An Improved Authentication Scheme for Remote Data Access and Sharing Over Cloud Storage in Cyber-Physical-Social-Systems

Now-a-days all social networking organizations or any other organizations are using cloud services to manage and store their data as this services offer resources at a very cheap cost but this advantage often suffers from data security and to provide data privacy and security some public or private cloud offer data encryption but this is not sufficient for complete data security and for authentication of share users. Below are the main points which describe security issues at solved in propose paper

1. User Anonymity: No existing technique offer anonymization of user identity information such as ‘username’ and cloud server can know the name of user and can record all activities and can raise internal security attack (means cloud server employees can see the username and his activities). To avoid this problem author applying anonymity on user identity such as username which means username will be hashed or encrypted so nobody can identify id of user.
2. User or Cloud Impersonation Attack: when data owner or share data user request for any file then cloud server can log all this information and later can use this information to access or steal data and to avoid this problem author us maintaining or creating session once after login and once after logout then session will be closed so cloud server cannot steal information.

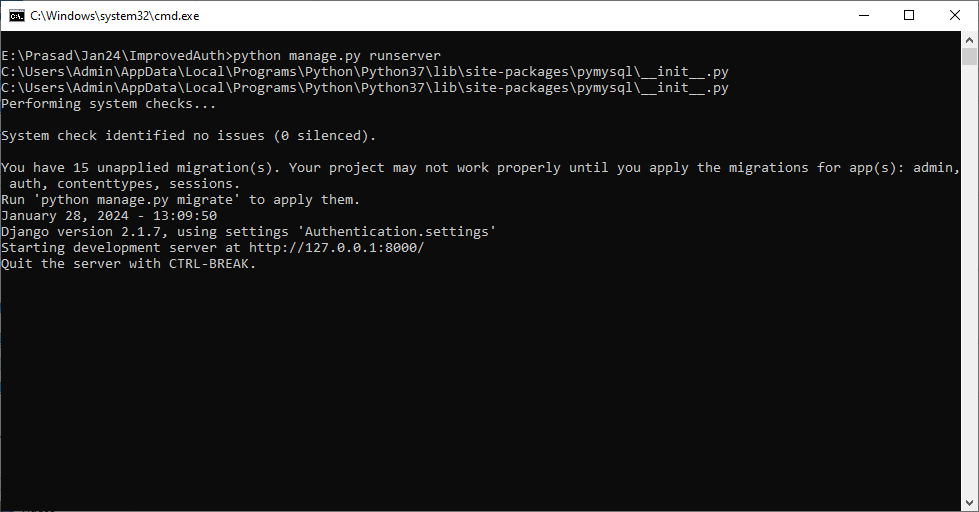
Above 2 points are the main contribution of the paper and whenever data owner or user access cloud server then following modules get executed

1. User Registration: In this module user has to register himself with cloud by giving username, password and biometric details and then application will hashed username to provide anonymity to user identity and then biometric image will also be hashed and saved in database
2. User Login/Verification: In this module data owner or mobile user will enter username, password and biometric image and then cloud will verify all details and upon valid login will server access to data page.
3. Upload File: Data owner can upload encrypted file by applying ECC (Elliptic Curve Cryptography) and then this file will be shared with any other user who has valid login details and cloud server will re-encrypt data and send to share user and then valid user can decrypt it. Here we are employing CHACHA as extension encryption algorithm which is more than 50% lighter than ECC
4. Change Password: Data owner or mobile user can send request to cloud for password change
5. Download Own/Share File: owner or user can download data after verification and then can decrypt and access data.
6. Computation Graph: using this module we will plot comparison between propose ECC computation time and extension CHACHA computation time

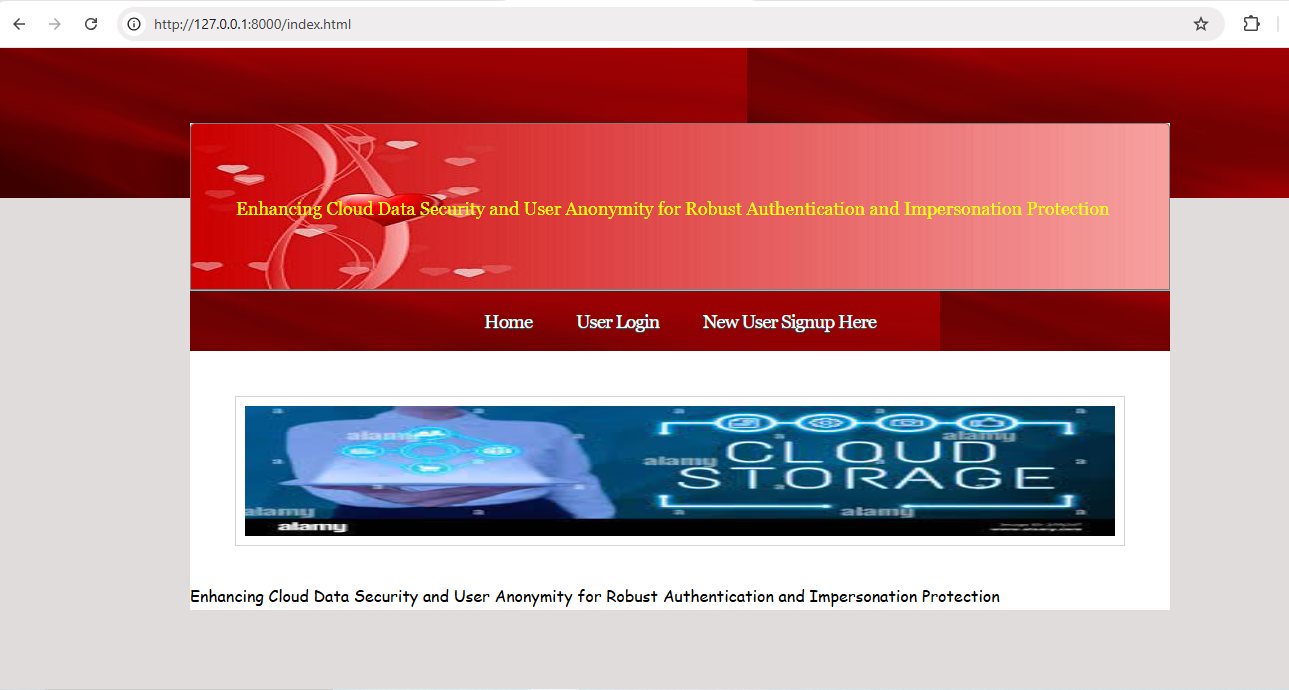
To run project first create database in MYSQL by copying content from ‘db.txt’ file and then paste in MYSQL

SCREEN SHOTS

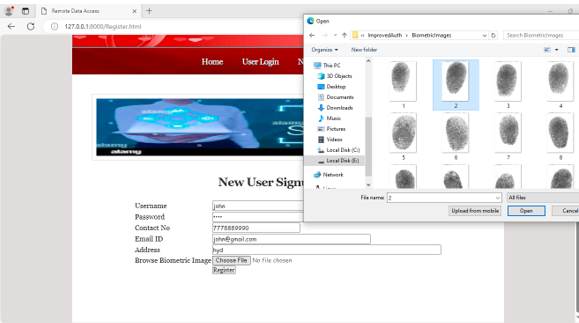
To run project double click on ‘run.bat’ file from to start python Cloud server and get below page



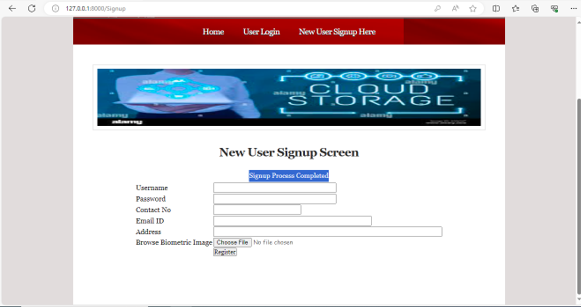
In above screen python server started and now open browser and enter URL as <http://127.0.0.1:8000/index.html> and press enter key to get below page



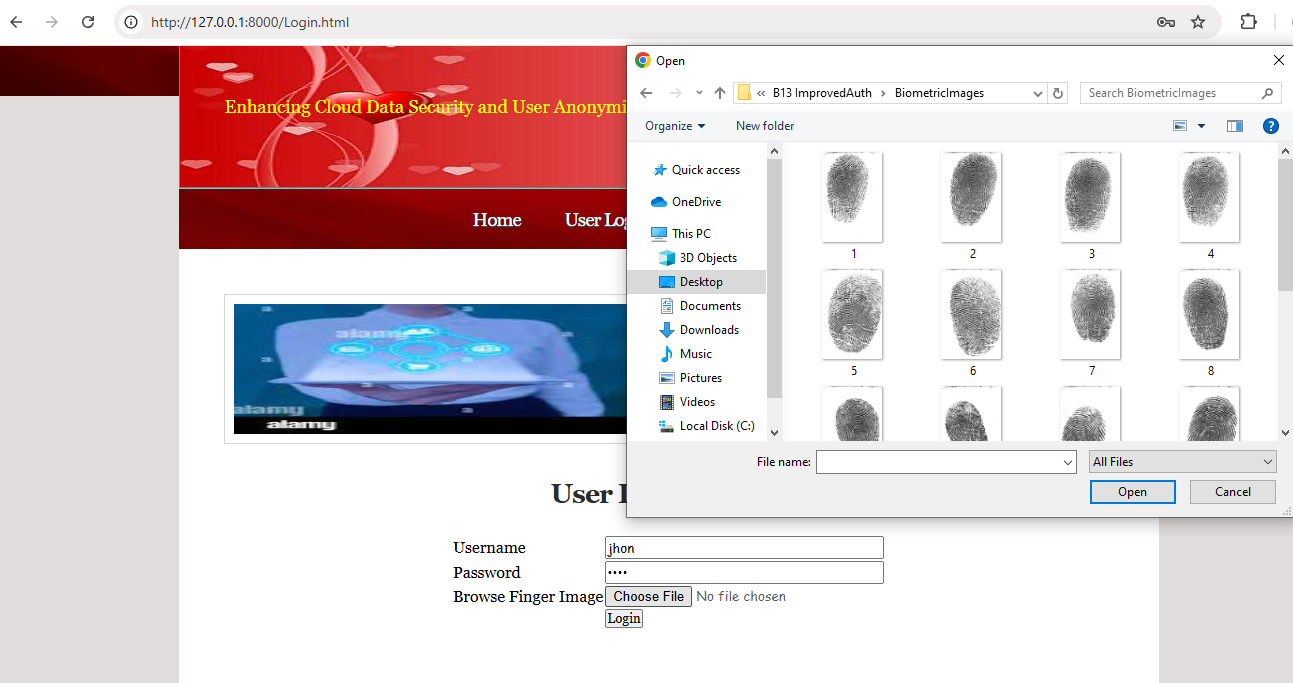
In above screen click on ‘New User Signup Here’ link to get below signup page



In above screen user entering signup details and then uploading user biometric image and then click on ‘Register’ button to get below page



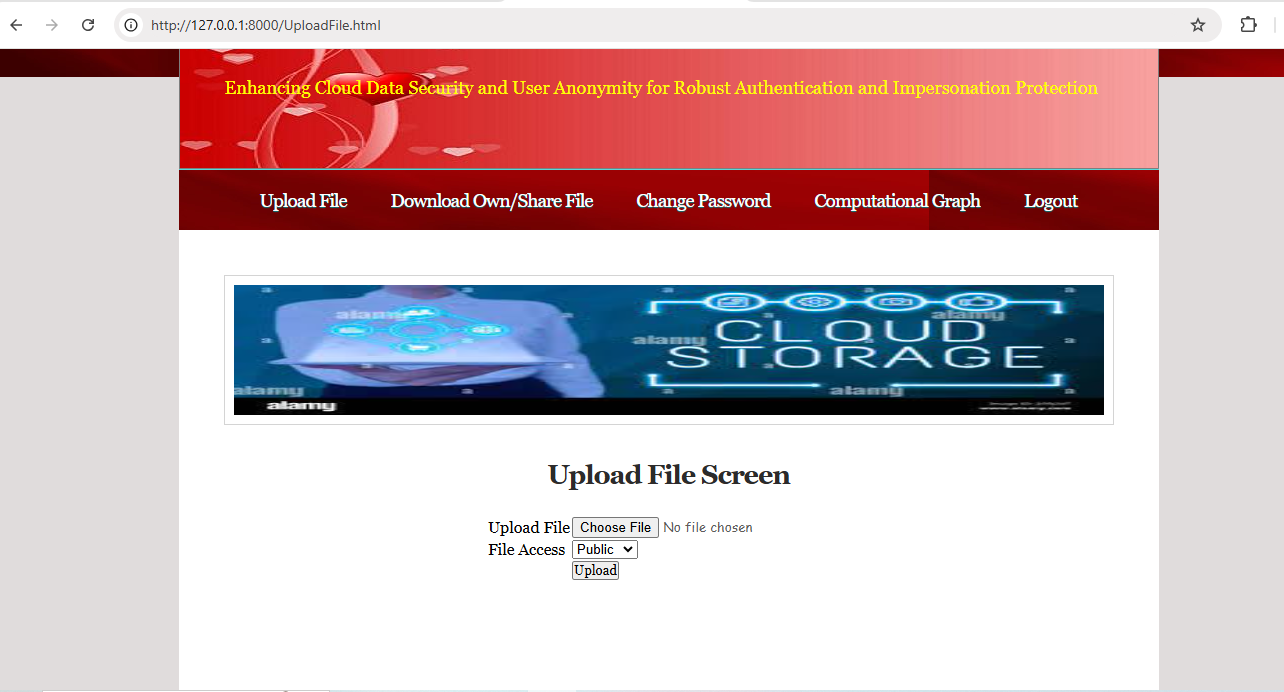
In above screen user sign up completed and now click on ‘User Login’ link to get below page



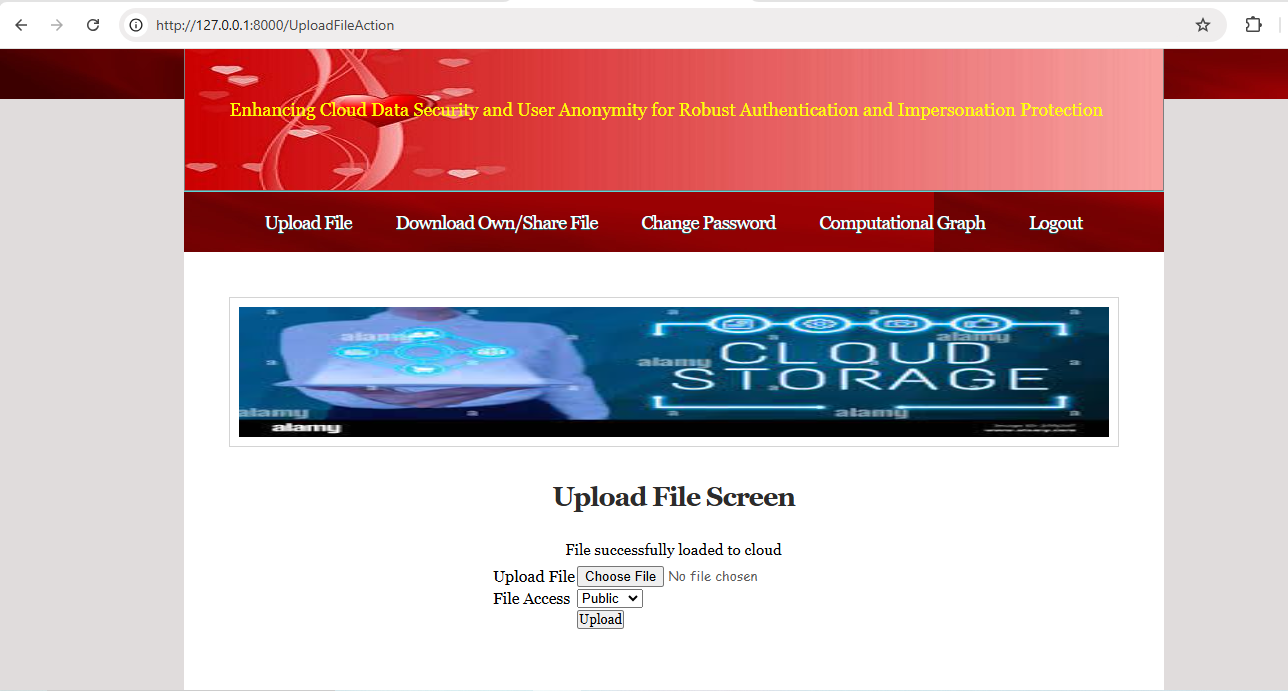
In above screen user is entering login details and then uploading biometric image and then press buttons to get below page



User will get above page after successful login and by clicking on ‘Upload File’ link he can upload files like below page



In above screen selecting and uploading file and then click on ‘Open’ button to save file in encrypted format and get below page



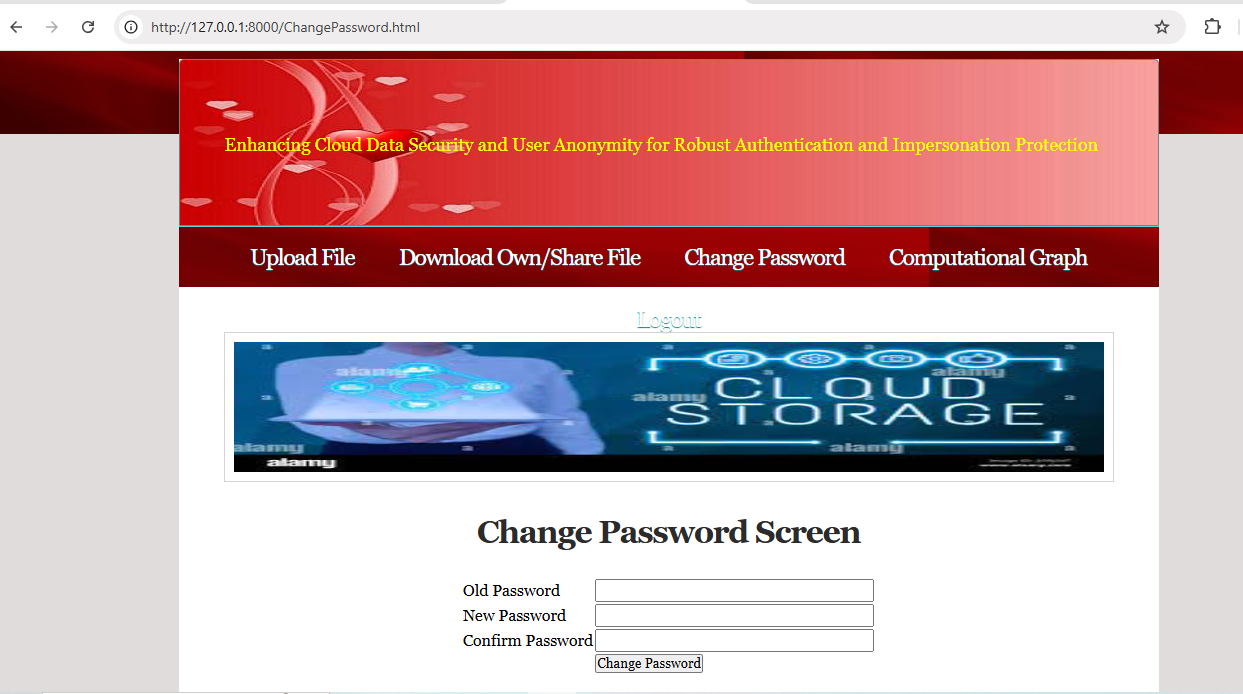
In above screen can see file saved in cloud and in below screen can see file is in encrypted format



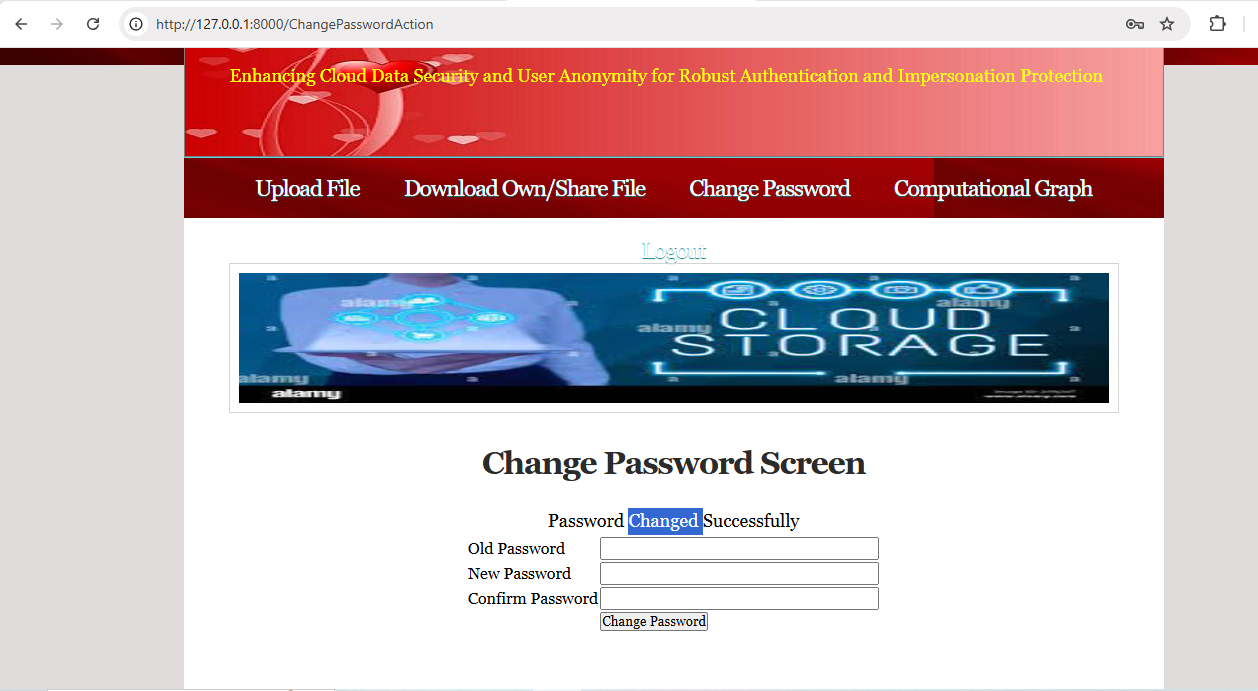
In above screen user can view files from all data owners and can click on ‘Click Here’ link to download file and will get below page



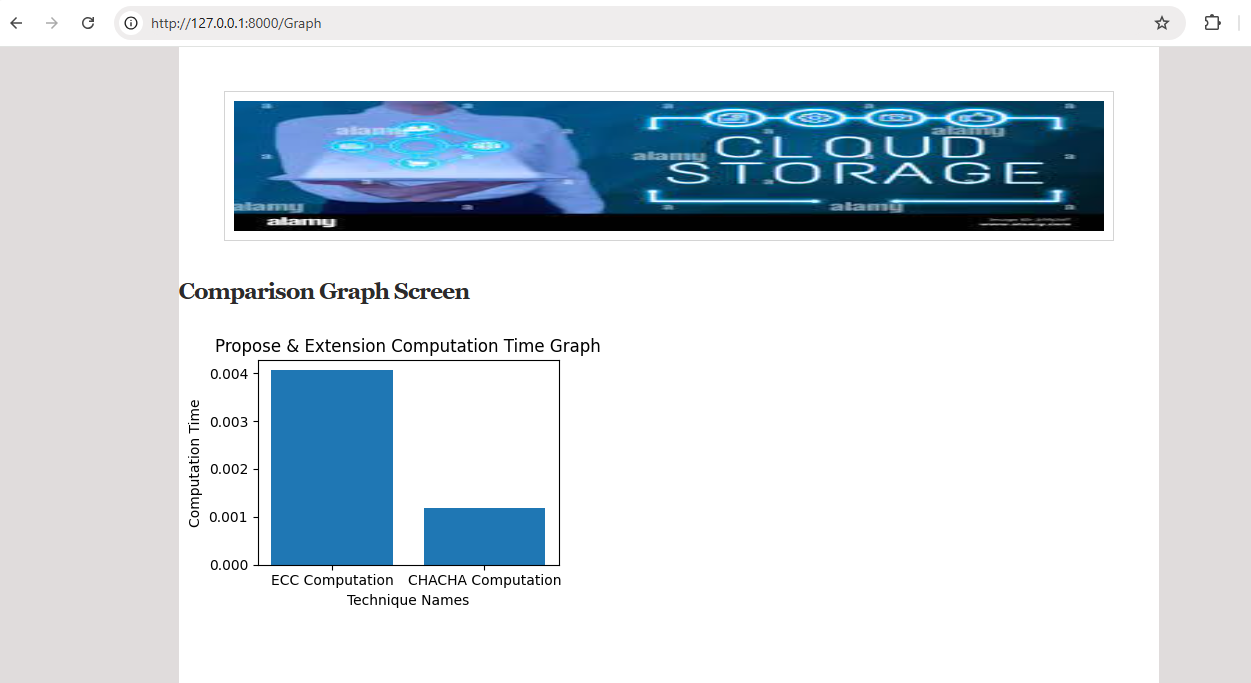
In above screen in browser top panel can see file is downloaded in decrypted format and now click on ‘Change password’ link to change password



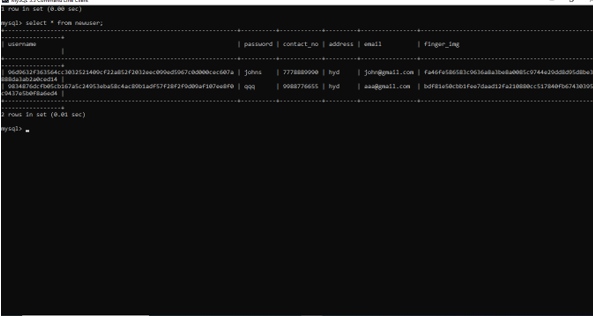
In above screen user will use this module to update passwords and then click button to get below page



In above screen password changed successfully and now click on ‘Computation Graph’ button to get below page



In above graph x-axis represents algorithm names and y-axis represents computation time and in both algorithms extension CHACHA took less computation time.



In above database screen can all finger images and usernames are anonymized to provide security to user details from cloud.