Honey Cloud: A Honeypot Network Approach for Enhanced Security to the Cloud

In this project we are developing Honeypot server to detect and prevent attacks. Honeypot is an additional server which sit between user and cloud server and whenever any user send request then Honeypot will intercept that request and authenticate user and his request and if user authenticated then it allow user to access cloud server and if user is not authenticated and send request with fake password then Honeypot will monitor all his activity and serve him fake responses and the attacker with think he successfully attack server and keep sending malicious activities and Honeypot will record all his activity and later admin will block such IP address or instruct server from serving such IP Address.

In propose work designing Honeypot server which accept user request to upload, download and share file. While sharing file users will gave sharing permission and password to genuine users and then shared users can give password to download file. If any malicious user try to download file with fake password then Honeypot server will serve him blank page.

In propose paper if we serve blank page to attacker then he will easily understand that Honeypot serving him empty response then he will stop doing further activity and Honeypot cannot extract more information him and to avoid this problem in extension work instead of serving empty response Honeypot serve fake file which assure attacker that server has successfully hijack and he continue sending malicious activity which help Honeypot extract more information from him.

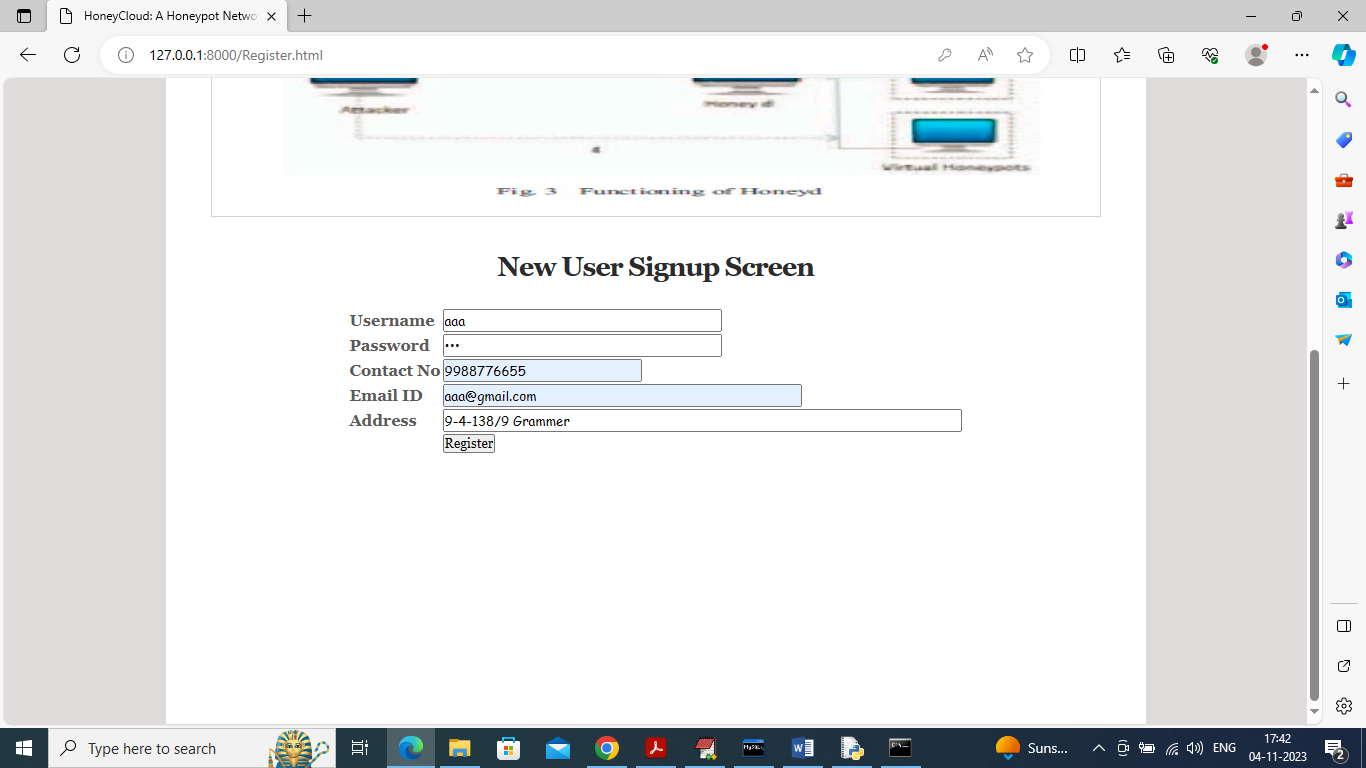
SCREEN SHOTS

To run project install MYSQL and then copy content from DB.txt file and then paste in MYSQL console to create database, install python 3.7 and then install all packages from requirements.txt file just by copying and pasting in command prompt.

After all packages installation double click on run.bat file to start DJANGO server and then open bowser and enter URL as <http://127.0.0.1:8000/index.html> and then press enter key to get below page



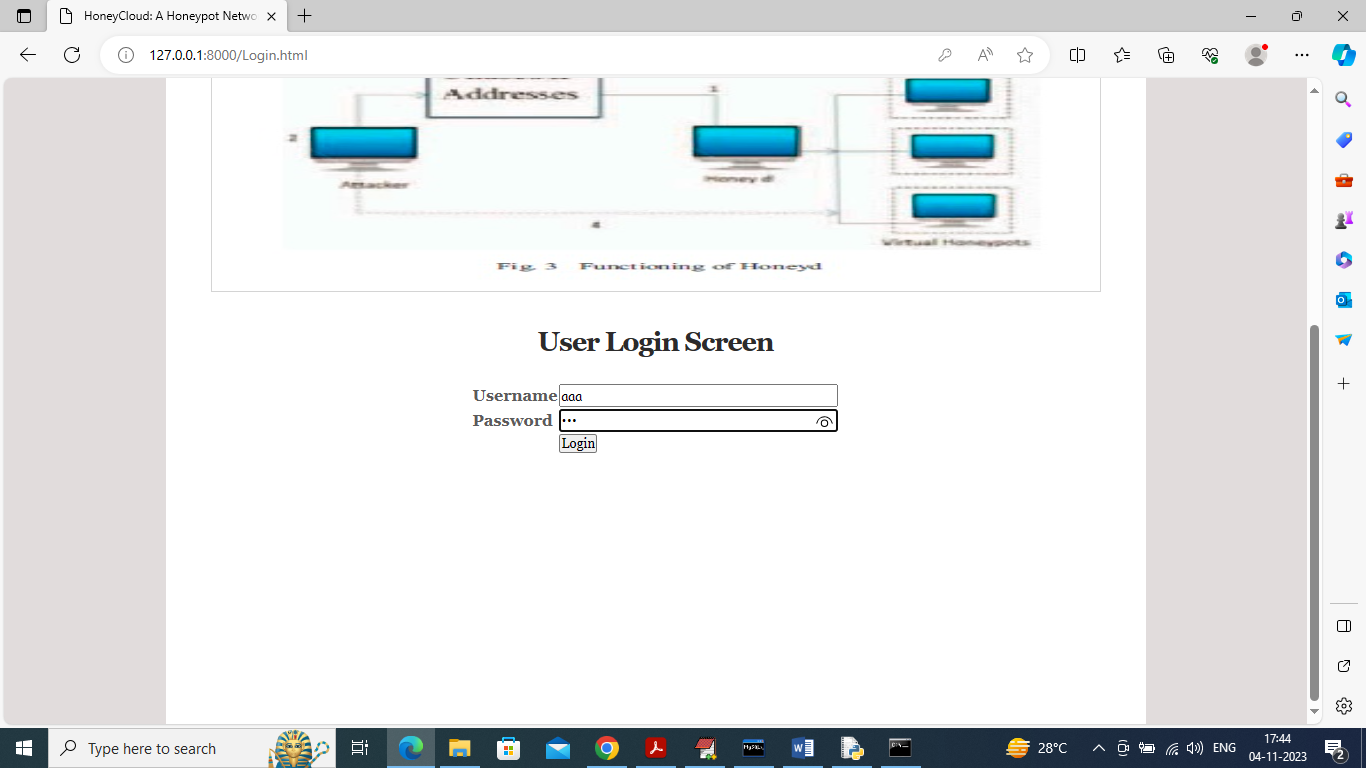
In above screen click on ‘Register Here’ link and register some users



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



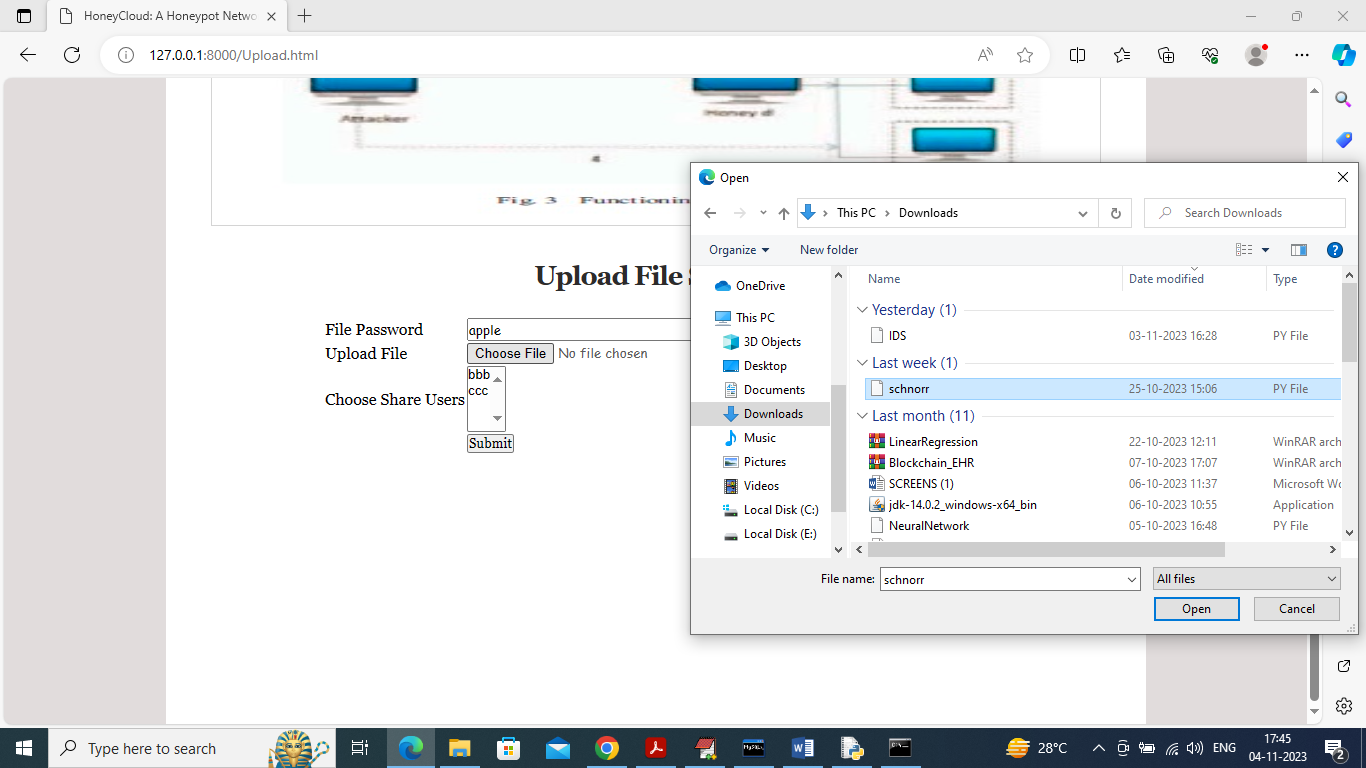
In above screen user signup process completed and similarly you can add many more users and now click on ‘Login’ link to get below login screen



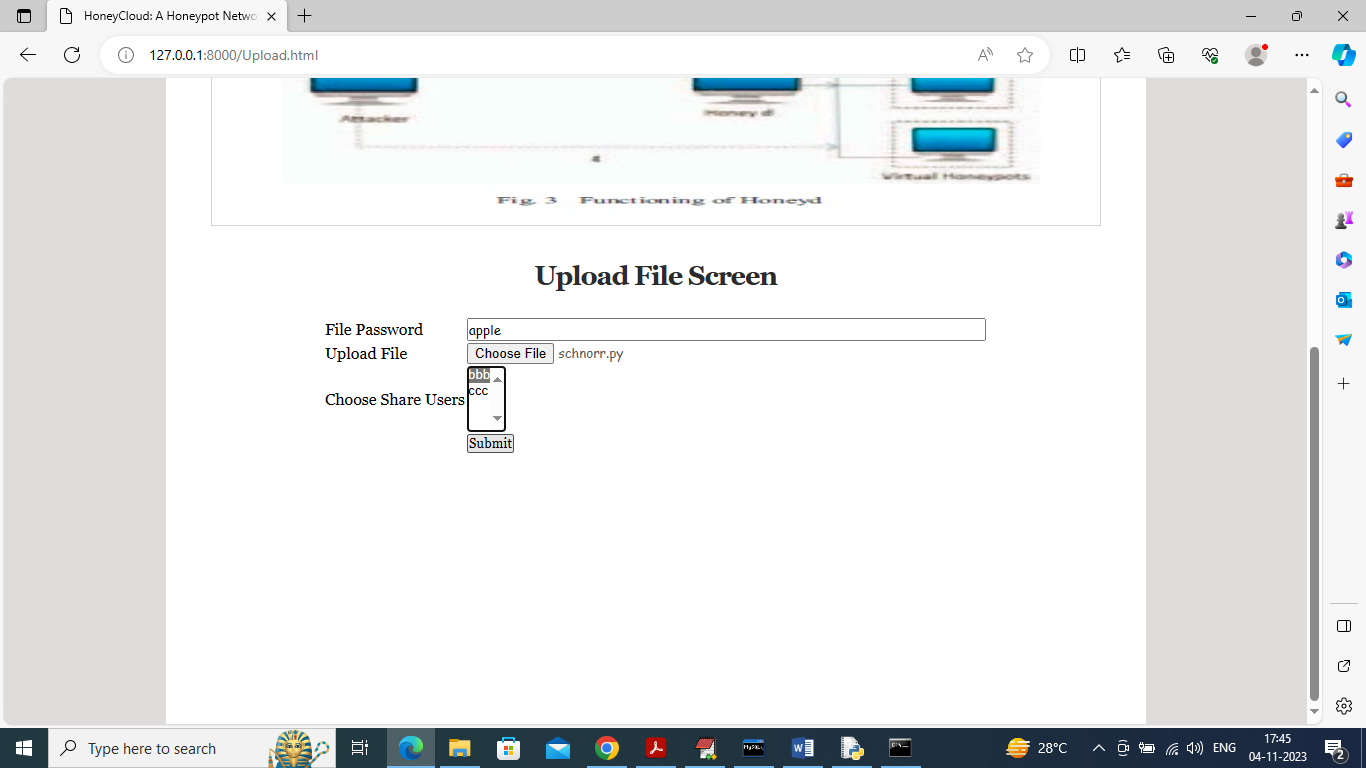
In above screen user ‘aaa’ is logged in and after login will get below screen



In above screen now user can click on ‘Upload File’ link to upload files



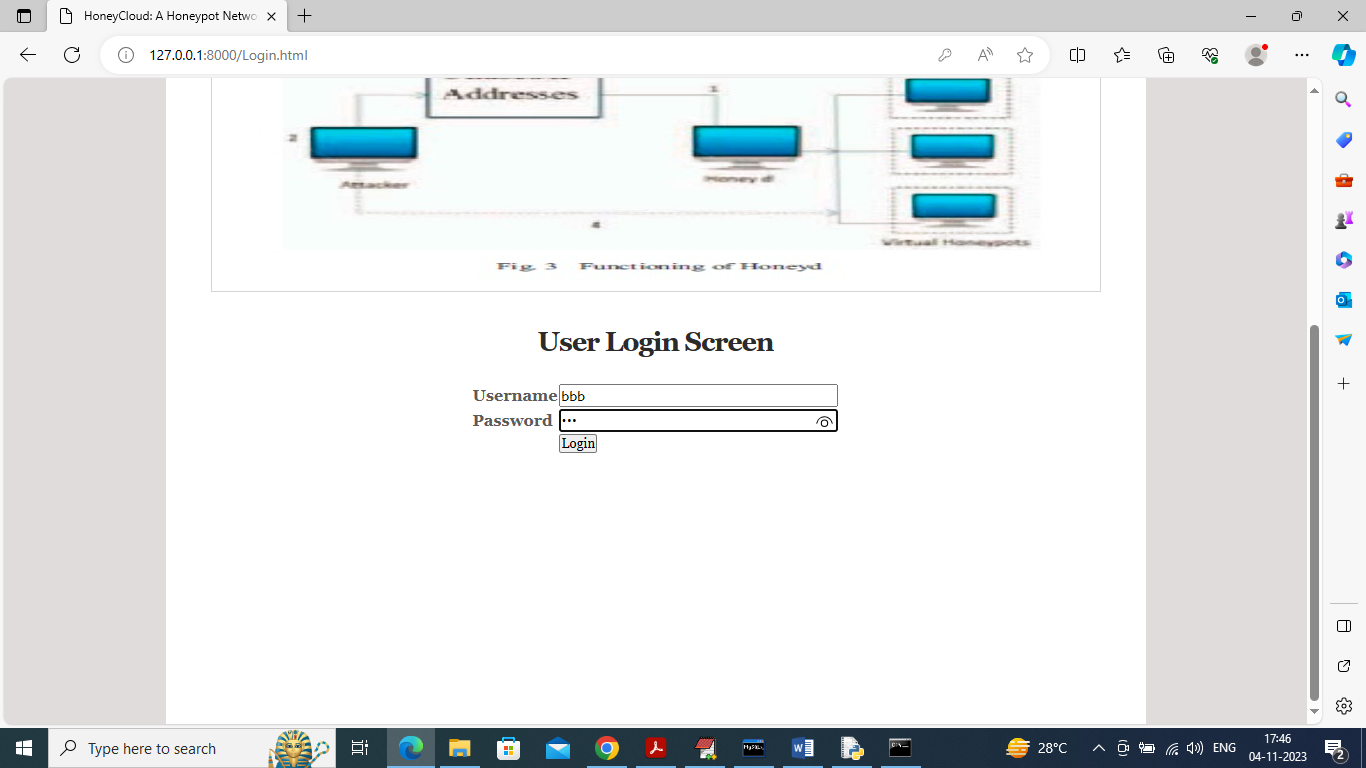
In above screen in first field we need to enter file password and then click on ‘Choose File’ button to select any file and then select require users with whom you want to share file and you can select multiple users by holding CTRL key from keyboard



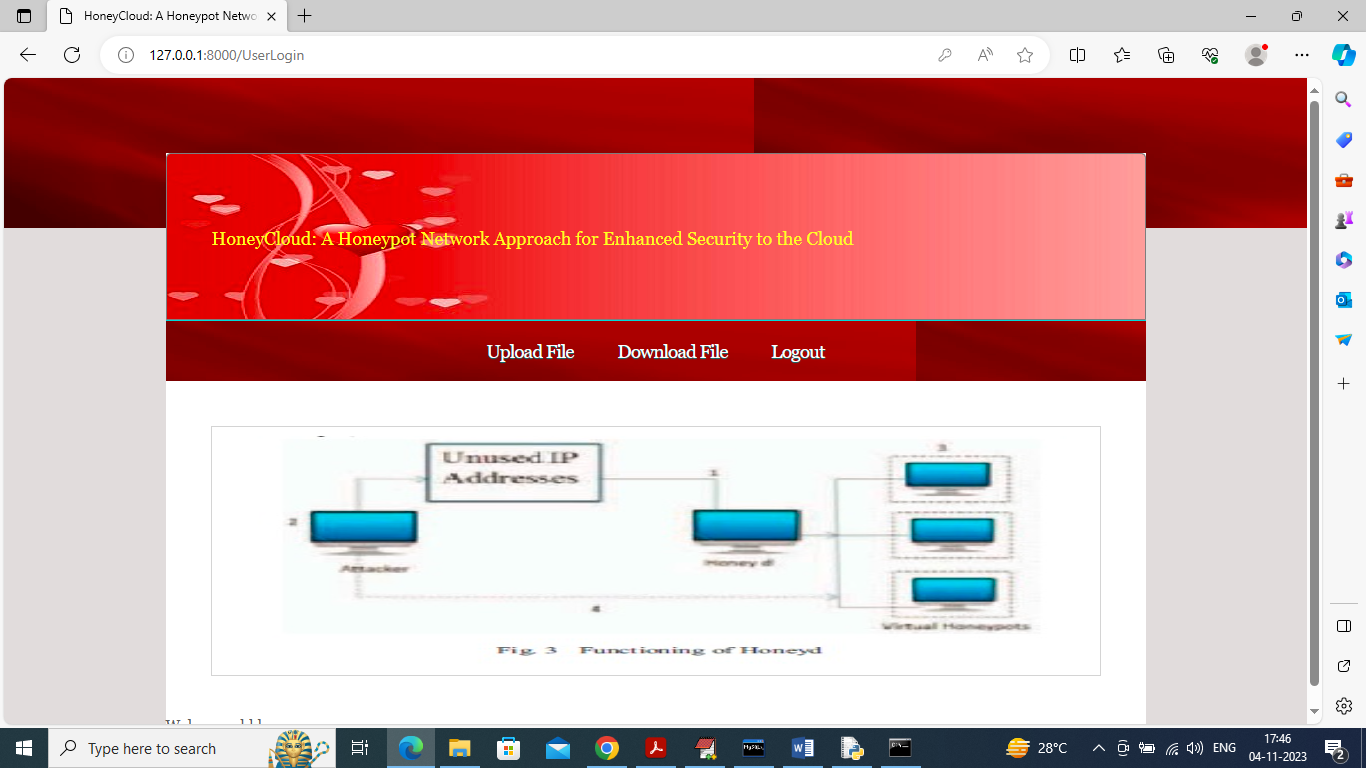
In above screen user aaa is sharing file with bbb and now click on ‘Submit’ button to upload file



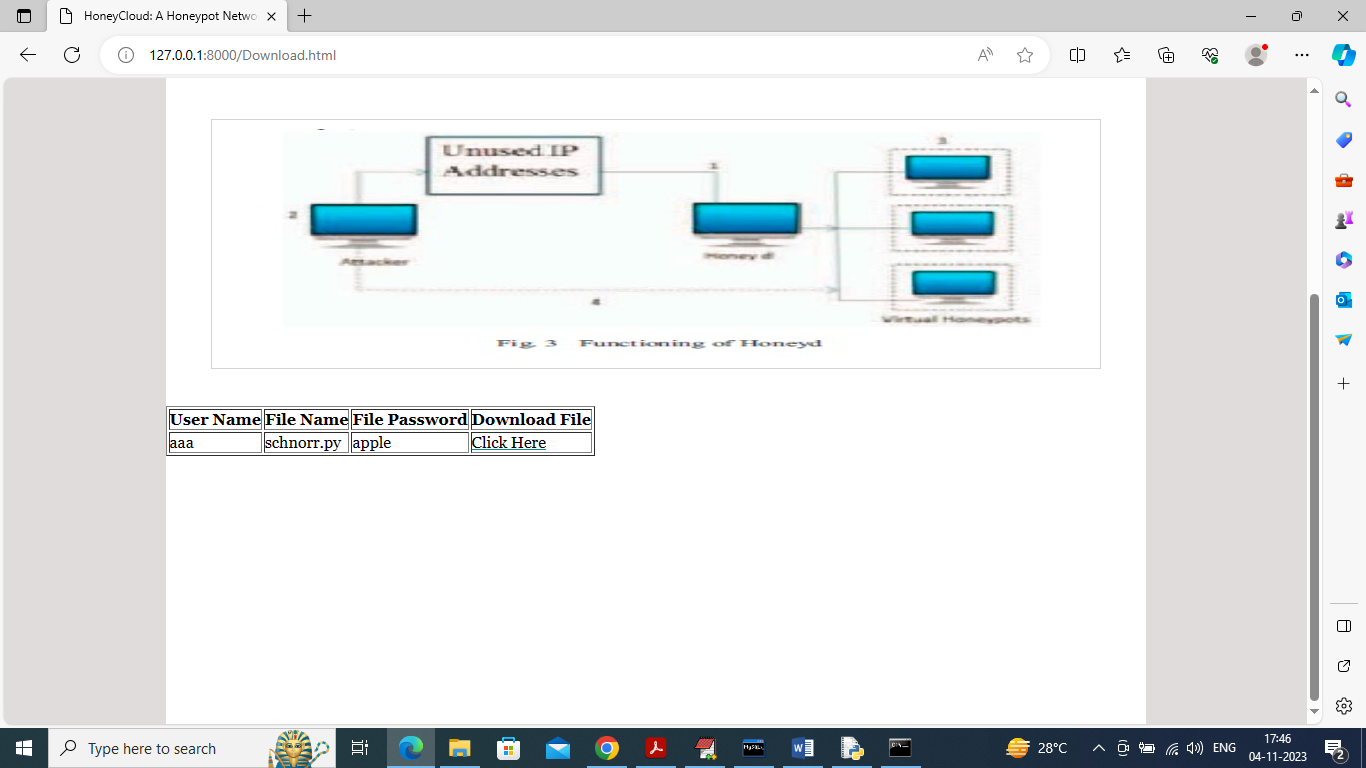
In above screen in blue colour text can see file is uploaded and now logout and login as user bbb to download file



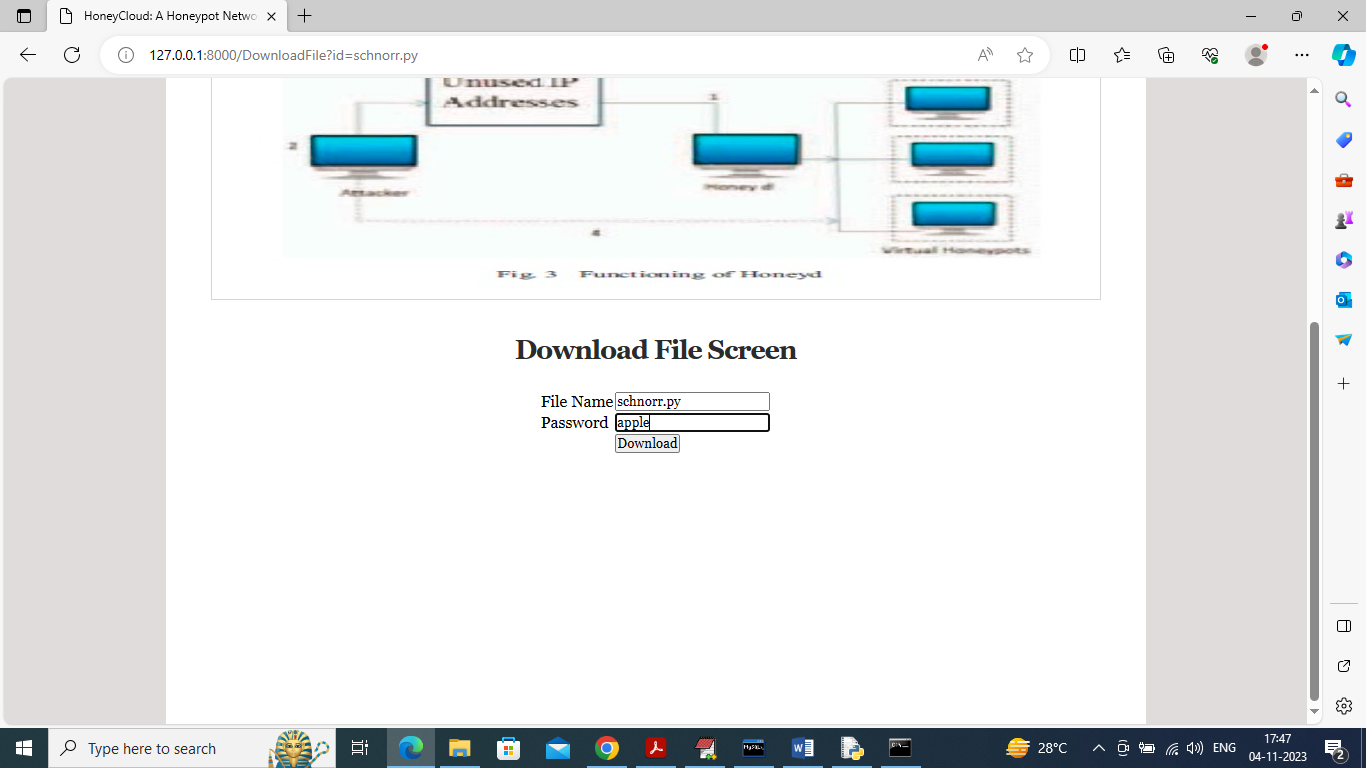
In above screen user bbb is login and after login will get below screen



In above screen now click on ‘Download File’ link to get below screen



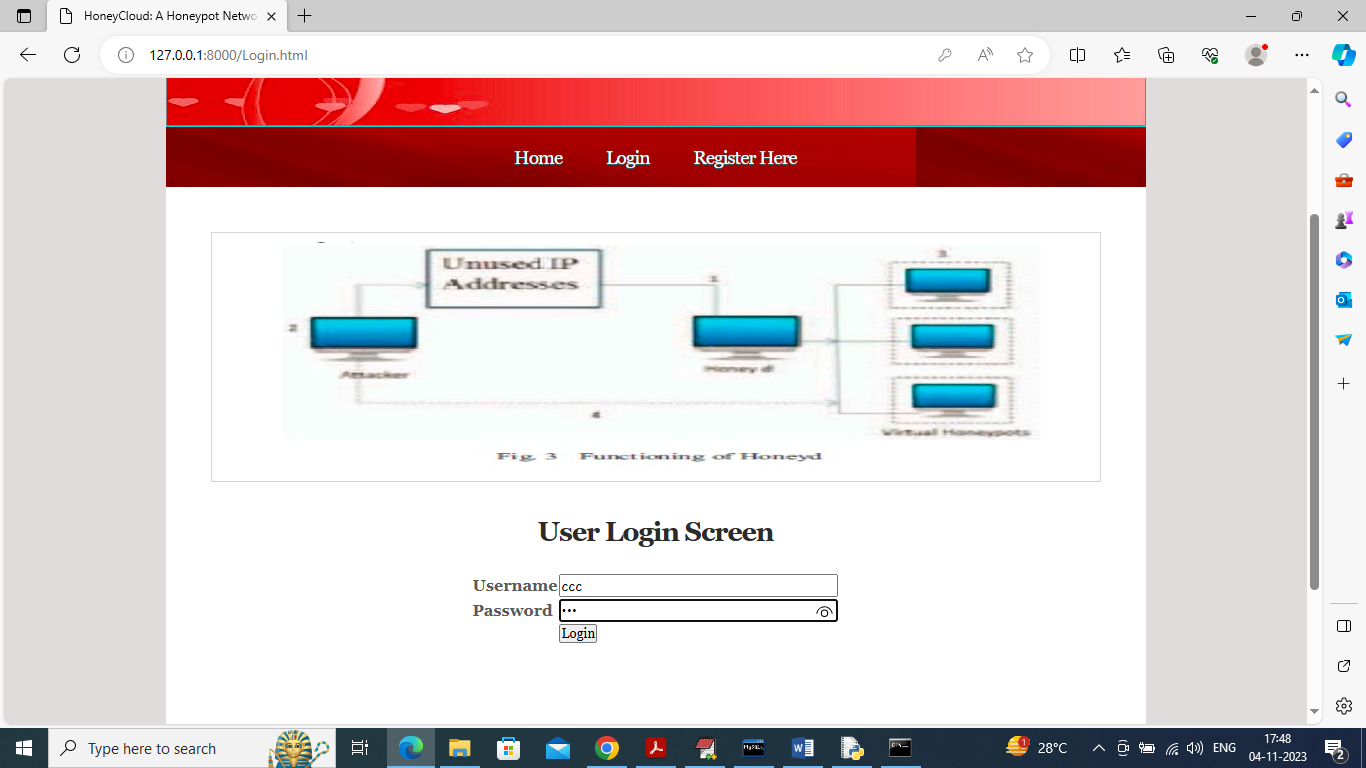
In above screen bbb user can see all files list shared by other user and password of file also will be visible to him as user aaa has given share permission to him. now any time bbb user can click on ‘Click Here’ link to download file and to get below screen



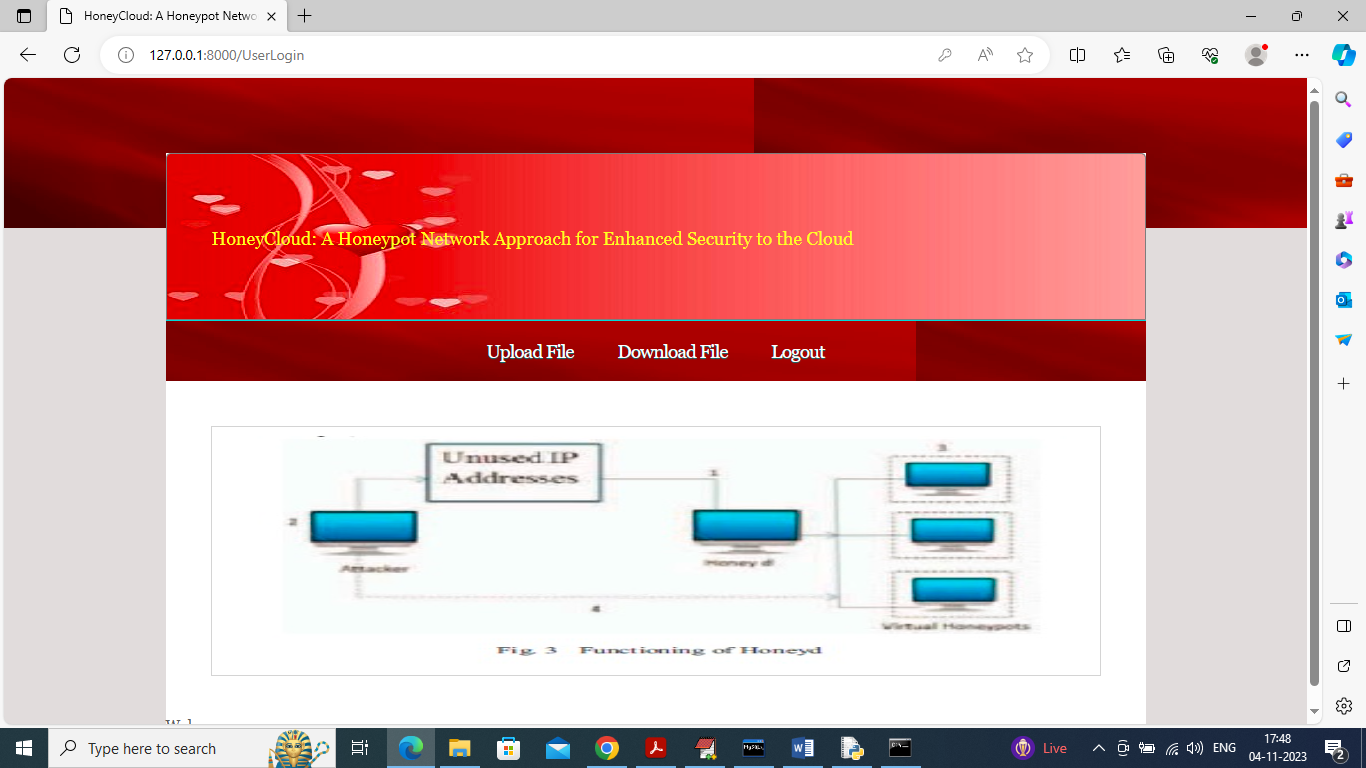
In above screen user bbb entered password as ‘apple’ and its correct password and file will be downloaded in browser status bar



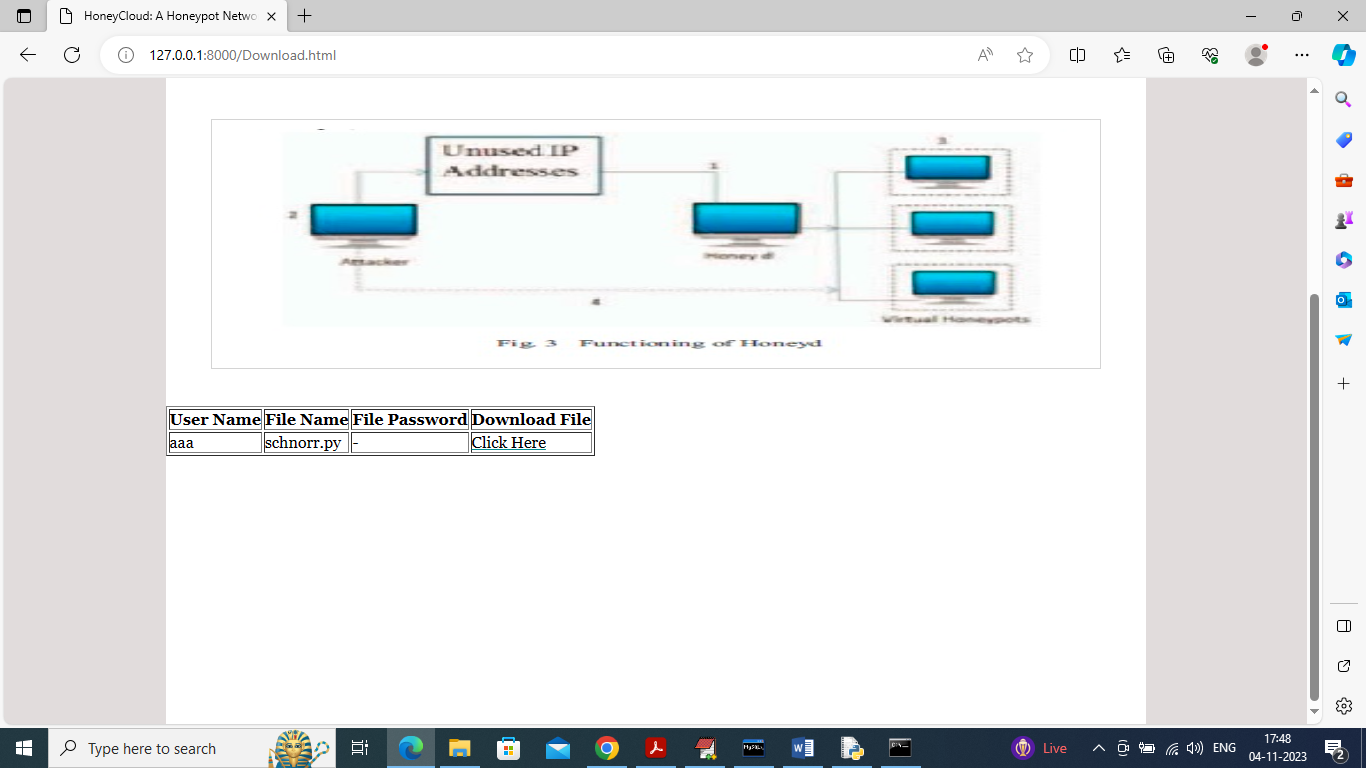
In above screen in top right side of browser file is downloaded and now logout and login as user ccc who don’t have share permission



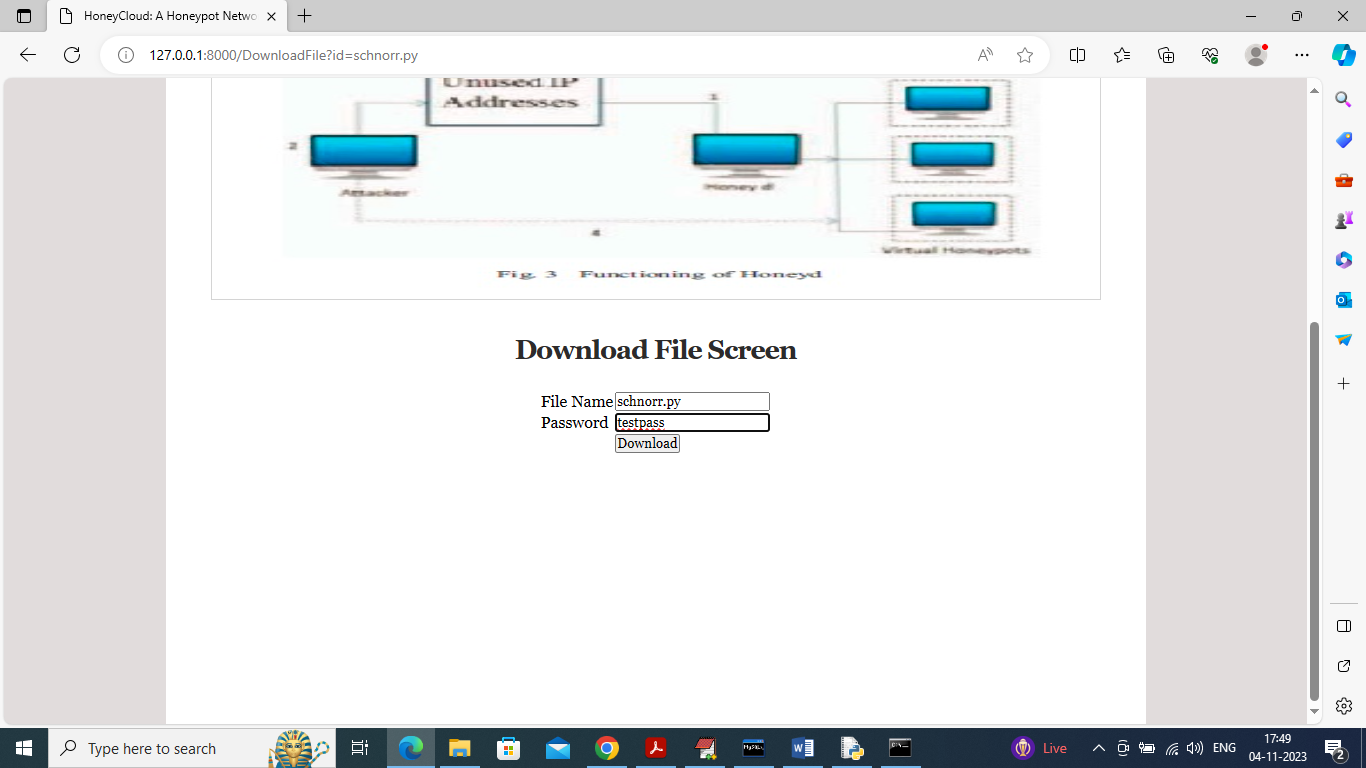
In above screen user ccc is login and after login will get below screen



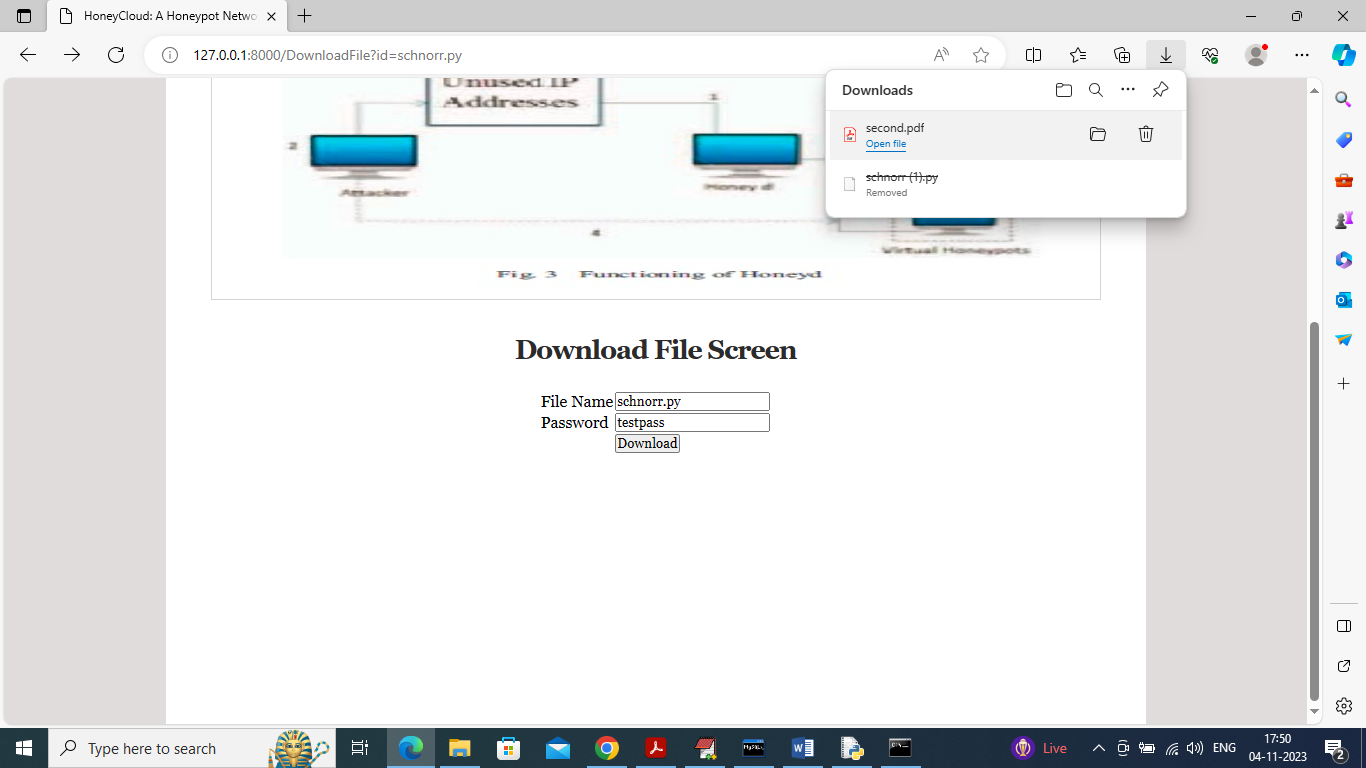
In above screen now user can click on ‘Download File’ link to get below screen of file list



In above screen ccc user also got file list but he don’t have share permission so file password is disabled and now if he want he try to download file with fake password and then Honeypot detect him and serve fake response



In above screen ccc user try to download file with fake password and then will get below response from Honeypot



In above screen in browser top right we can see Honeypot serve ccc user fake file called ‘second.pdf’ instead of original file ‘schnorr.py’. In the same way Honeypot serve fake response to gather information from attacker and then prevent all those attackers from getting access to genuine data