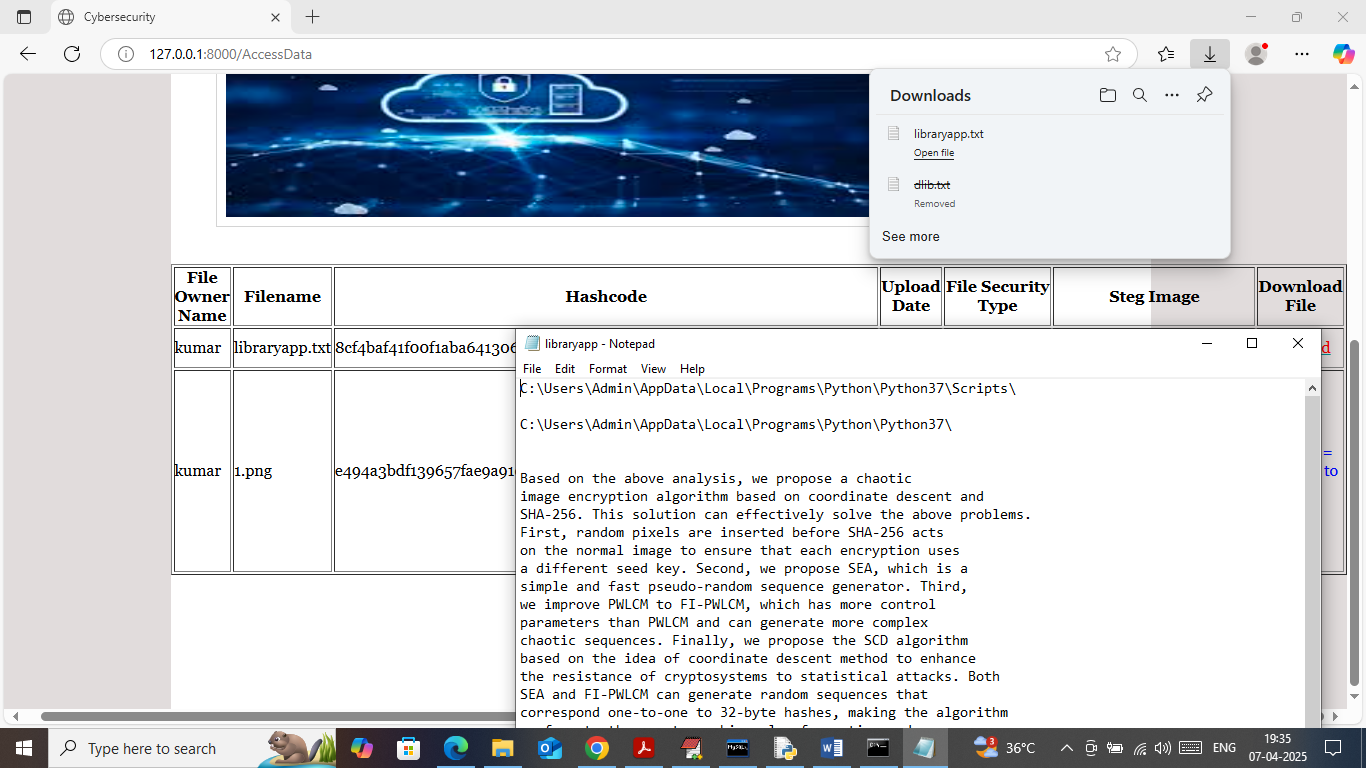
In above screen in text field I entered some message to hide and then selecting and uploading image and then press buttons to get below page



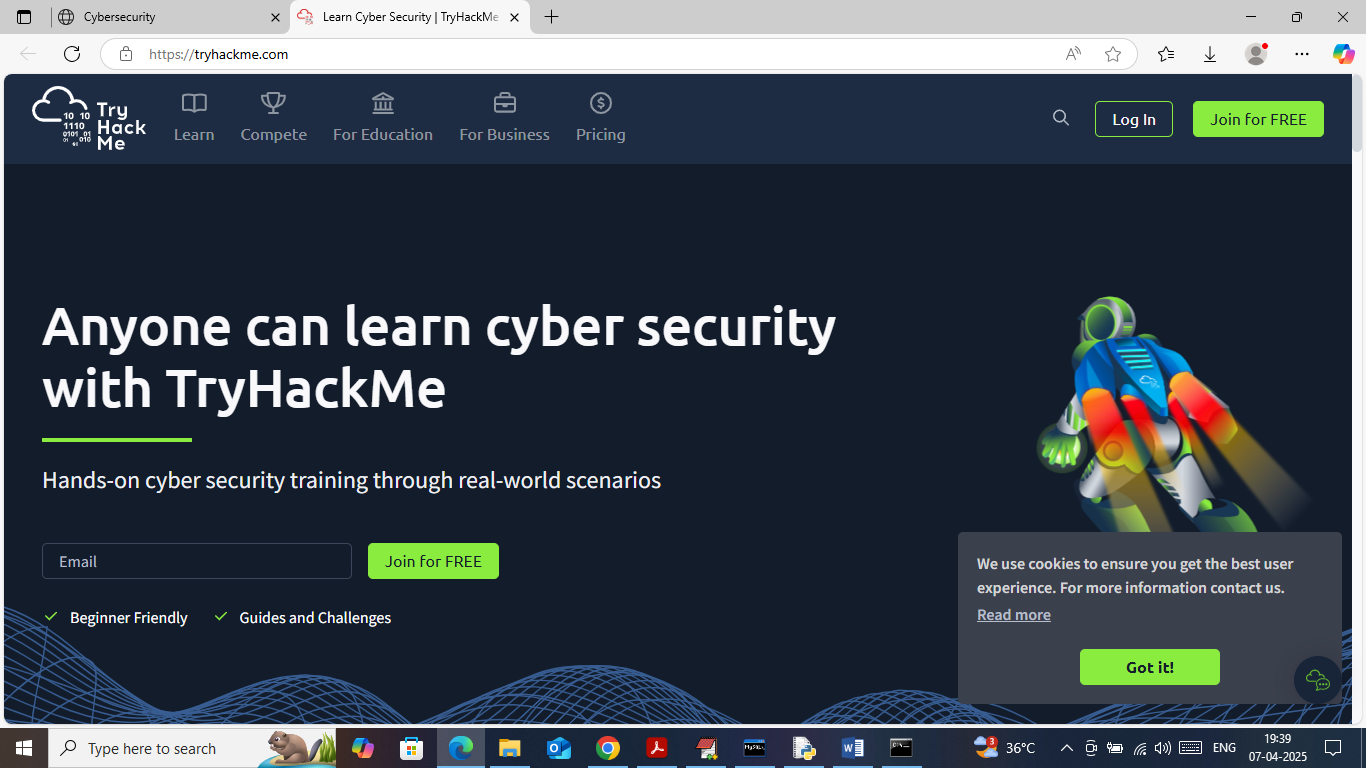
In above screen can see message successfully hidden in image and similarly you can upload and test any number of files. Now click on ‘Access Data’ link to access past uploaded files



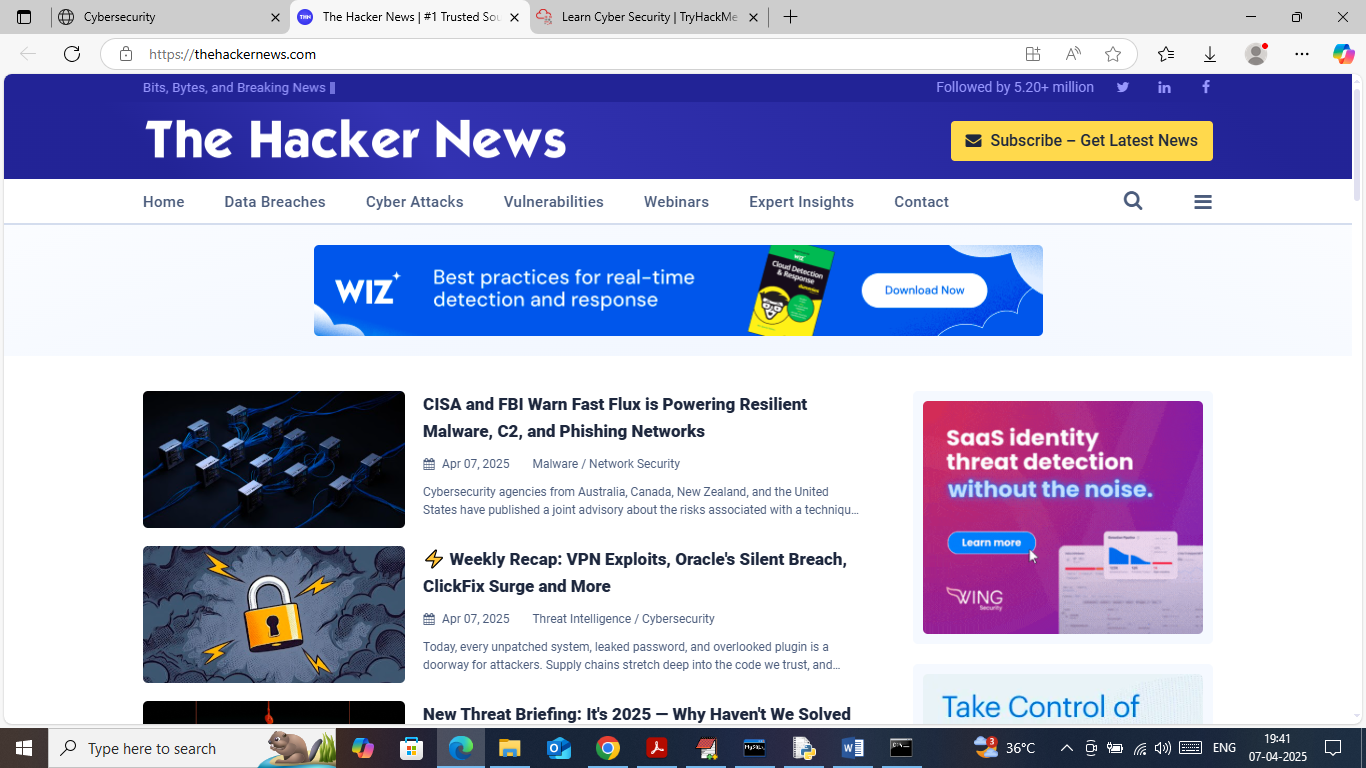
In above screen can see all uploaded files along with Hashcode and encryption type as ‘Steganography or Hybrid’. If encryption type ‘Steganography’ then system will display image along with ‘Extracted hidden message in blue text’. If encryption type is ‘Hybrid Encryption’ then user can click on red ‘Download’ link download file in decrypted format



In above screen can see file is downloaded in decrypted format and can see decrypted text. Similarly you can upload and download any number of files and now click on ‘Learning Tools’ link to learn about tools



In above screen can learn about tools and now click on ‘News Updates’ to get below page



In above screen user can read latest news on Cybersecurity.

So by using above applications you can secured data with Steganography and Hybrid encryption.