Decentralization and Security Issues in Blockchain Enabled Internet of Things

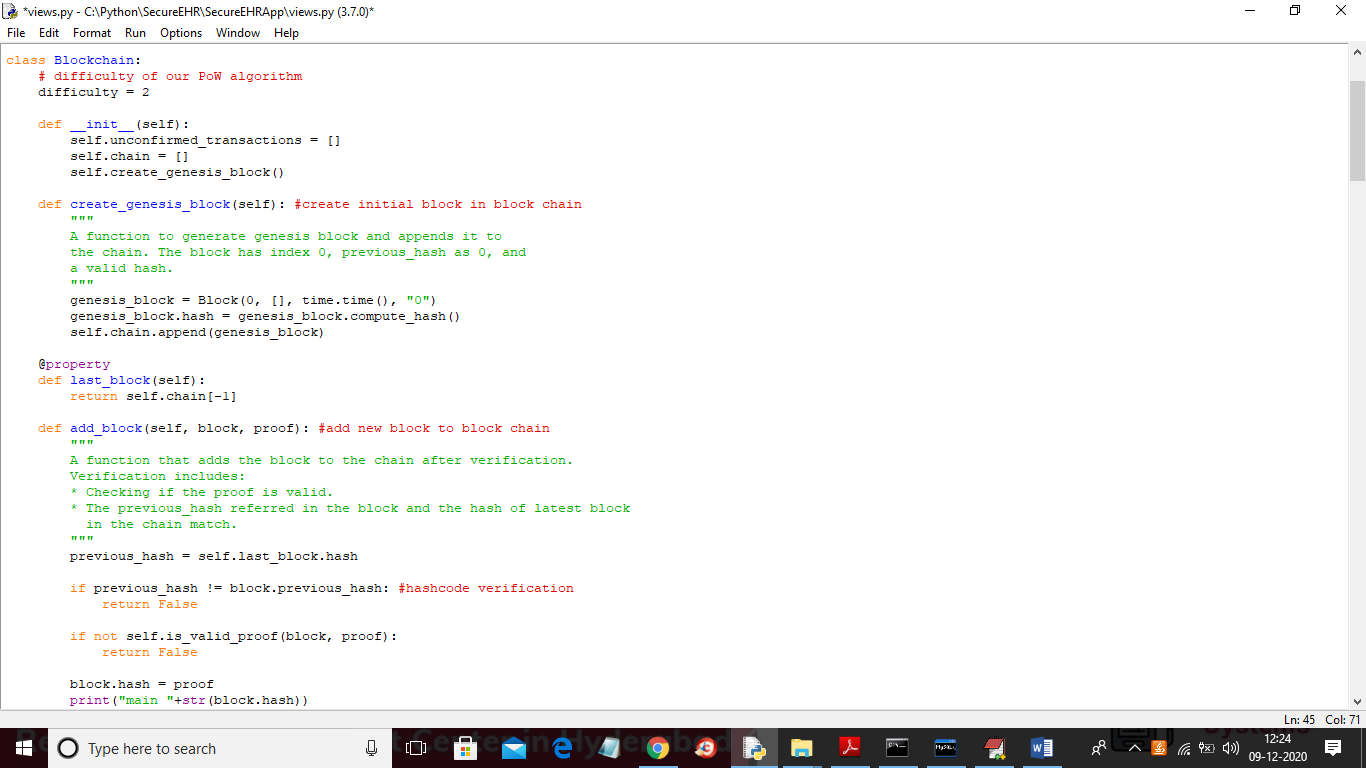
In this paper author is describing about security issues for patient health record stored in Decentralized (data will be maintained at multiple peer or systems) Blockchain server. Now-a-days patient data can be shared between multiple hospitals, insurances agencies, Government and lab. Due to sharing of data there will be data security issues raised for patient as this data can be misuse by agency peoples or attackers may steal this data. To overcome from this problem author is using Decentralized Blockchain server which maintain data as blocks of trees and at each transaction all previous hash code will be verified and if verification successful then data will be consider as intact and if data changes then Blockchain server will notify that system in under attack and it gather data from another working node.

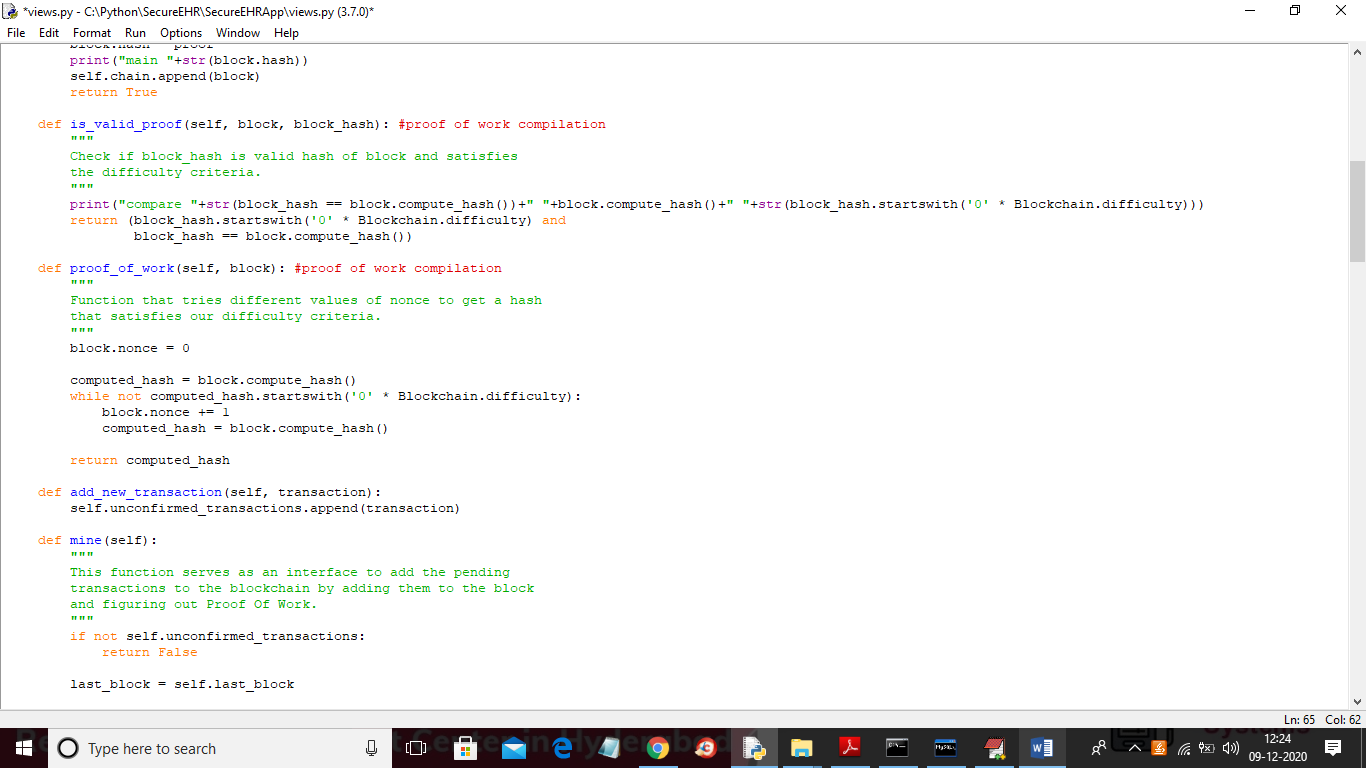
Due to this transaction hash code verification and immutable data storage make Blockchain secure and trustable in current market. To further secure data author is using encryption algorithms before storing data in Blockchain and author has describe many traditional and new encryption algorithms such as ABE, IBE, CPABE and many more. Python currently does not support ABE algorithm so I am using AES algorithm to encrypt patient data before storage.

This project can be run by following users

1. Users: This are patients who create their medical profiles and give permission access to Healthcare agents and this permission can be controlled by access control program to decide which users allowed to access patient data
2. Healthcare Agents: This can be doctors, insurance companies or government users and here government can access patient data to know how many peoples are suffering from which disease. Insurance companies can access this data to decide to give insurance policy to patients or not and doctors can access this data for treatment.
3. Cloud Storage: Here Blockchain encrypted data storage will be consider as cloud storage as we don’t have any cloud server so we are storing data in Blockchain server.

In propose paper author is gathering patient data from IOT sensors but we don’t have such sensors so we are entering patients records manually and then share with different users. See comments in below code screen shots to understand Blockchain working procedure

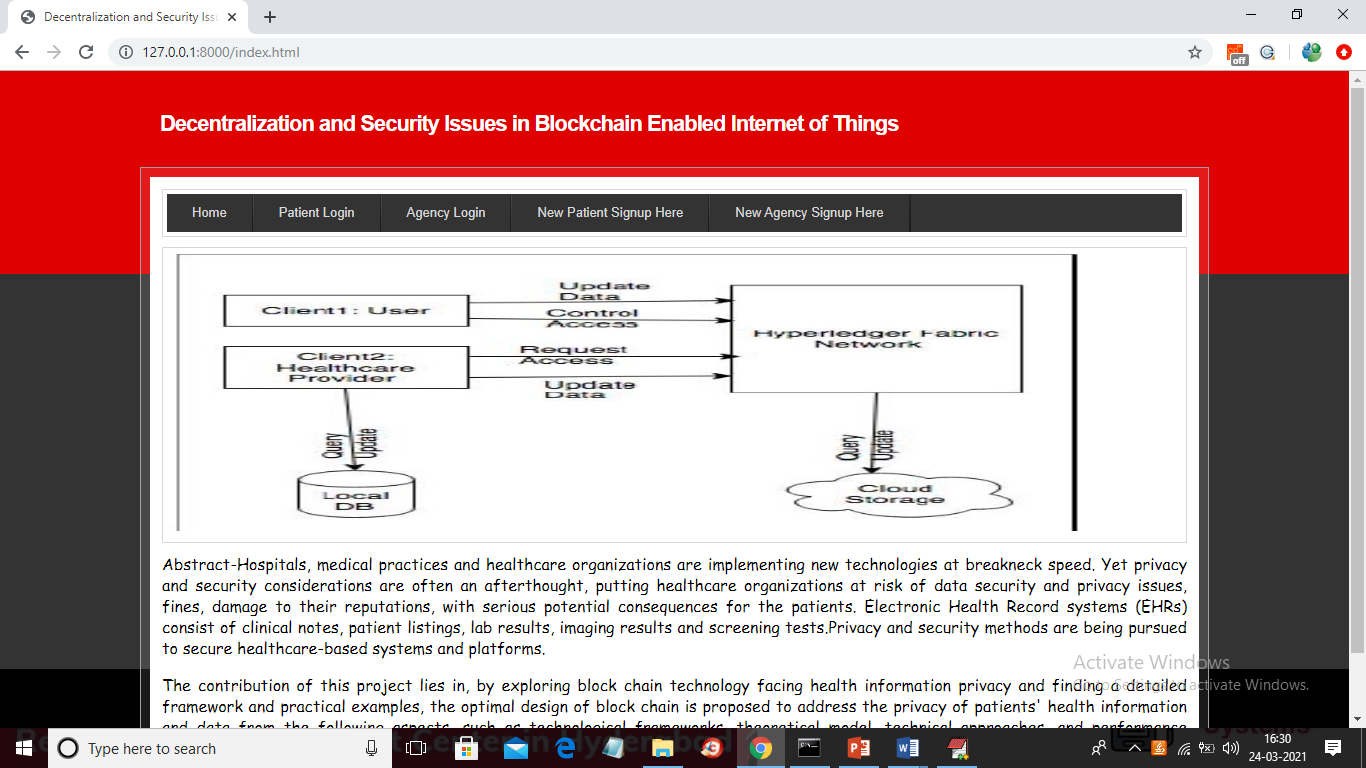




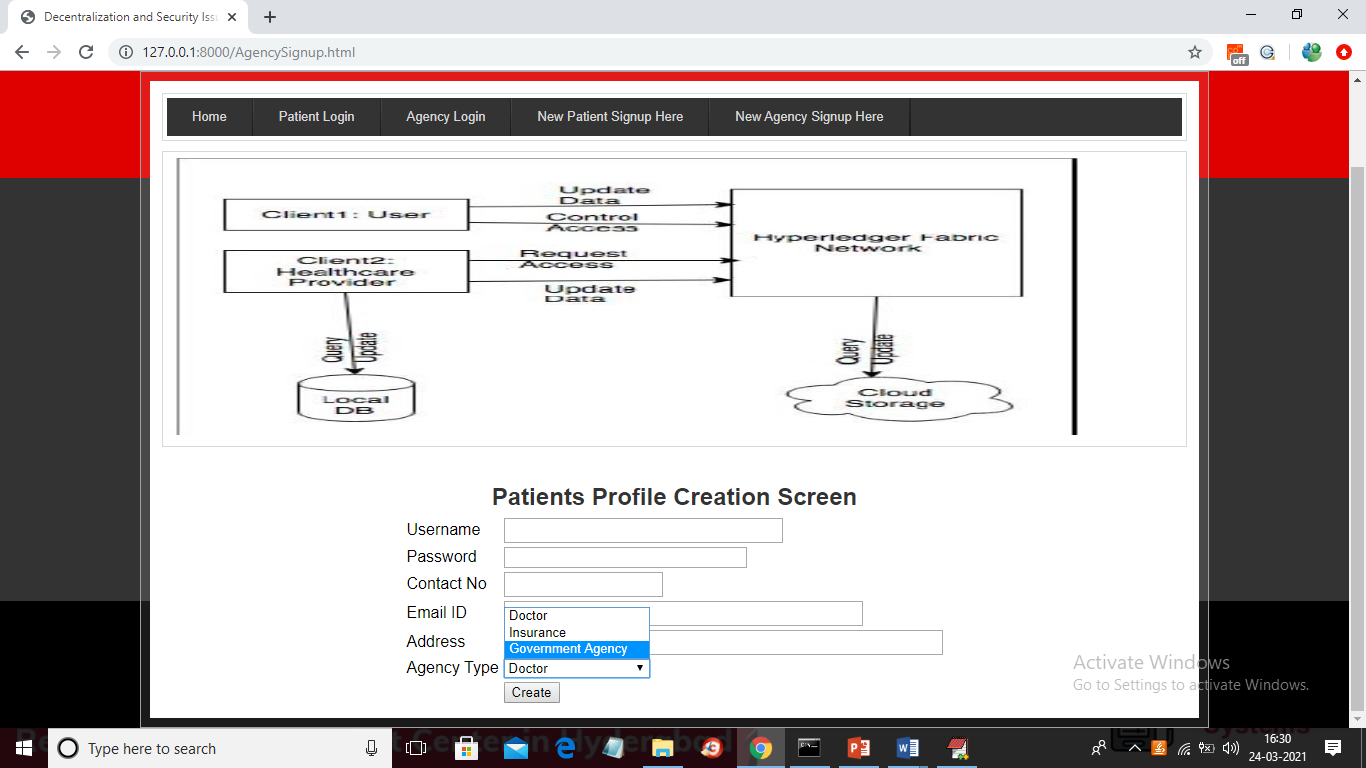
In above two screen read comments to understand block chain working procedure

SCREEN SHOTS

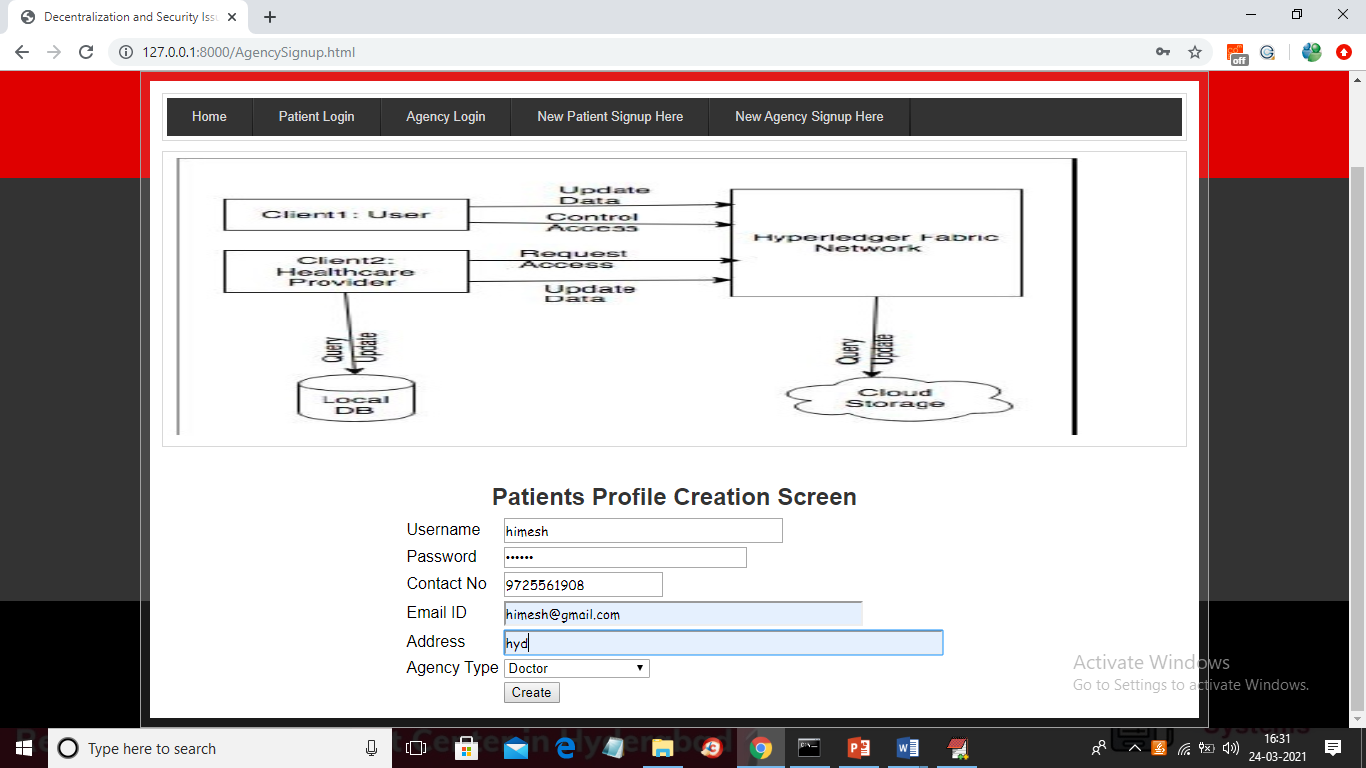
Deploy code in python DJANGO webserver and then open browser and enter URL as ‘http://127.0.0.1:8000/index.html and then press enter key to get below home page



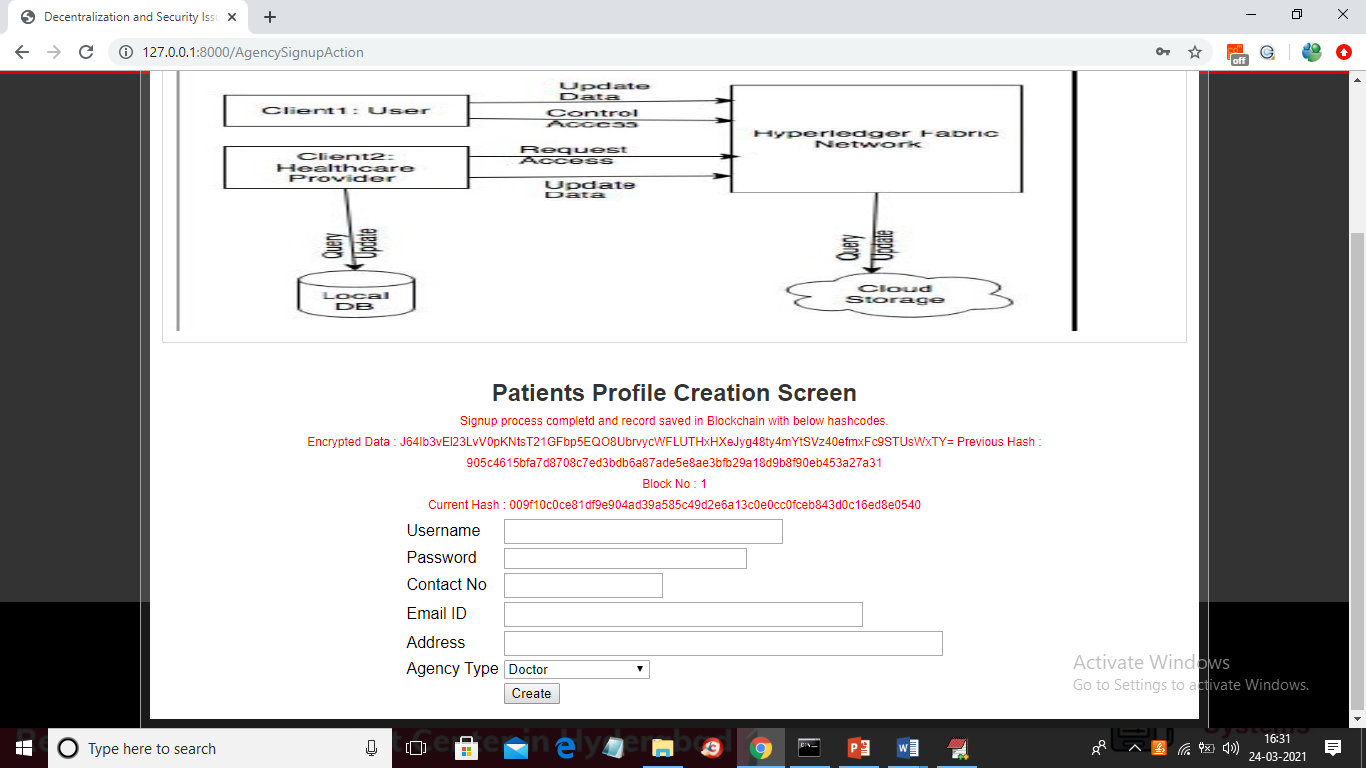
In above screen click on ‘New Agency Signup Here’ link to add new agency users such as doctors, government agencies or insurance companies.



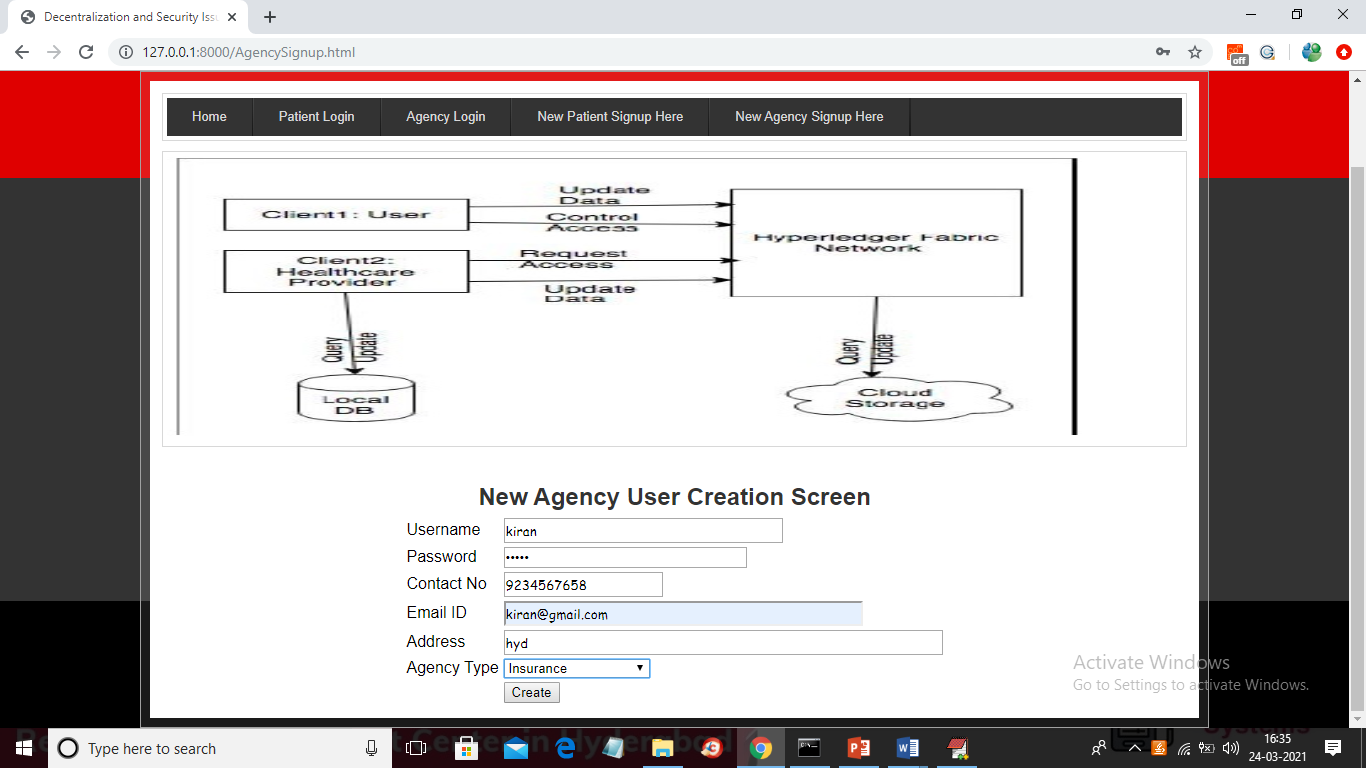
In above screen we can signup user with various types



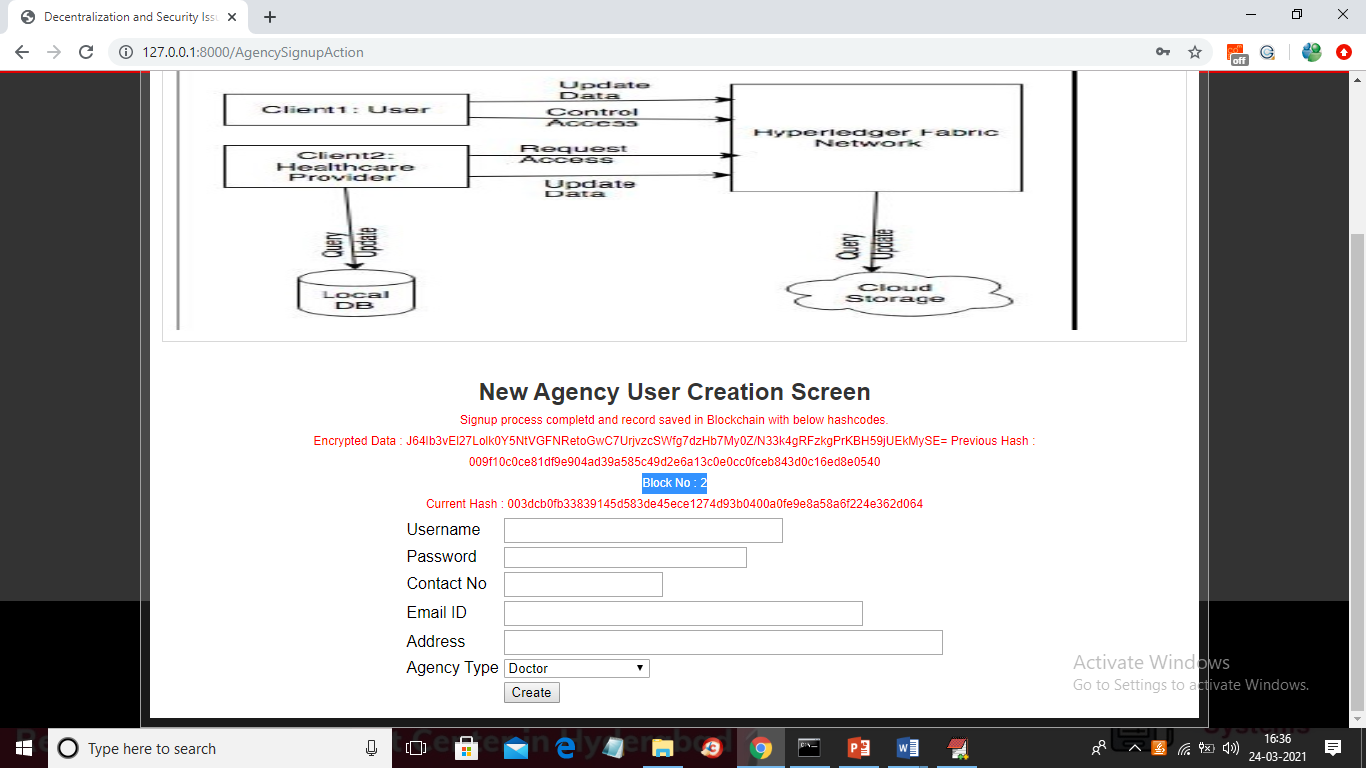
In above screen adding one user as doctor and after pressing button will get below screen



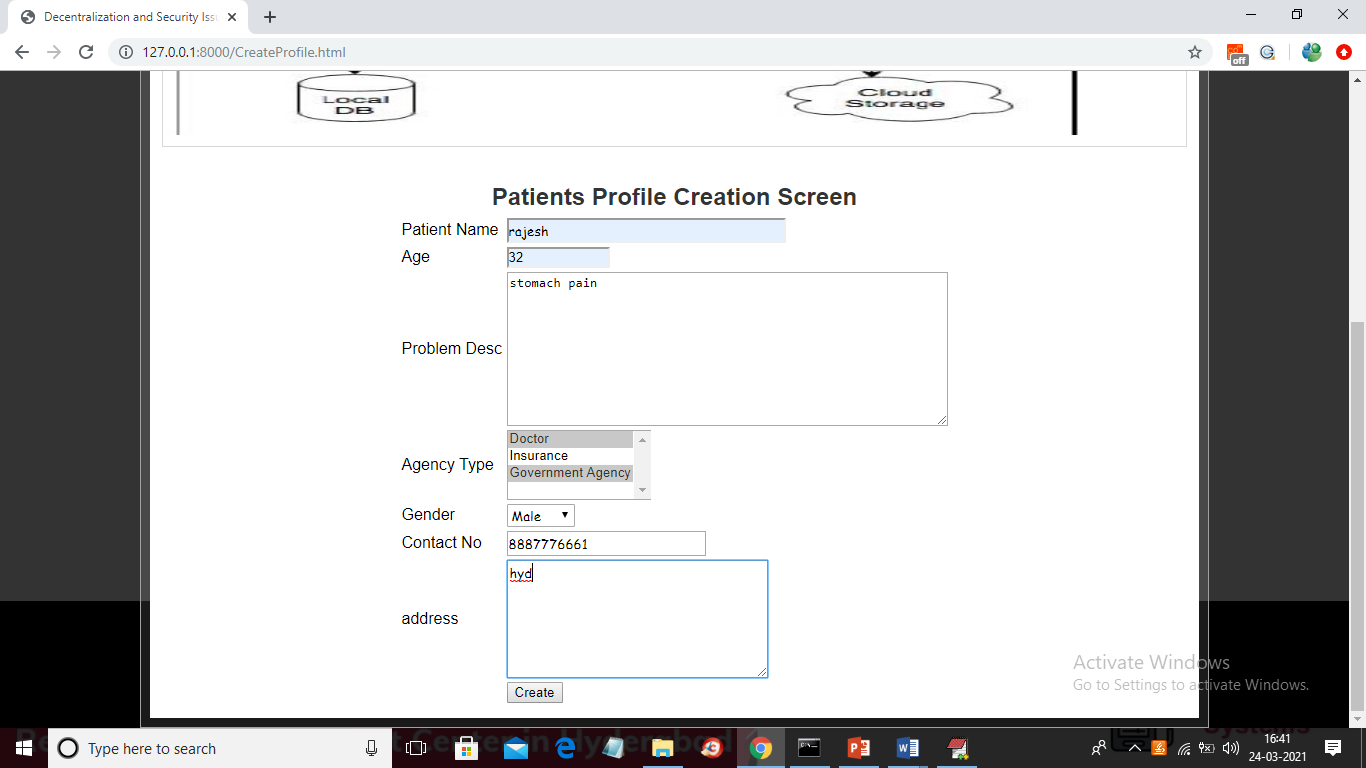
In above screen in red colour text we can see Blockchain response about record store with encrypted data, current hash, previous block hash code and block number. Blockchain maintain above all details in its storage and this store values will be available for life long. Similarly we can add another agency user



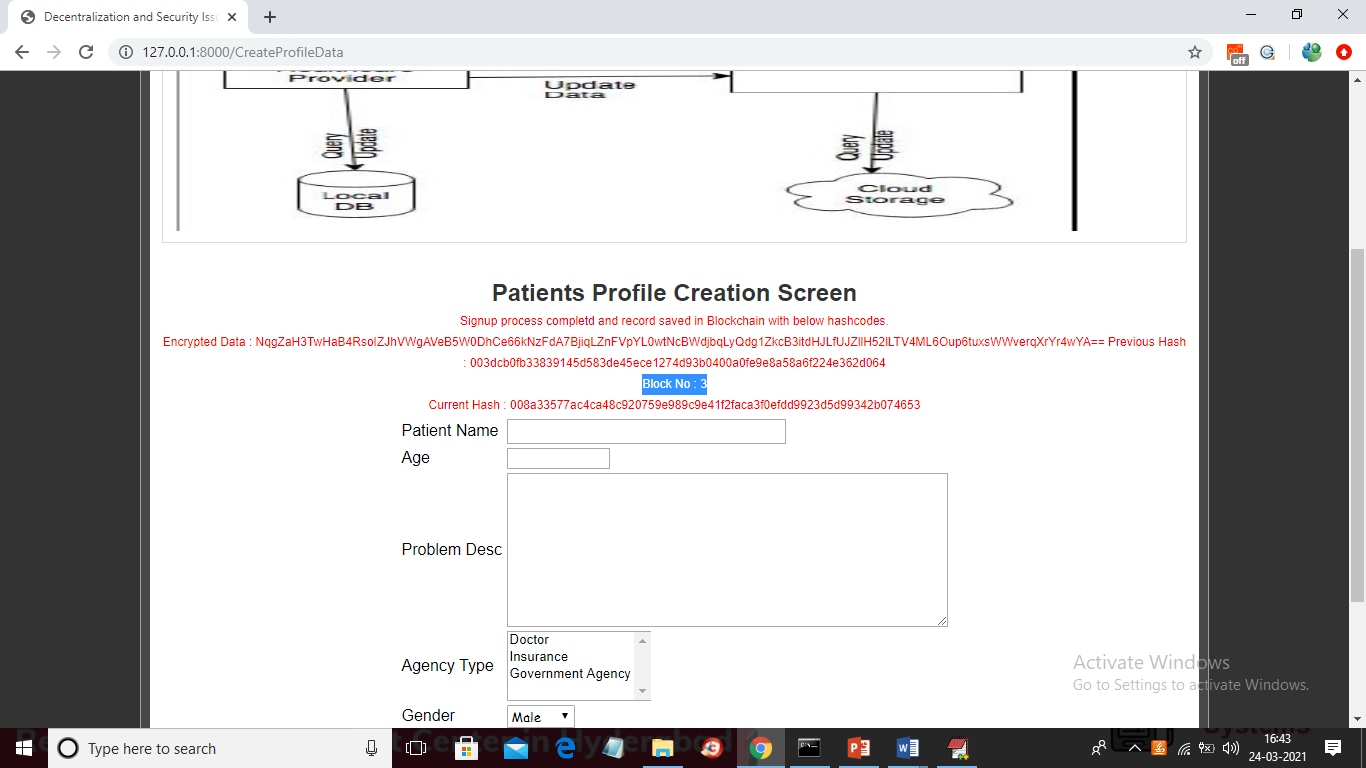
In above screen adding another user type as insurance and click button to get below output



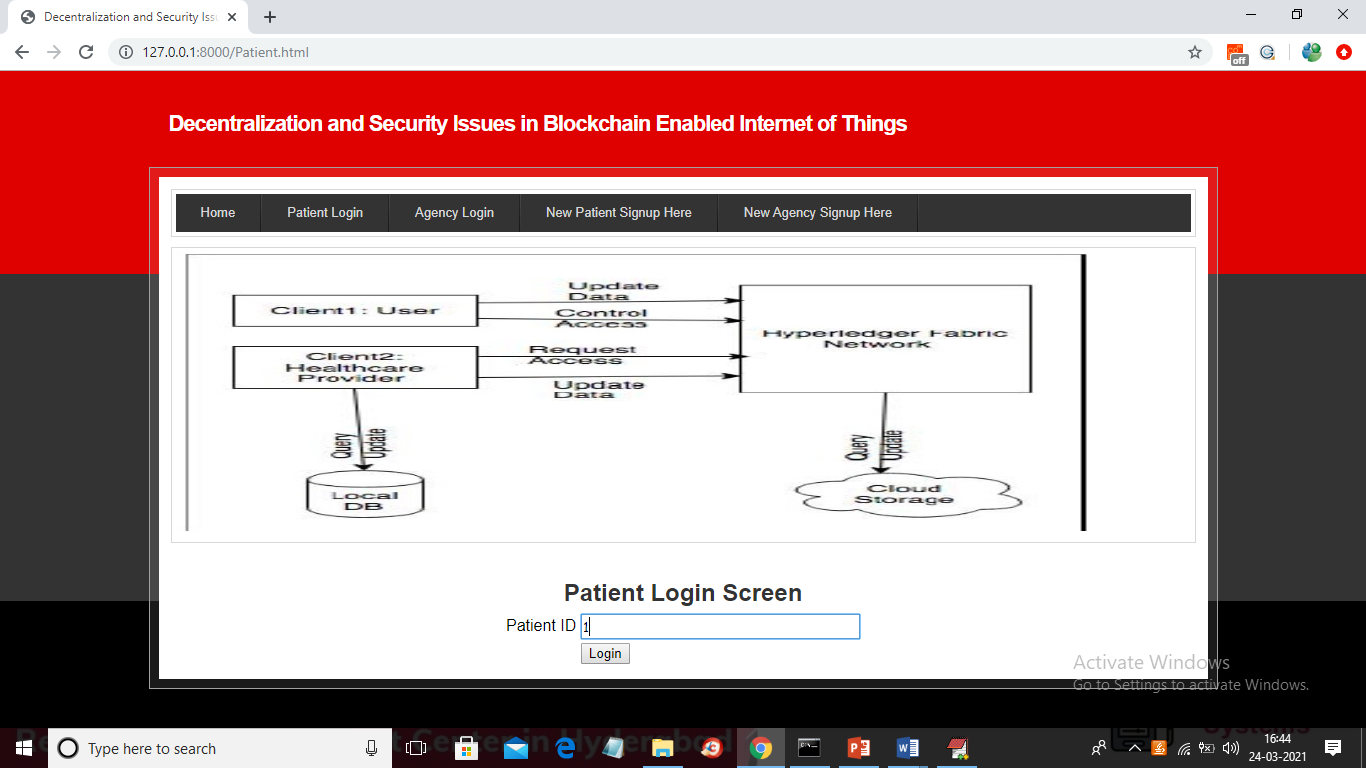
In above screen for insurance user another block created in Blockchain with block number as 2 and if you want you can check that previous hash code of current record will be matched with current hash code of previous record. So with current and previous hash code management Blockchain verify all transactions and now click on ‘New Patient Signup Here’ link to add patient profile



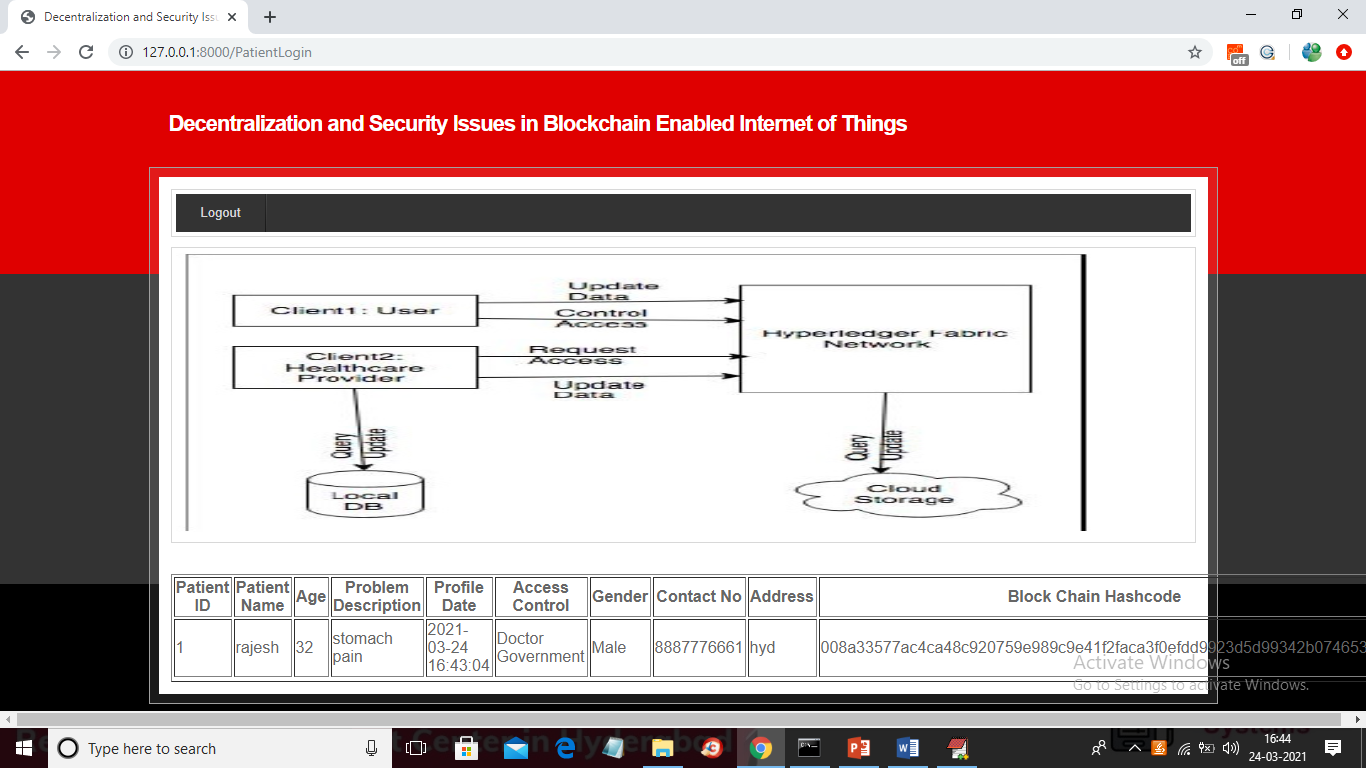
In above screen patient creating his profile and while creation he is selecting which users can be allowed to share or access data and in above screen patient selected all ‘Doctors’ and ‘Government Agencies’ can access his data and now click on ‘Create’ button to get below screen



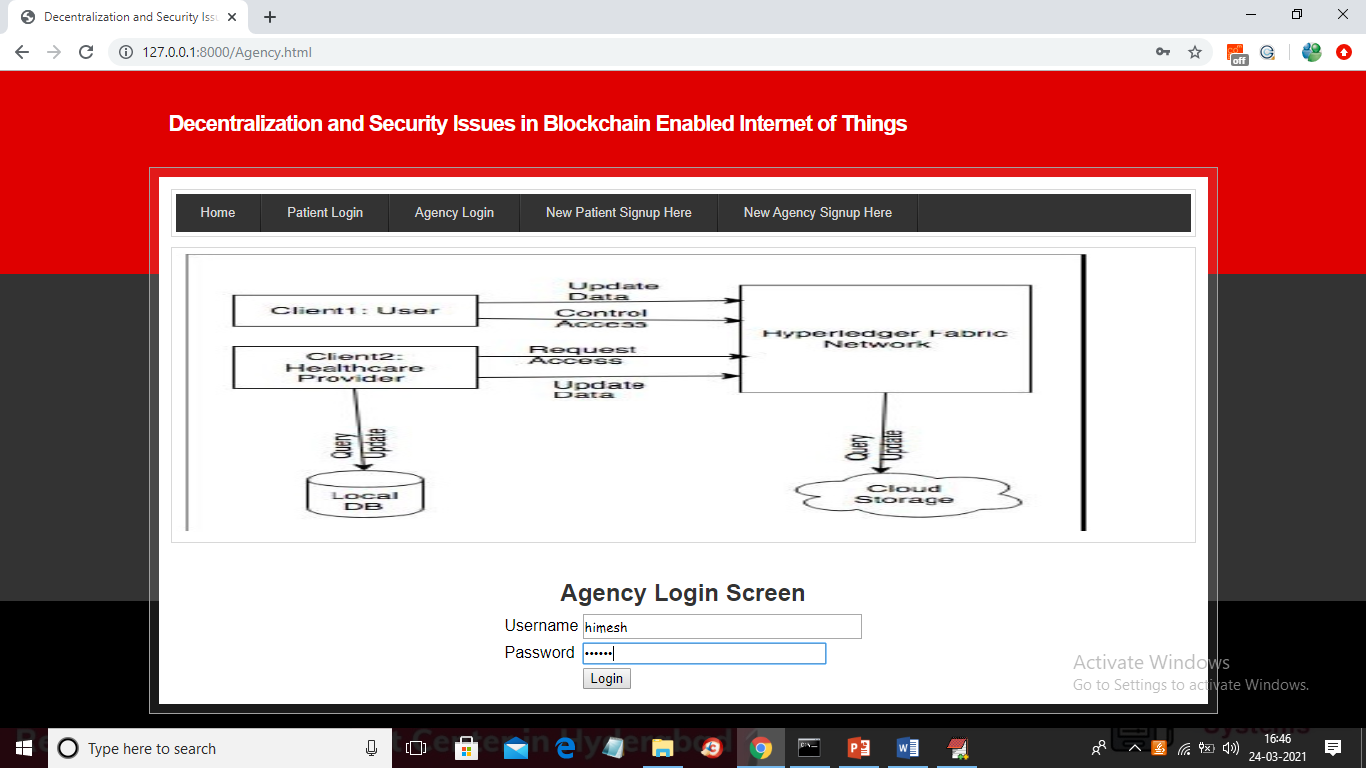
In above screen patient profile created with block no 3 and now ‘Patient’ can click on ‘Patient Login’ link to get below login screen



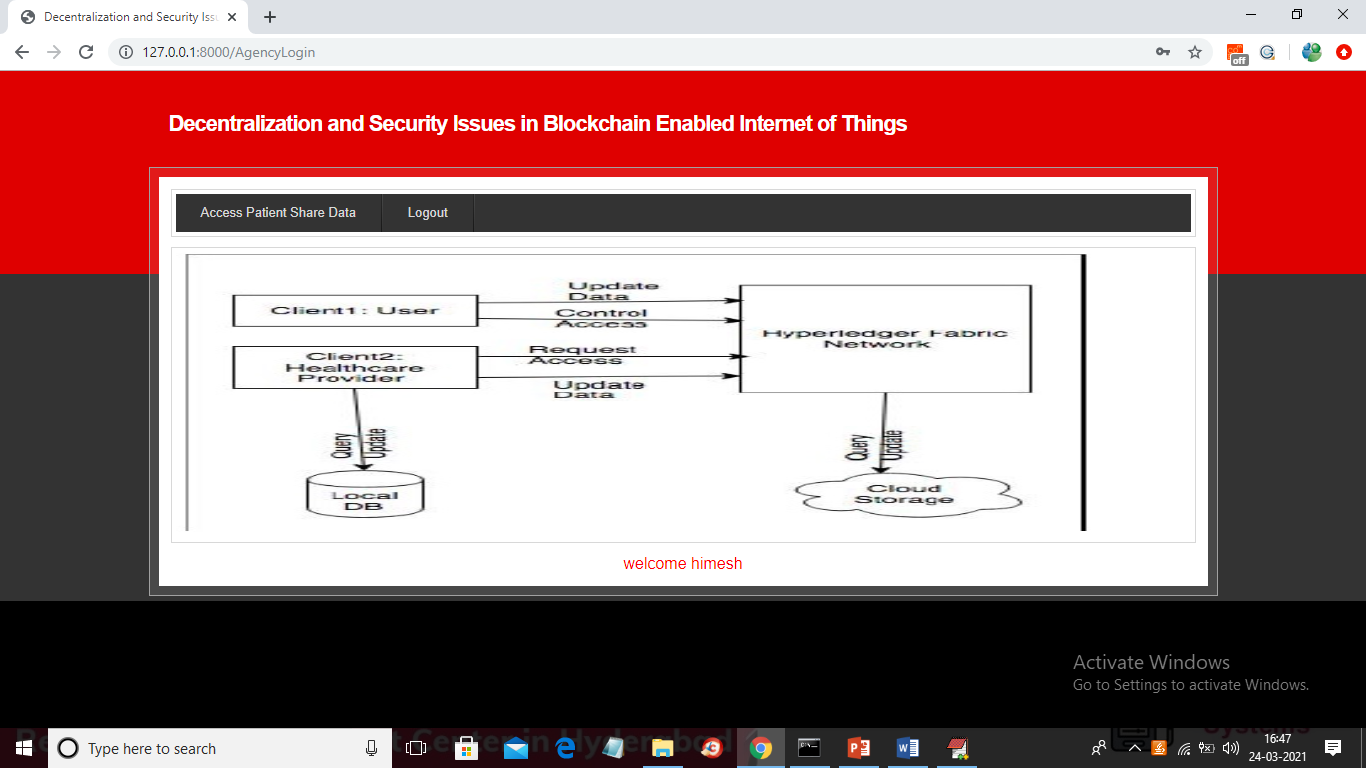
In above screen patient can enter his ID and then click on ‘Login’ button to get below screen



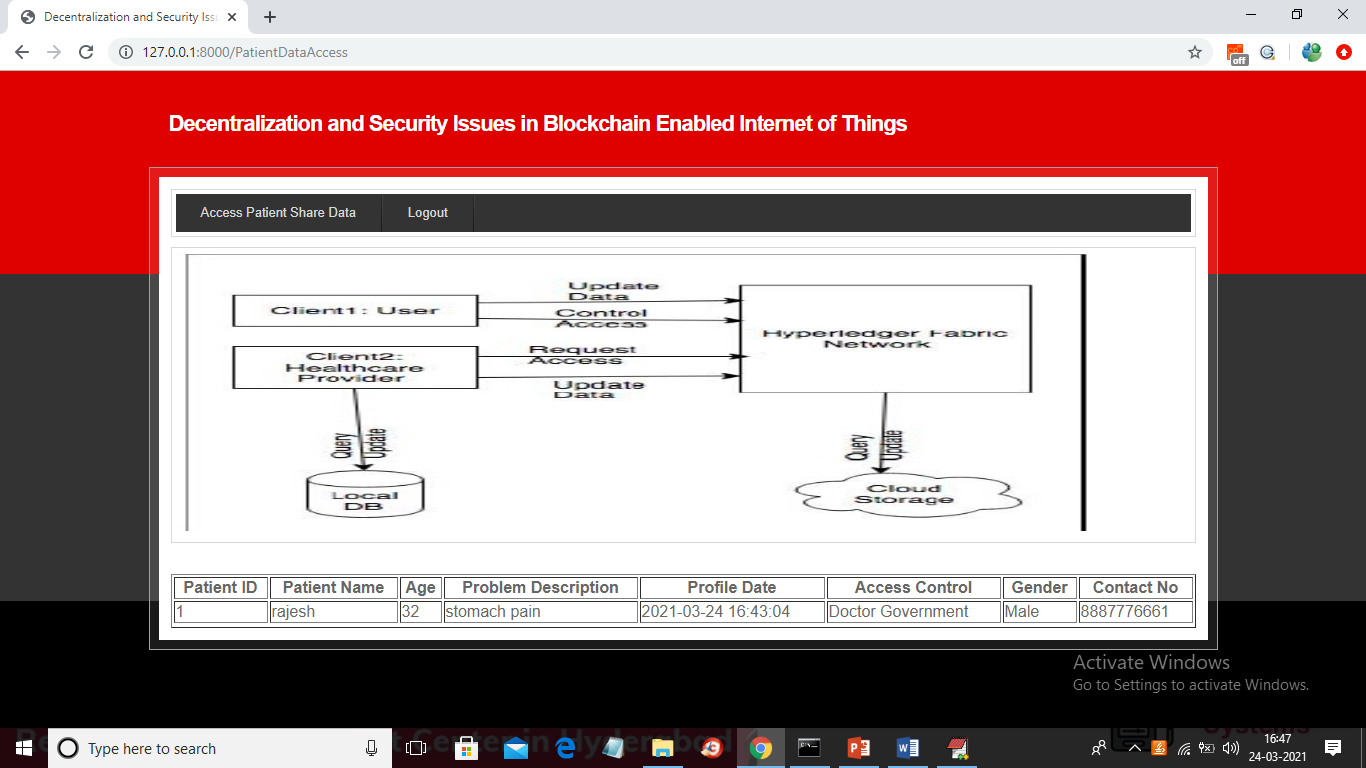
In above screen patient can view all his data in decrypted format from Blockchain server with associated hash code. Now logout and login as Doctor to access this patient data



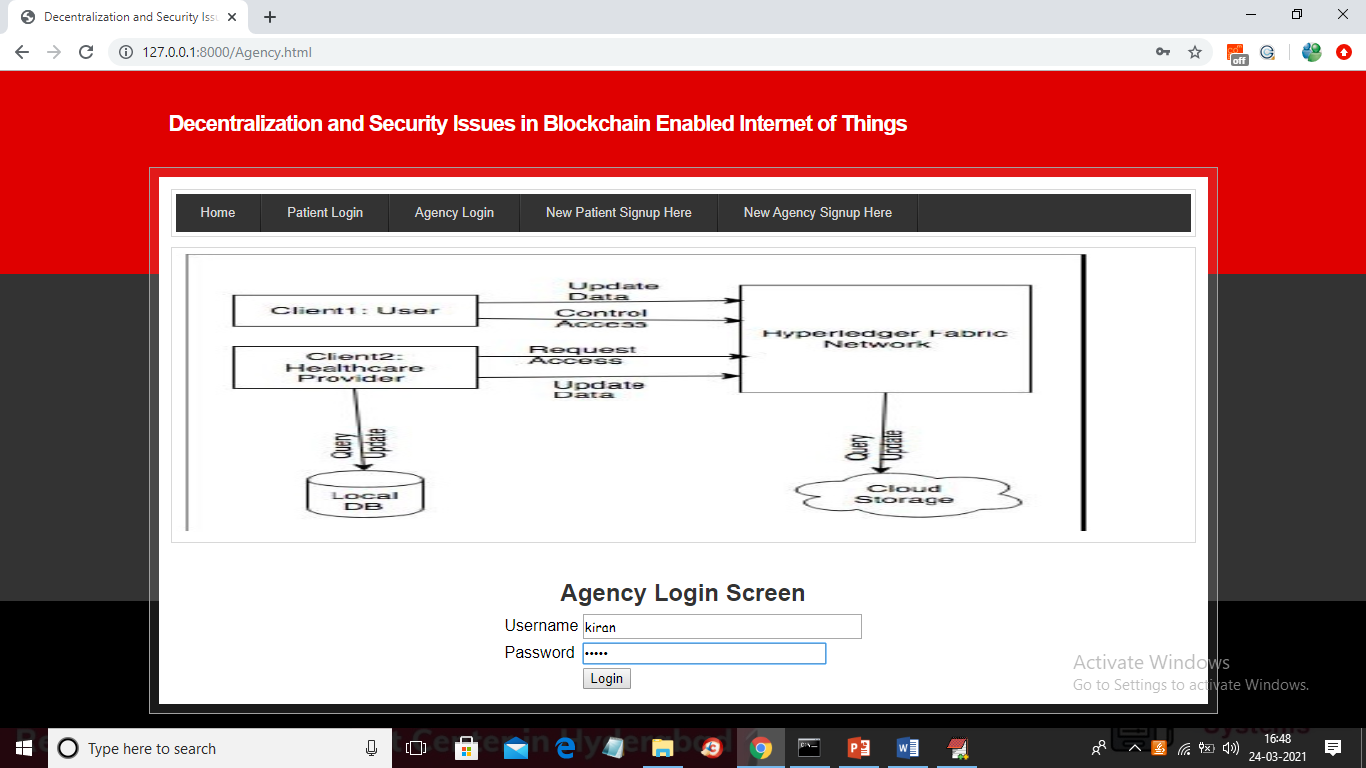
In above screen doctor himesh is login and he has permission to access patient data so he can see all records



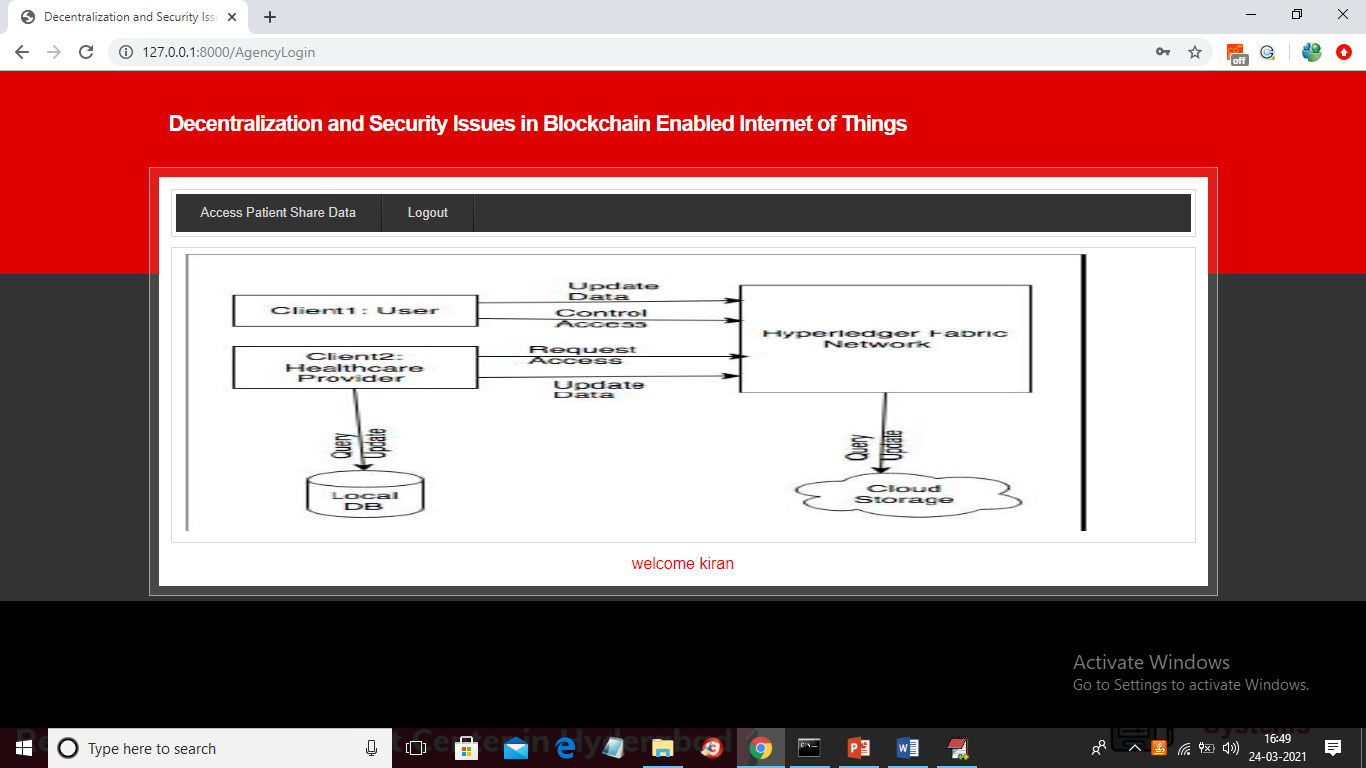
In above screen now can click on ‘Access Patient Share Data’ link to get below screen



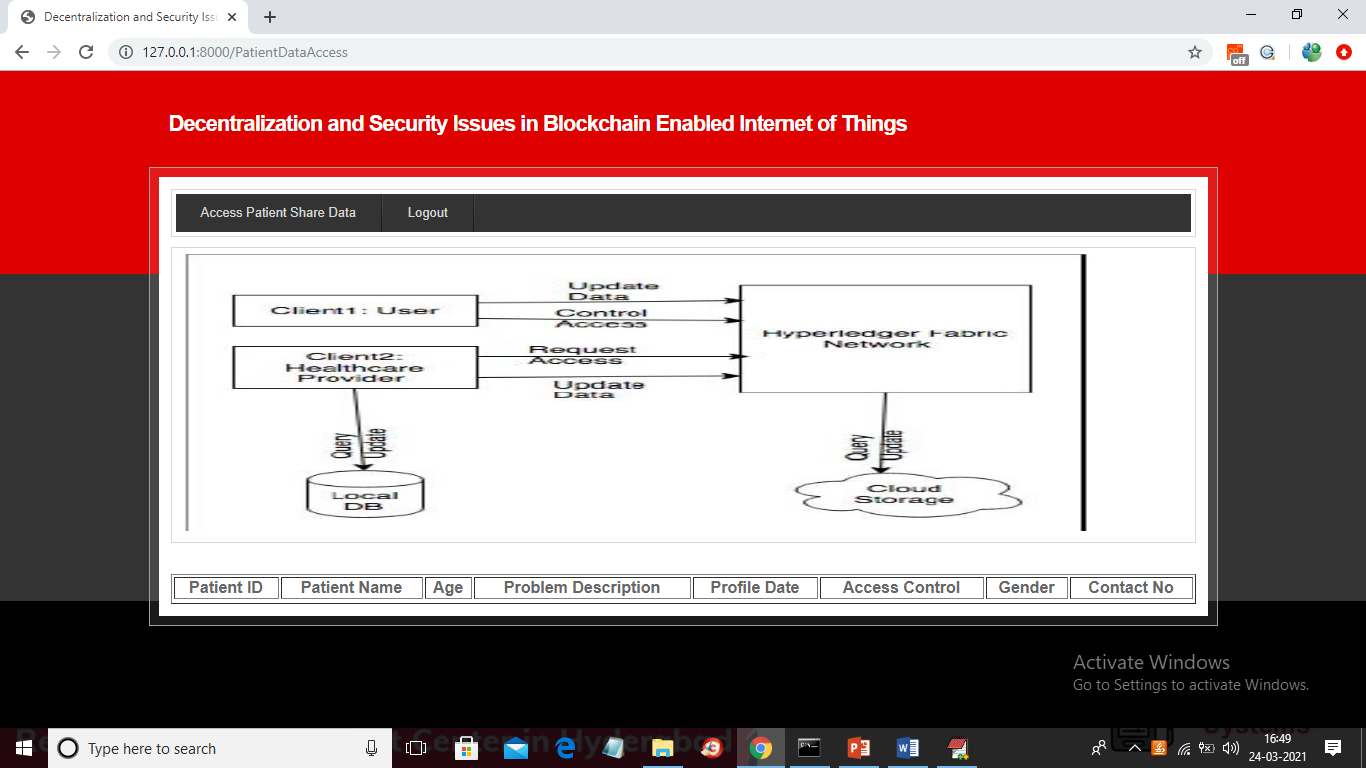
In above screen now doctor can see all data of patients and now login as insurance person and try to access patient data



In above screen insurance person ‘kiran’ is login and after login will get below screen

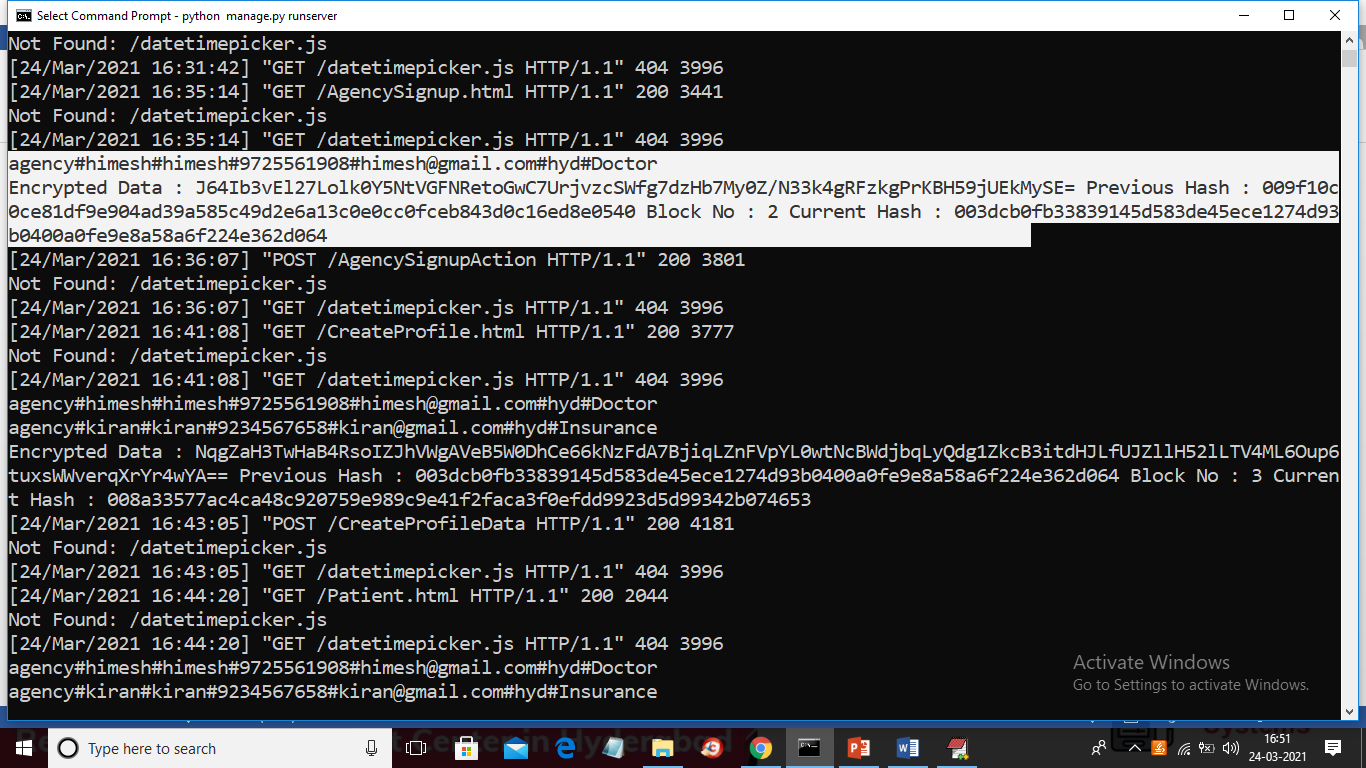


In above screen now insurance person can click on ‘Access Patient Share Data’ link to get below screen



In above screen insurance user has no permission to access share data so Blockchain server not showing any data to this user.

Similarly you can add any numbers of records and check Blockchain hash code and its encrypted data storage. In server below console also we can track all Blockchain hash code and encrypted data details



In above screen see selected text to get hash code details