IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

HEALTHCHAIN: A BLOCKCHAIN BASED PRIVACY PRESERVING SCHEME FOR PATIENT CENTERED HEALTH RECORDS AND EXCHANGE

[1]Bhagitha Paramesh

[1]Student (Pursuing Master of Technology, Mtech in CS)

[1]Computer Science,

[1]A P J AbdulKalam Technological University(KTU), Kerala, India

Abstract: Blockchain technology expeditiously acquire traction in healthcare industry as one of the most stimulating technical evolution. Particularly blockchain technology presents various possibilities for healthcare industry such as lesser transaction costs, increase in regulatory reporting, expeditious healthdata management,data integrity and healthcare records generality. In the context of smart health blockchain may stipulate distinct benefits,especially from a context-aware perspective where efficient and personalized solutions may be provided to the citizen and the society in broad. This work presents how blockchain technology transmutes the healthcare system and how does blockchain works in healthcare industry. we will cover the future potential of this technology in the industry and consider current usage and also portrays some problems in healthcare industry and its solutions using blockchain technology.

***Index Terms* - Blockchain , Healthcare , Smart health , Healthdata , Data integrity.**

I. INTRODUCTION

The Internet of Things (IoT) is an emerging technology that connects a large number of smart devices with Internet, where devices collect and exchange data to help people monitor changes and can be respond to them [1, 2]. Currently, it can be applied in many fields, like vehicular network [3], smart grid industry [4], smart home [5], by using IoT, smart healthcare has received more attentions.

IoT technology based smart healthcare has been proposed to improve efficiency and accuracy, break geographical limitations for remote monitoring [6], conduct disease risk assessment [7], and construct disease prediction systems [8]. In smart healthcare system, IoT devices, such as wearable sensors, keep collecting users' physiological data, such as electrocardiogram (ECG), blood pressure, temperature etc, these physiological data are sent to the user's local gateway to perform further data processing and then sent to a healthcare provider for diagnosis and feedback, so that users can better understand their own health status. However, these personal smart health devices are small and low power consumption, resulting in limited computing and storage capacity [1]. Therefore, smart health devices need additional methods to assist in computing and storage. So , a common approach is to outsource personal health data and electronic health records (EHRs) to cloud servers [7].

Cloud-based healthcare system improves efficiency and reduces cost compared with traditional healthcare system. However, there will be still many drawbacks in the system: (1) Large-scale smart health devices need high computing and storage capabilities of cloud servers. As it is a centralized storage unit any attacking may lost all the data (2) Health data is highly sensitive and should be protected well. Cloud server may leak user privacy for commercial benefits. For example, the users may only allow their health data to be accessed by authorized professional healthcare staffs, but cloud providers may leak users' personalized EHRs, for medical research, drug advertising , without the user's permission [9]. (3) When a medical dispute occurs, the user may suspect that the original EHRs stored in the cloud has been modified by the third party. Besides, it is difficult to share the data stored in cloud among different platforms with specific access control policies.

The blockchain technology provides a public, digitized distributed ledger, which is firstly proposed by Satoshi Nakamoto [10]. It has been widely used in cryptocurrency transactions such as Bitcoin [10] and Ether [11]. Blockchain is a chain of blocks that can exchange information. This technique was originally described in 1991 by group of researchers. It is like digital time stamps that cannot be tampered like a notary. Blockchain is a distributed ledger ,completely opens to anyone with smart contracts[3]. Once some data is recorded inside a blockchain it is very difficult to change it. Now let's know more about a block,a block consist of data,hash and hash of previous block. The first element in the block is data, data is the details of transactions or the records of patients ,it is depends up on where the blockchain is used. For example in bitcoin block the data will be the sender details,the receiver details and the amount of bitcoin for the transaction. The second element in the block is hash, hash is the identifier of the block data which is a random value generated when each block is created and unique like finger print. The data change in the block will result the change of hash value ,even a change in cases of the letters the whole hash value will change. The third element is the hash of previous block,this effectively creates the chain of block and makes the chain secure[4]..

In this paper, I propose Healthchain, a blockchain framework for patient centered health records and exchange. In Healthchain, users can periodically upload the health data and publish them as a transaction. Doctors or artificial intelligence (AI) health analyzers can diagnose anytime and anywhere based on the data and publishes the diagnosis as a transaction. It is not appropriate to record users' complete data on the blockchain, as resource requirements for each node on the blockchain will be extremely high. Otherwise, the blockchain will be too complex to maintain, search and verify. Considering the limited storage capacity of each blockchain node, we introduce ETHERIUM tool for storing the data to implement blockchain. In this way, Healthchain supports large-scale health data and has good scalability.

I propose a blockchain-based smart healthcare framework for health data exchange , named Healthchain. In Healthchain, users are enabled to upload IoT data and read doctors' diagnoses, and meanwhile, doctors are allowed to read users' IoT data and upload diagnose.the laboratory reports can be uploaded by the authority and both the user or patients and doctors can access the reports if the patient allows. In addition, all IoT data and diagnoses cannot be tampered with or denied, which can avoid medical disputes.

II. Related Works

The emergence of 5th generation of wireless networks will help the blockchain to develop a faster and secure data management. As the customary speed of smart phones and tablets increased with the previous generation networks,5G promises reduced latency and higher capacity will enhance blockchain dominance.The new generation of faster-than-ever mobile (wireless) communications technology, 5G, is around the corner. With its unprecedented data transfer speed and strength, it will help accommodate advances made in AI, machine learning, neural networks and blockchain across various verticals, including healthcare. As this new technology ecosystem come out, blockchain assures significant change in capturing and managing patient health records and claims data.

A promising approach has been considered to improve the quality of healthcare service , an online medical primary diagnosis system, which can provide convenient medical decision support through applying mobile communication and data analysis technology.an cost-effective and privacy-preserving online medical particular diagnosis framework (CINEMA). Within CINEMA framework, users can approach online health primary diagnosing service accurately without expose their medical data. Specifically, based on fast secure permutation and alikeness methods, the encrypted user's query is immediately operated at the service provider without decryption, and the diagnosis result can only be decrypted by the user, in the meantime, the diagnosis model in service provider can also be secured. Through extended analysis, we show that CINEMA can ensure that user's health information and healthcare service provider's diagnosis records must keep confidential, and has significantly decrease computation and communication overhead. In addition, performance evaluations via implementing CINEMA exhibit its effectiveness in terms of important atmosphere.

In addition to the problems pointed out above, there are still difficulties in key management and flexible revocation. Therefore, we propose Healthchain, which not only supports finegrained access control for large-scale data, but also implements key management and flexible revocation using independent key transactions.

III. System Model and Design Goals

In this section, we introduce the system model, and design goals of a blockchain-based smart healthcare architecture, named Healthchain.

User nodes. There are many lightweight user nodes that only store the block headers of Userchain, and they can only generate and publish transactions add new user transactions to a new Ublock. In addition, all user nodes can also implement information search on Docchain but cannot add transactions on Docchain.

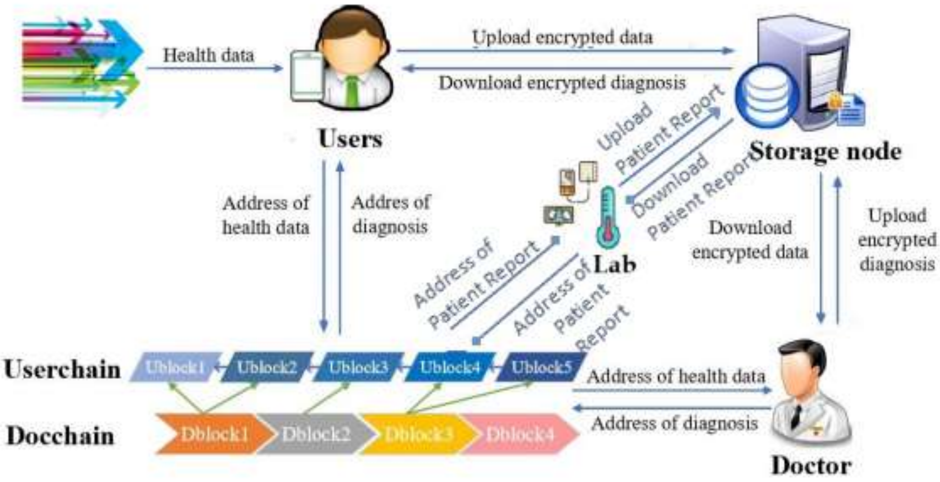
Doctor nodes. Each one doctor node can be not only a real doctor from a hospital, but also an artificial intelligence health analyzer from a smart healthcare service company. They can provide continuous diagnosis based on users' data. All hospitals and companies in Healthchain form a consortium, and all doctor nodes' behaviors is restricted by the rules of the consortium. Authorized doctor nodes can read the information on Userchain and generate transactions for Docchain. Specially, doctor nodes themselves cannot add transactions to Docchain.

Lab nodes. The patient will be the data owner,but every time the patient need to depend on the laboratory for some lab reports. The lab node upload all the patient centric data and reports to the storage node and at any time the patient can access the data and can be validate by sending it for the diagnose.

Accounting node. It's a special node in the system It can verify that whether the transactions from doctor nodes are correct and valid. At each time period, all accounting nodes select a leader. The leader aggregates valid transactions from doctor nodes in the consortium, and generates new Dblock and adds new Dblock to Docchain.

Storage nodes. They collaboratively store complete encrypted users' data and encrypted doctors' diagnoses in a distributed manner. In this paper, we assume that each storage node is Etherium-based, where Etherium system is managed and maintained by the consortium of healthcare providers, e.g., hospitals.Ethrium is a tool to implement blockchain. Anyone can find the complete file stored in Etherium via the hash string of the file on Userchain or Docchain. Etherium makes it possible to distribute high volumes of data with high efficiency.

Userchain. It's a public blockchain, which is used to publish users' data. Anyone can join Userchain to read transactions, send transactions, at any time. Userchain consists of a series of Ublocks and grows over time. Each Ublock contains the hash of the previous Ublock and transactions generated by users.



Docchain. It's a consortium blockchain, which is used to publish doctors' diagnoses. Only doctor nodes authorized by consortium can generate diagnosis transactions, which can be added to Docchain by the accounting nodes. However, anyone can read the information on Docchain. Docchain consists of a series of Dblocks and grows over time. Each Dblock contains the hash of the previous Dblock and transactions doctors generated.

As illuminated in Fig. 3.1, here we briefly show data flows in our scheme: health data of the user node periodically upload to the storage node. User node adds the hash of the encrypted data as a transaction to Userchain. The doctor node decrypts the users' data and gives real-time online diagnoses. Then the doctor sends the encrypted diagnosis to the storage node and generates a transaction for diagnosis which includes the address of the encrypted diagnosis. Users read the information on Docchain to understand their own health status.

3.1 Design goals

We aim to achieve privacy-preserving for intelligent medical systems, and the following design goals should be met.

High efficiency: Real-time online diagnosis is also very important, which can even save the lives of users. Therefore, the user's health data and the the doctor's diagnosis is uploaded in time and read with specific access policies.

Privacy-preserving: Each user's health data can be only obtained by himself/herself and his/her authorized professional healthcare staff and also the, doctor's diagnosis can be accessed by the diagnosed user and the authorized professional healthcare staffs. No adversary can get the user's private information.

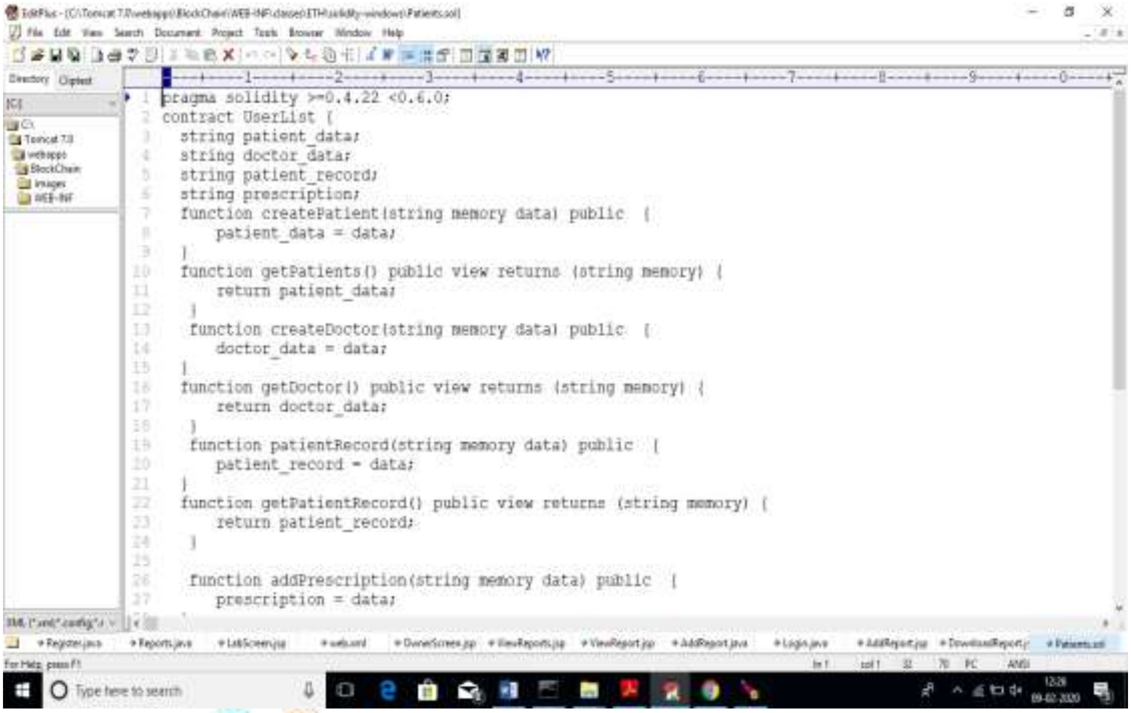
Accountability: In order to prevent medical disputes, the doctor needs to be responsible for the diagnosis he/she has made and cannot tamper with or deny it. Anyone can audit whether past diagnoses have been tampered with.

On-demand revocation: The user can revoke the right of a doctor to access his/her IoT data at any time. The revoked doctor cannot read the data after revocation, which is called forward security.

IV. Proposed Schema : Healthchain

In this project total 3 users are available Patients, doctors and Lab. Patients will register with the application and then create profile and give access to doctors.Doctors will register with the application and then login and access all those patients' records who gave permission to this doctor. Doctor will add prescription to patient profile.Lab person will login to application using username and password and after login he will upload reports of patients. Patients can login and download or view reports based on filtration .

In this project we described the concept to store patient medical records using block chain technology as its provide inbuilt support to secure data store in it. To store details we are using block chain ETHEREUM tool and using below code we generate solidity program. In fig 4.1 screen functions define to store patient, doctors and prescription details with reports.



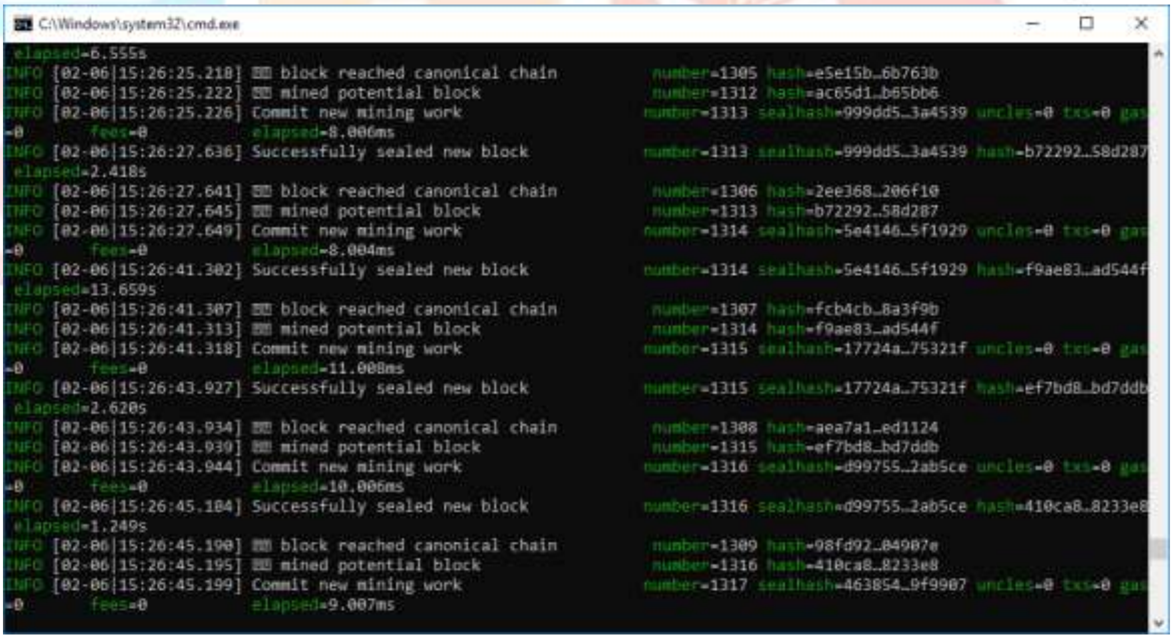
```
pragma solidity >=0.4.22 <0.6.0;
contract UserList {
  string patient_data;
  string doctor_data;
  string patient_record;
  string prescription;
  function createPatient(string memory data) public  {
      patient_data = data;
  }
  function getPatients() public view returns (string memory) {
      return patient_data;
   }
   function createDoctor(string memory data) public  {
      doctor_data = data;
  }
  function getDoctor() public view returns (string memory) {
      return doctor_data;
   }
   function patientRecord(string memory data) public  {
      patient_record = data;
  }
  function getPatientRecord() public view returns (string memory) {
      return patient_record;
   }

   function addPrescription(string memory data) public  {
      prescription = data;
```

Fig 4.1: solidity program: screen functions define to store patient, doctors and prescription details with reports.

IV. IMPLEMENTATION AND EVALUATION

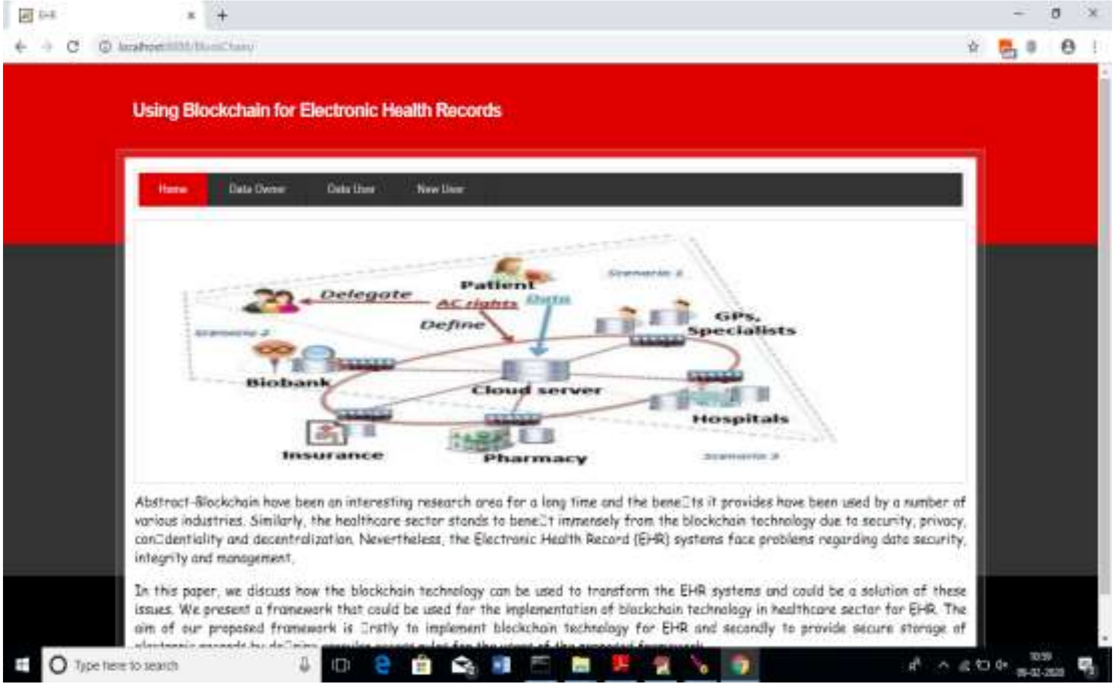
In this section we would like to share some implementation steps and screenshorts.



```
 elapsed=6.555s
INFO [02-06|15:26:25.218] ▯▯ block reached canonical chain          number=1305 hash=e5e15b…6b763b
INFO [02-06|15:26:25.222] ▯▯ mined potential block                  number=1312 hash=ac65d1…b65bb6
INFO [02-06|15:26:25.226] Commit new mining work                   number=1313 sealhash=999dd5…3a4539 uncles=0 txs=0 gas
=0       fees=0            elapsed=8.006ms
INFO [02-06|15:26:27.636] Successfully sealed new block            number=1313 sealhash=999dd5…3a4539 hash=b72292…58d287
 elapsed=2.418s
INFO [02-06|15:26:27.641] ▯▯ block reached canonical chain          number=1306 hash=2ee368…206f10
INFO [02-06|15:26:27.645] ▯▯ mined potential block                  number=1313 hash=b72292…58d287
INFO [02-06|15:26:27.649] Commit new mining work                   number=1314 sealhash=5e4146…5f1929 uncles=0 txs=0 gas
=0       fees=0            elapsed=8.004ms
INFO [02-06|15:26:41.302] Successfully sealed new block            number=1314 sealhash=5e4146…5f1929 hash=f9ae83…ad544f
 elapsed=13.659s
INFO [02-06|15:26:41.307] ▯▯ block reached canonical chain          number=1307 hash=fcb4cb…8a3f9b
INFO [02-06|15:26:41.313] ▯▯ mined potential block                  number=1314 hash=f9ae83…ad544f
INFO [02-06|15:26:41.318] Commit new mining work                   number=1315 sealhash=17724a…75321f uncles=0 txs=0 gas
=0       fees=0            elapsed=11.008ms
INFO [02-06|15:26:43.927] Successfully sealed new block            number=1315 sealhash=17724a…75321f hash=ef7bd8…bd7ddb
 elapsed=2.620s
INFO [02-06|15:26:43.934] ▯▯ block reached canonical chain          number=1308 hash=aea7a1…ed1124
INFO [02-06|15:26:43.939] ▯▯ mined potential block                  number=1315 hash=ef7bd8…bd7ddb
INFO [02-06|15:26:43.944] Commit new mining work                   number=1316 sealhash=d99755…2ab5ce uncles=0 txs=0 gas
=0       fees=0            elapsed=10.006ms
INFO [02-06|15:26:45.184] Successfully sealed new block            number=1316 sealhash=d99755…2ab5ce hash=410ca8…8233e8
 elapsed=1.249s
INFO [02-06|15:26:45.190] ▯▯ block reached canonical chain          number=1309 hash=98fd92…04907e
INFO [02-06|15:26:45.195] ▯▯ mined potential block                  number=1316 hash=410ca8…8233e8
INFO [02-06|15:26:45.199] Commit new mining work                   number=1317 sealhash=463854…9f9907 uncles=0 txs=0 gas
=0       fees=0            elapsed=9.007ms
```

Fig 5.1 : Blockchain etherium server initialising

Initially we have to start the blockchain Ethereum server. Once started u will get fig 5.1. U need to wait till above screen displayed messages as 'block reached Canonical chain' and it will take nearly half an hour to setup and to starts displaying such messages. Once you are getting above messages then double click on 'initialize_blockchain.bat' to initialize block chain storage and after running this file you must get message as smart contract deployed successfully. After getting that message follow below instructions to run code .Deploy 'BlockChain' folder inside tomcat Web App folder and then start tomcat server and then open browser and enter the localhost url to get the below figure fig 5.2.

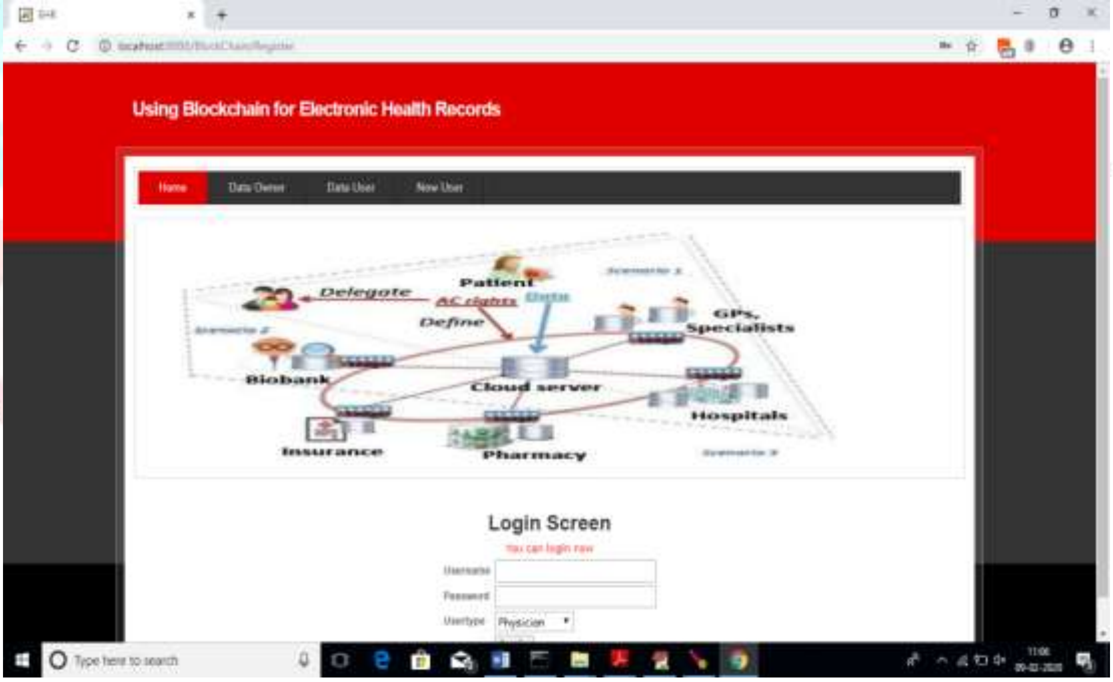


Abstract-Blockchain have been an interesting research area for a long time and the bene⬚ts it provides have been used by a number of various industries. Similarly, the healthcare sector stands to bene⬚t immensely from the blockchain technology due to security, privacy, con⬚dentiality and decentralization. Nevertheless, the Electronic Health Record (EHR) systems face problems regarding data security, integrity and management.

In this paper, we discuss how the blockchain technology can be used to transform the EHR systems and could be a solution of these issues. We present a framework that could be used for the implementation of blockchain technology in healthcare sector for EHR. The aim of our proposed framework is ⬚rstly to implement blockchain technology for EHR and secondly to provide secure storage of

Fig 5.2: webapp index page loading

Now we can register and then login. Here I am adding one patient details and DataOwner will be consider as patient. After adding patient details in block chain we will get below figure fig 5.3



Login Screen

You can login now

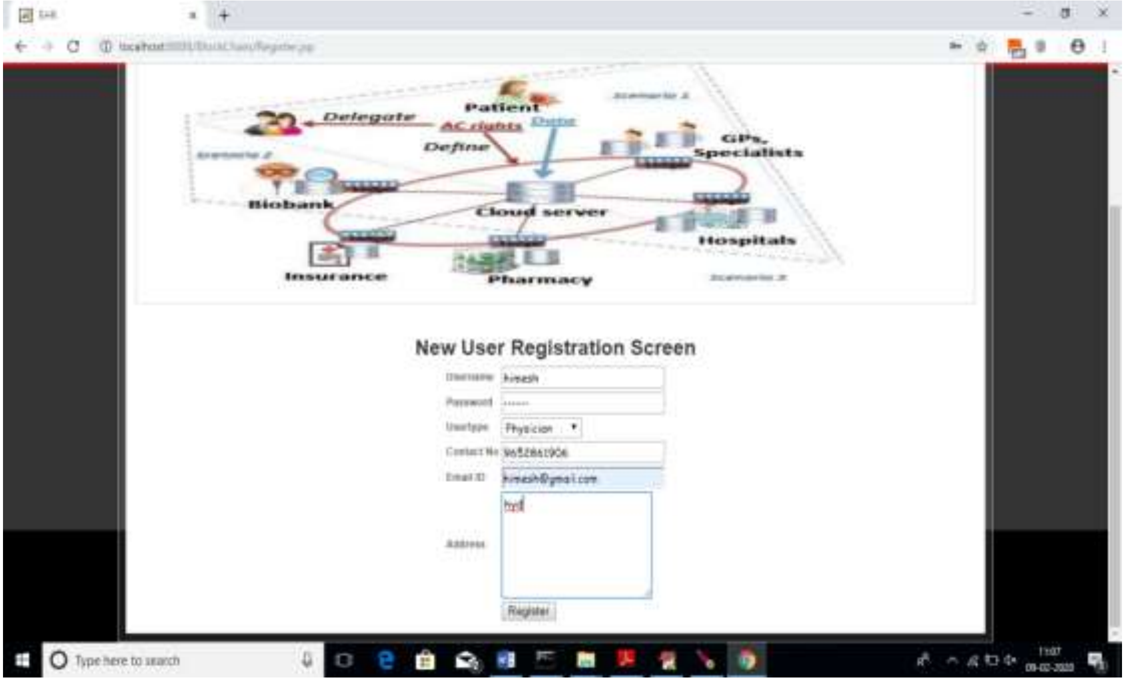
Username

Password

Usertype Physician ▾

Fig 5.3 : data owner uploading details to ublock

Now go back to ‘New User’ link again and add one doctor

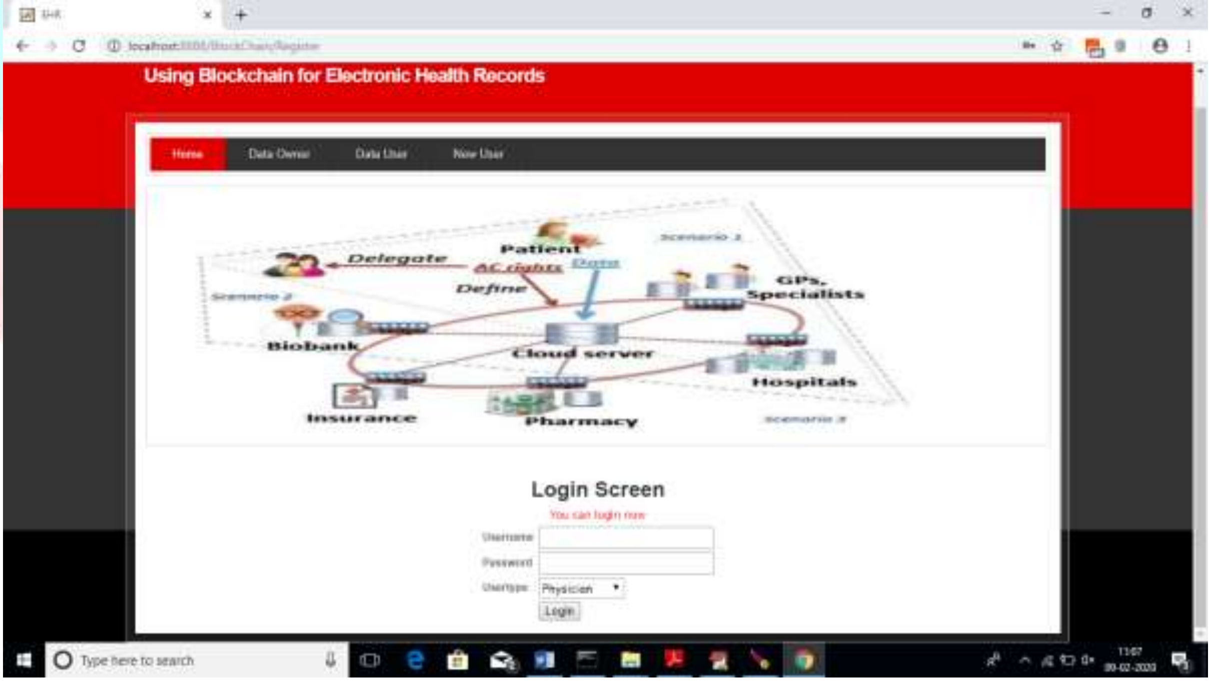


New User Registration Screen

Username: himesh
Password: ......
Usertype: Physician
Contact No: 9652861906
Email ID: himesh@gmail.com
Address: hyd

Fig 5.4 :doctor uploading details to dblock

In above figure fig 5.4 I am adding one doctor details and selected user type as ‘Physician’ and after adding detail will get below figure fig 5.5


Using Blockchain for Electronic Health Records

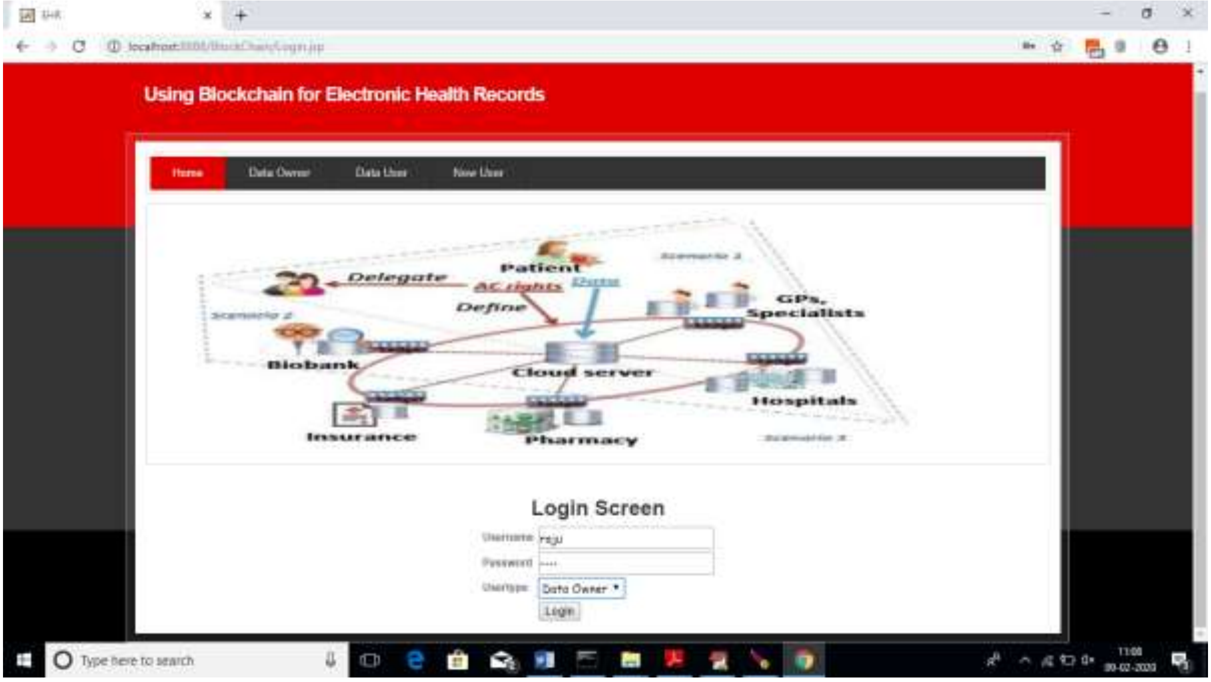
Login Screen

You can login now

Username:
Password:
Usertype: Physician

Fig 5.5 : data owner login screen

Now click on ‘Data Owner’ to login as patient, see below figure fig 5.6



Using Blockchain for Electronic Health Records

Login Screen

Username: raju

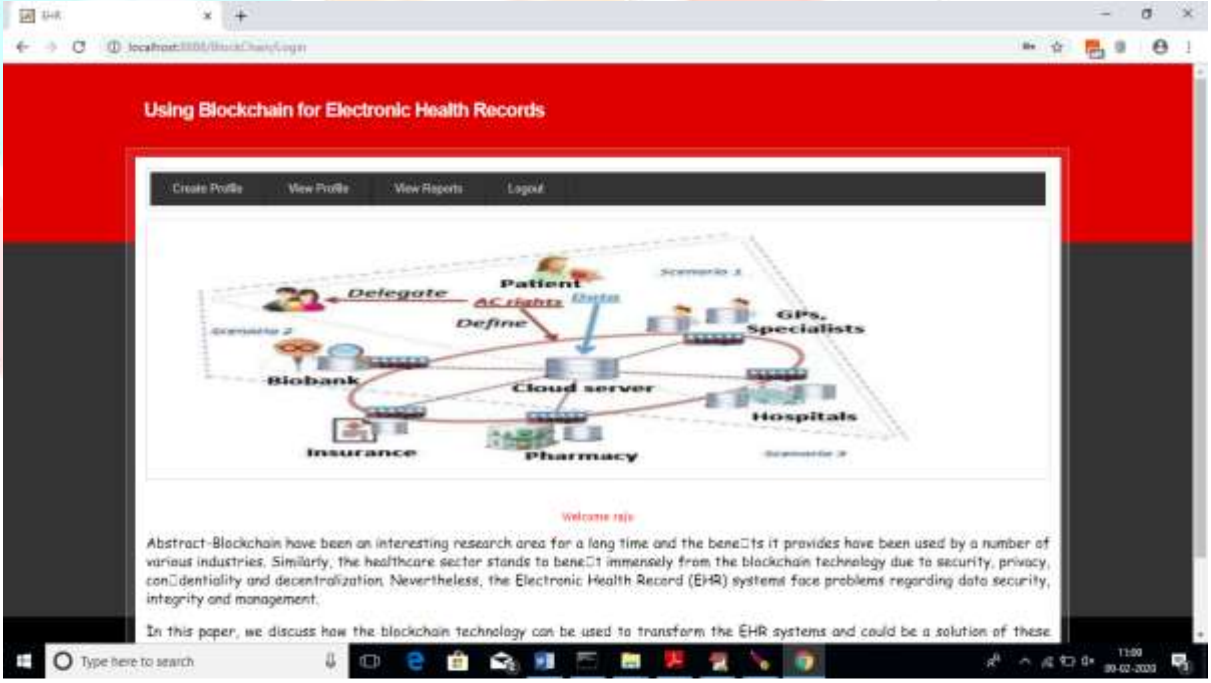
Password: ····

Usertype: Data Owner ▾

Login

Fig 5.7 : login as patient

In above figure fig5.7 I am login as patient by selecting user type as ‘Data Owner’ and after login will get below figure fig 5.8



Using Blockchain for Electronic Health Records

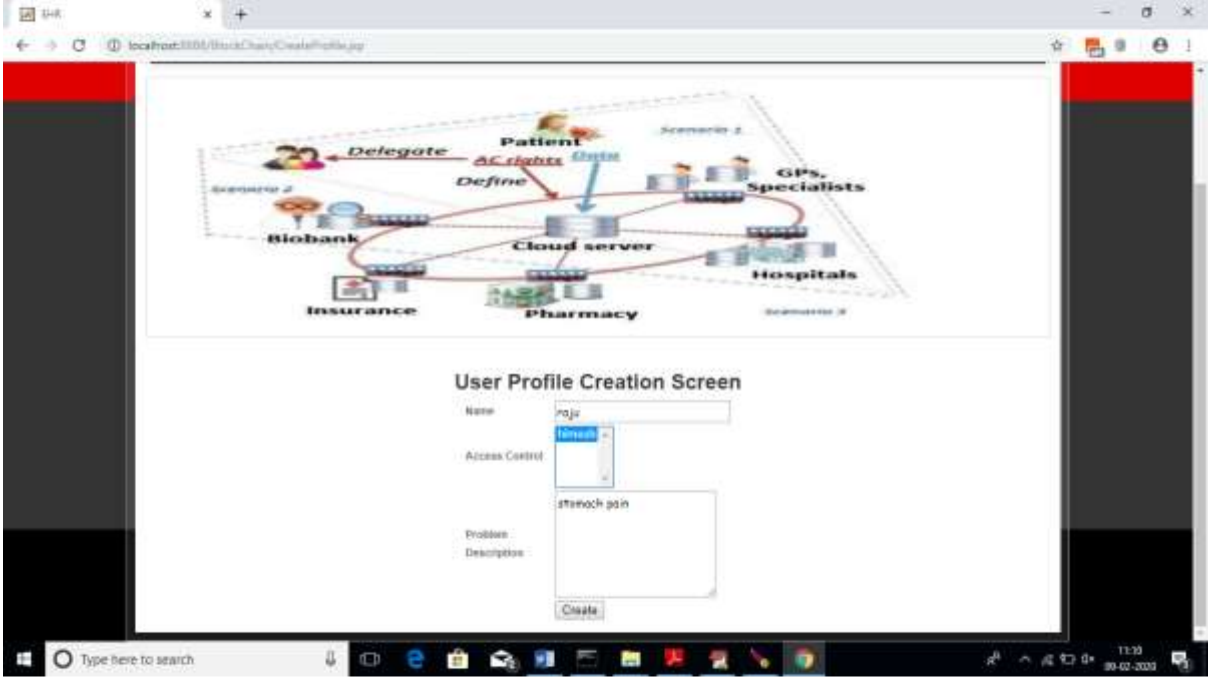
Welcome raju

Abstract-Blockchain have been an interesting research area for a long time and the bene□ts it provides have been used by a number of various industries. Similarly, the healthcare sector stands to bene□t immensely from the blockchain technology due to security, privacy, con□dentiality and decentralization. Nevertheless, the Electronic Health Record (EHR) systems face problems regarding data security, integrity and management.

In this paper, we discuss how the blockchain technology can be used to transform the EHR systems and could be a solution of these

Fig 5.8 : creating profile

In above screen click on ‘Create Profile’ link and add profile details



User Profile Creation Screen

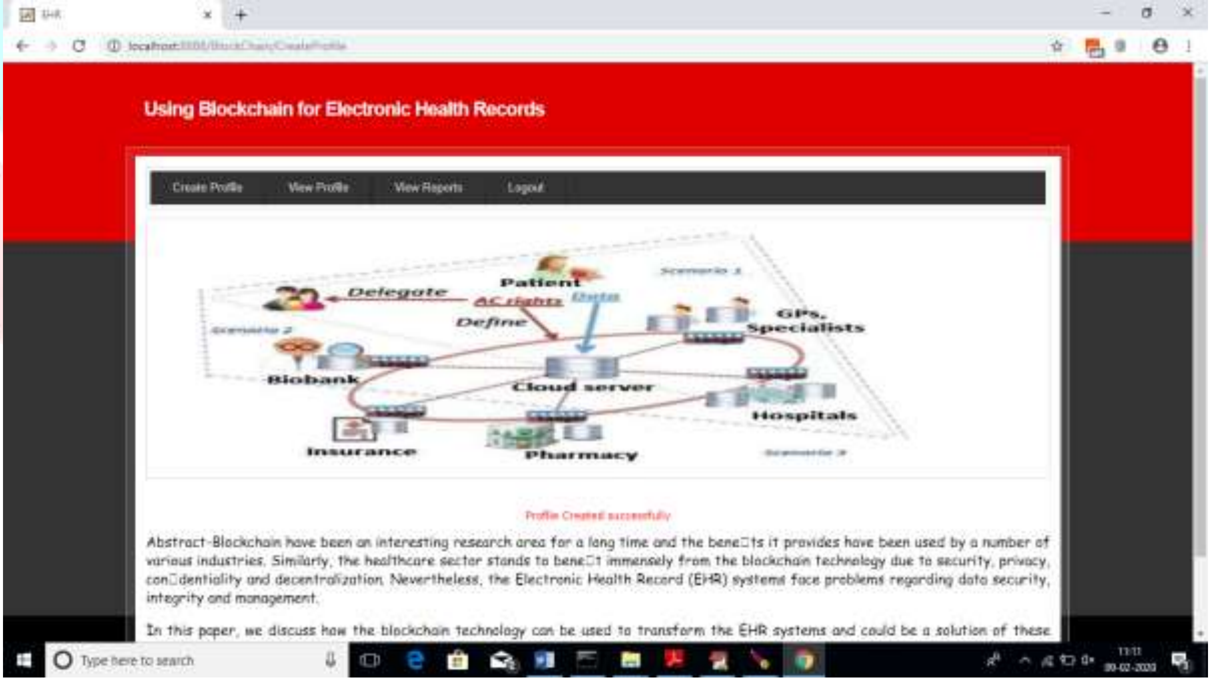
Name: raju

Access Control: [illegible]

Problem Description: stomach pain

Fig 5.9: user profile creation

In above figure patient will add his disease details and give access permission to doctor by selecting doctor name from drop down list. After adding disease details will get below figure



Using Blockchain for Electronic Health Records

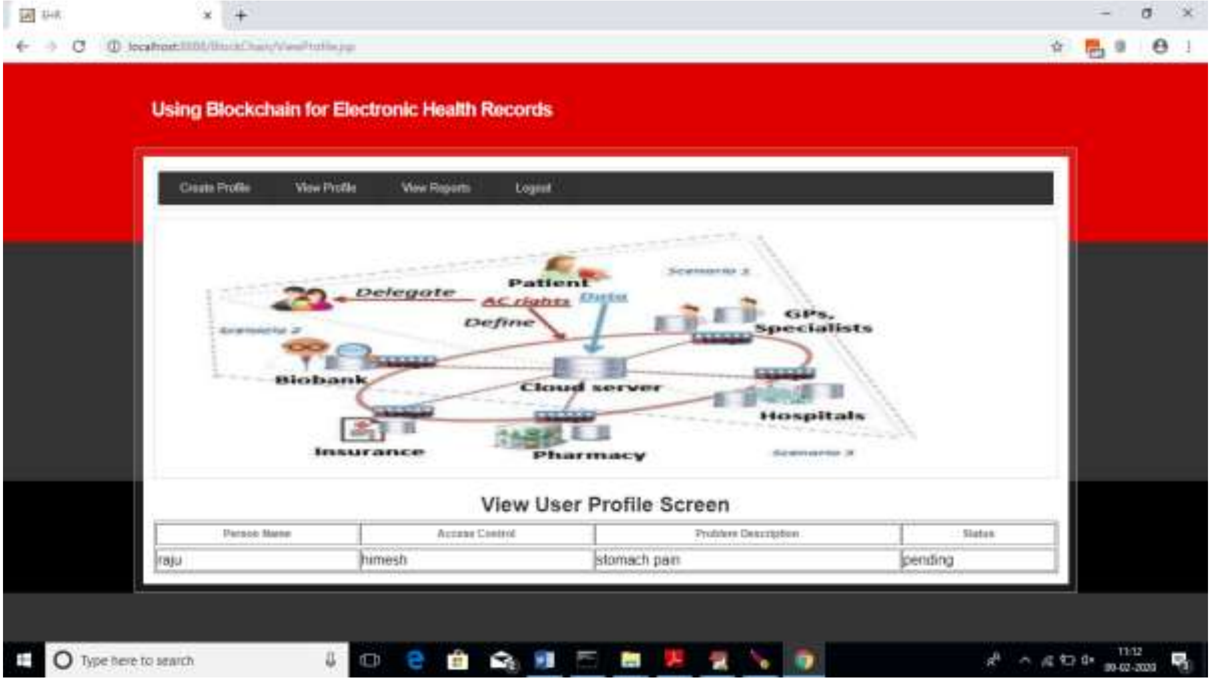
Profile Created successfully

Abstract-Blockchain have been an interesting research area for a long time and the bene□ts it provides have been used by a number of various industries. Similarly, the healthcare sector stands to bene□t immensely from the blockchain technology due to security, privacy, con□dentiality and decentralization. Nevertheless, the Electronic Health Record (EHR) systems face problems regarding data security, integrity and management.

In this paper, we discuss how the blockchain technology can be used to transform the EHR systems and could be a solution of these

Fig 5.10 : message shown : profile created successfully

In above figurewe got message as profile created and now click on ‘View Profile’ link to get details in below figure

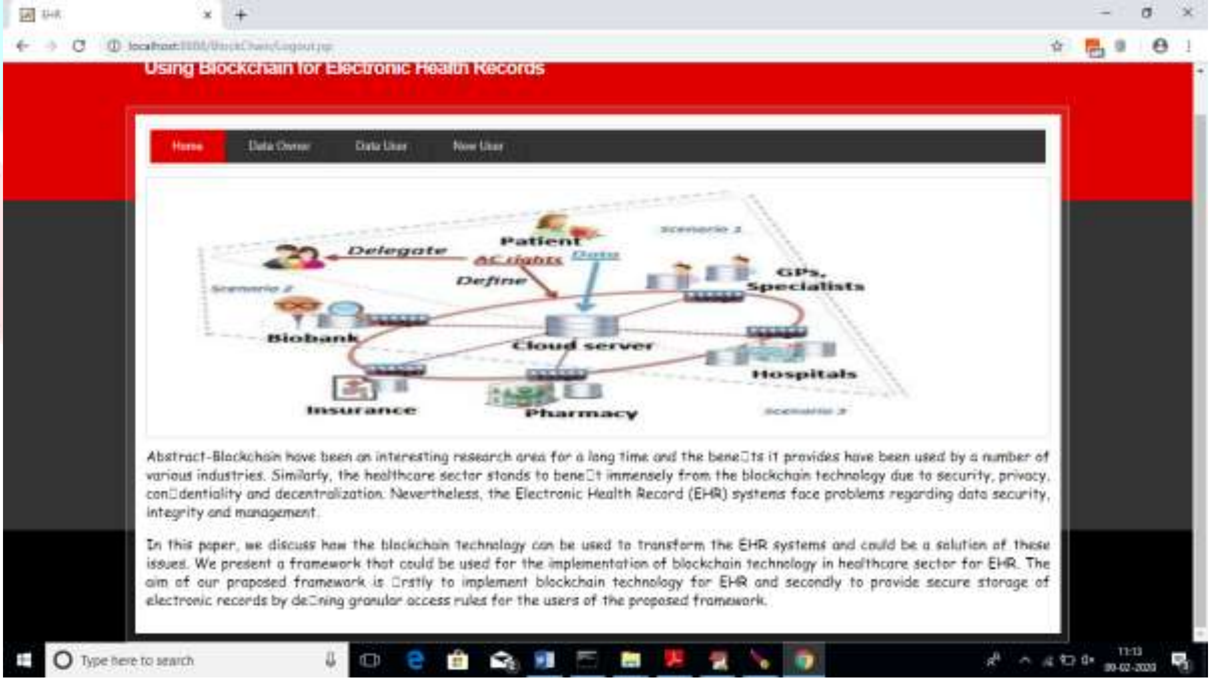


View User Profile Screen

Person Name	Access Control	Problem Description	Status
raju	himesh	stomach pain	pending

Fig 5.11 : view user profile screen

In above figure we can see all details and in last column we got message as pending which means no doctor has given any prescription. Now log out and login as doctor to give prescription to this patient

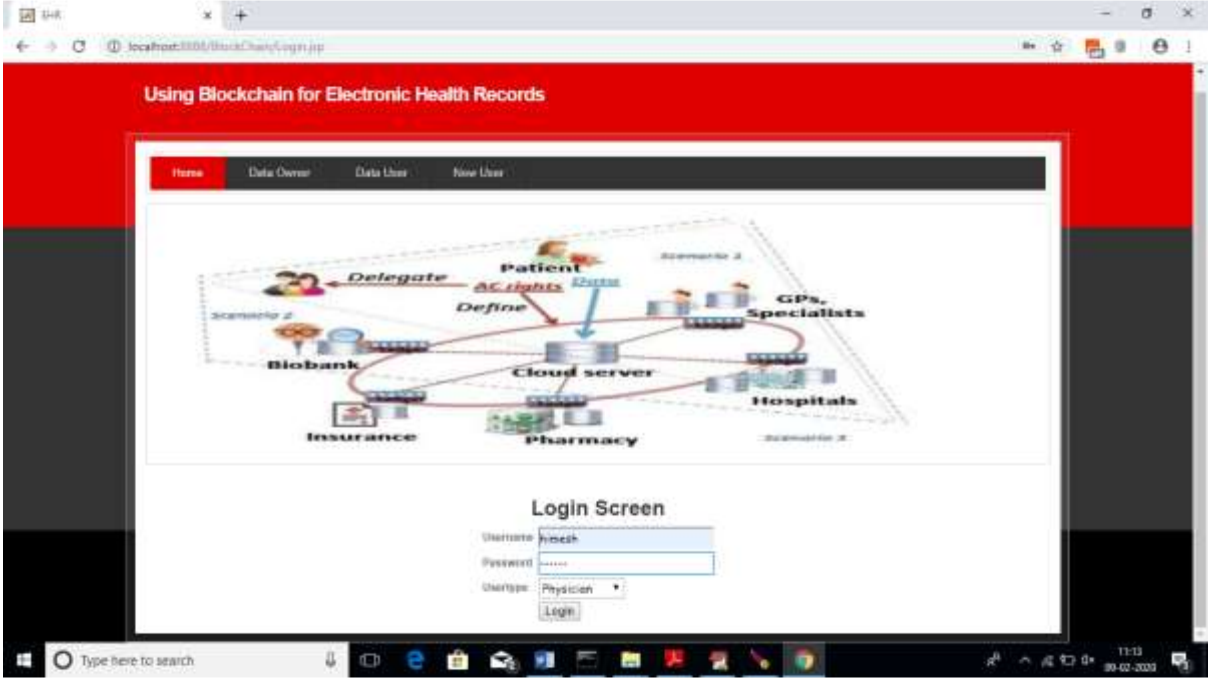


Abstract-Blockchain have been an interesting research area for a long time and the benefits it provides have been used by a number of various industries. Similarly, the healthcare sector stands to benefit immensely from the blockchain technology due to security, privacy, confidentiality and decentralization. Nevertheless, the Electronic Health Record (EHR) systems face problems regarding data security, integrity and management.

In this paper, we discuss how the blockchain technology can be used to transform the EHR systems and could be a solution of these issues. We present a framework that could be used for the implementation of blockchain technology in healthcare sector for EHR. The aim of our proposed framework is firstly to implement blockchain technology for EHR and secondly to provide secure storage of electronic records by defining granular access rules for the users of the proposed framework.

Fig 5.12 : DataUser selection link for doctor login

In above figure click on 'Data User' link to login as doctor



Login Screen

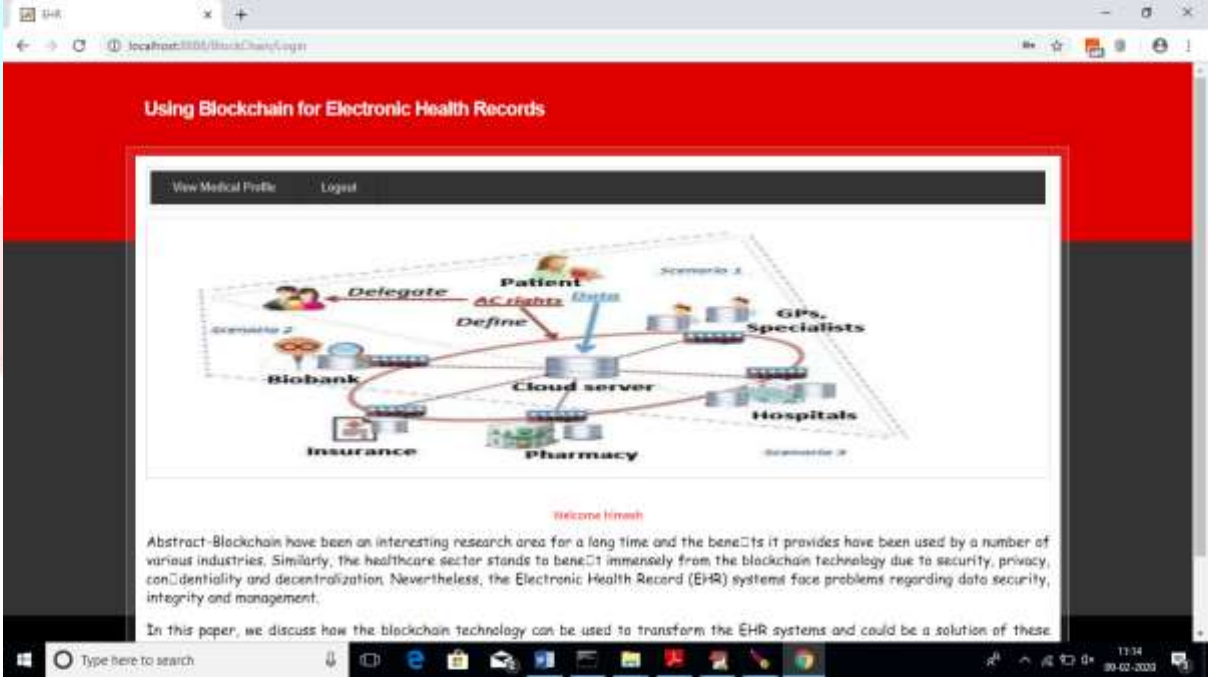
Username himesh

Password ......

Usertype Physician

Fig 5.13 : doctors login screen

In above figure I am login as doctor and after login will get below screen



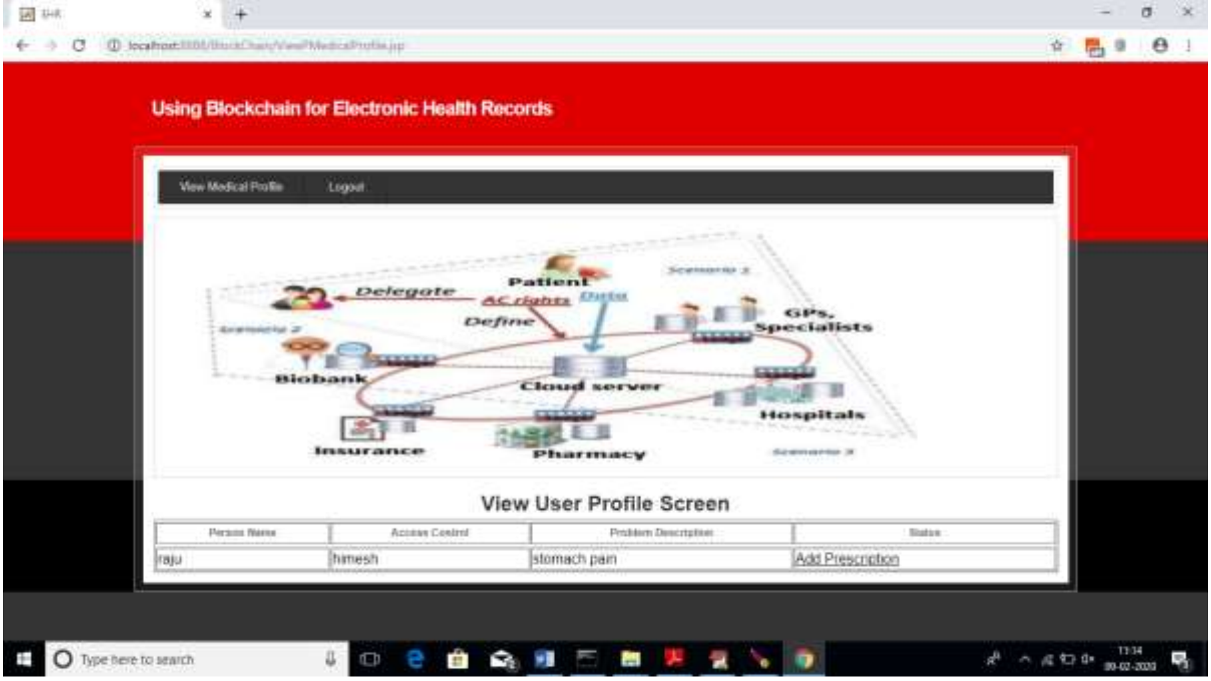
Welcome himesh

Abstract-Blockchain have been an interesting research area for a long time and the bene□ts it provides have been used by a number of various industries. Similarly, the healthcare sector stands to bene□t immensely from the blockchain technology due to security, privacy, con□dentiality and decentralization. Nevertheless, the Electronic Health Record (EHR) systems face problems regarding data security, integrity and management.

In this paper, we discuss how the blockchain technology can be used to transform the EHR systems and could be a solution of these

Fig 5.14 :welcome screen of doctor

In above figure click on ‘View Medical Profile’ link to get all patient records

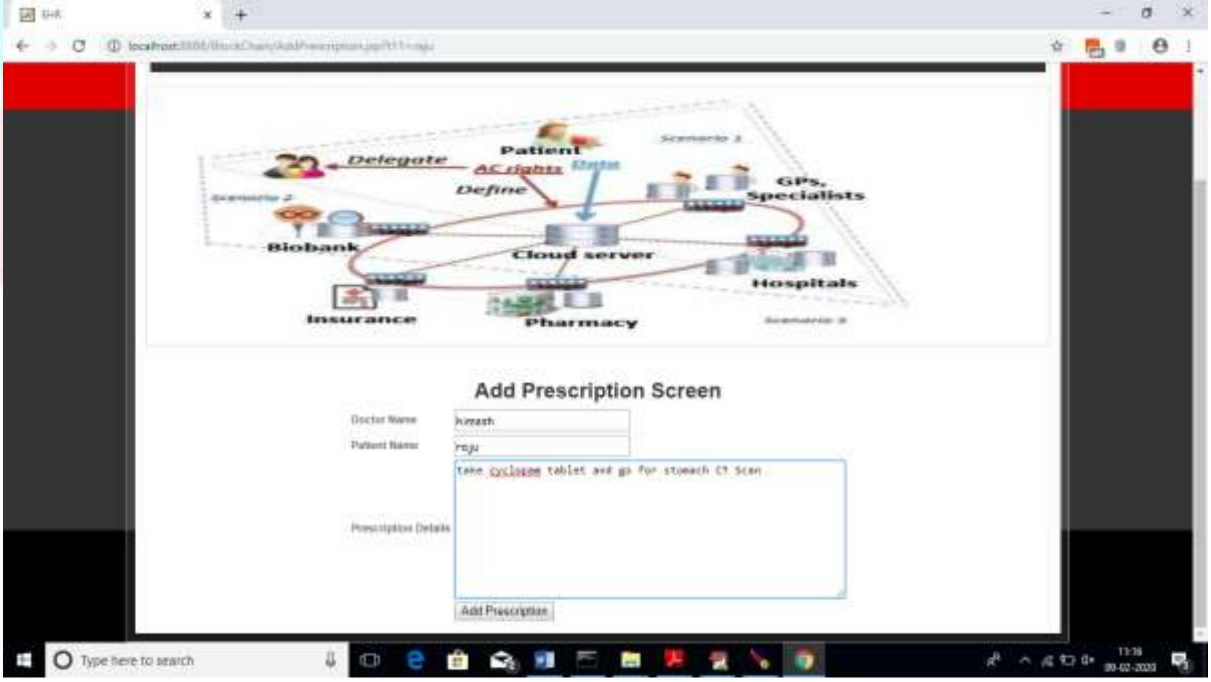


View User Profile Screen

Person Name	Access Control	Problem Description	Status
raju	himesh	stomach pain	Add Prescription

Fig 5.15 :doctor can view patient details and add prescription

In above figure doctor will click on ‘Add Prescription’ link to give prescription to patient. After clicking on ‘Add Prescription’ link will get below figure



Add Prescription Screen

Doctor Name: himesh

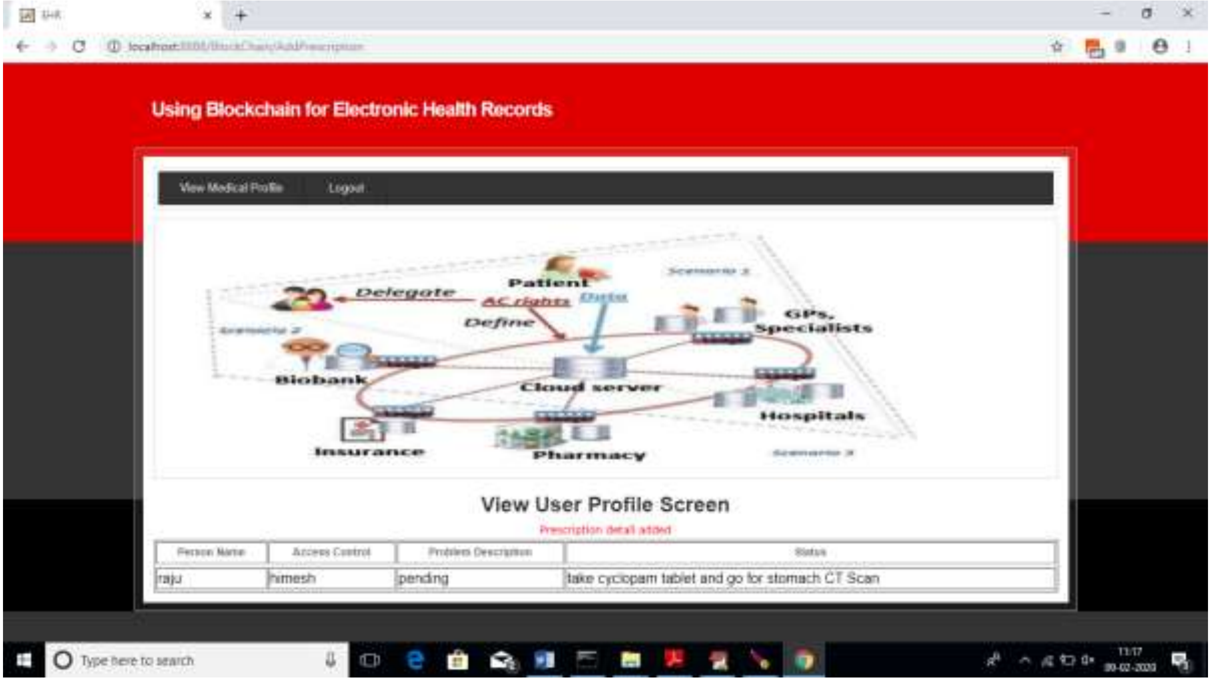
Patient Name: raju

Prescription Details: take cyclopam tablet and go for stomach CT Scan

Add Prescription

Fig 5.16 : Adding prescription

In above figure doctor added some prescription and patient can login and see that prescription.



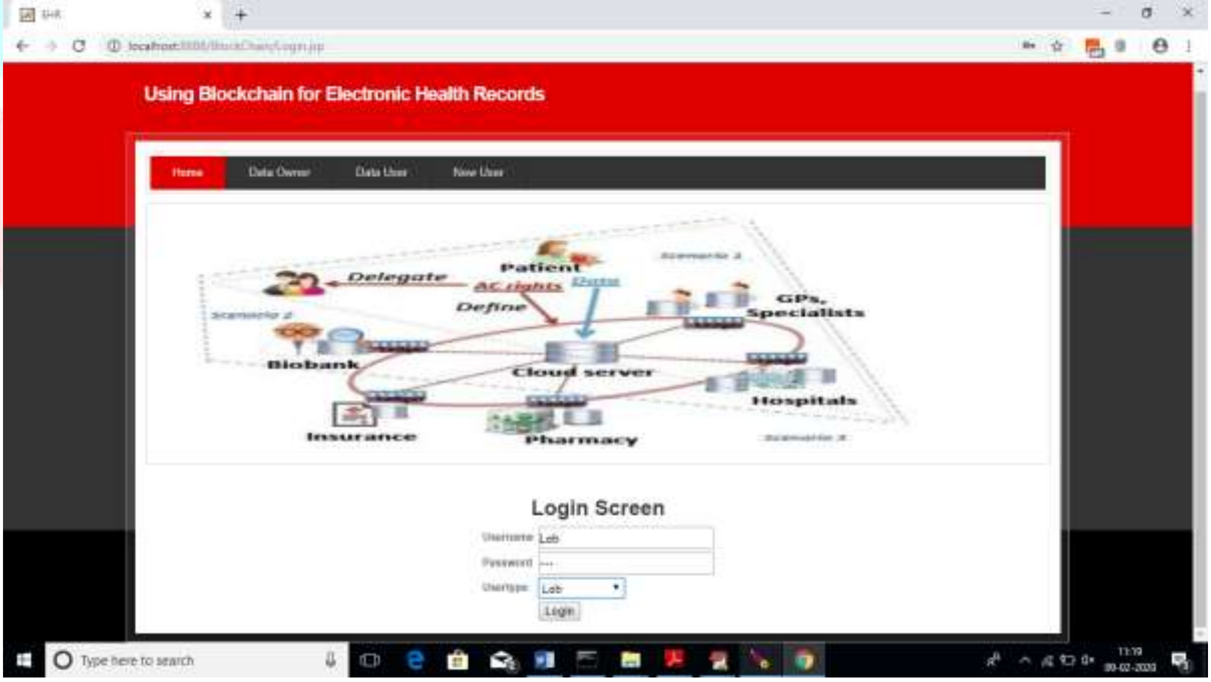
View User Profile Screen

Prescription detail added

Person Name	Access Control	Problem Description	Status
raju	himesh	pending	take cyclopam tablet and go for stomach CT Scan

Fig 5.17 : prescription added message for successful uploading

In above figure we can see status change to prescription from pending. Patient can view the prescription and go to lab for test. Now login as lab to upload report. Logout and click on 'Data User' link to get below figure



Login Screen

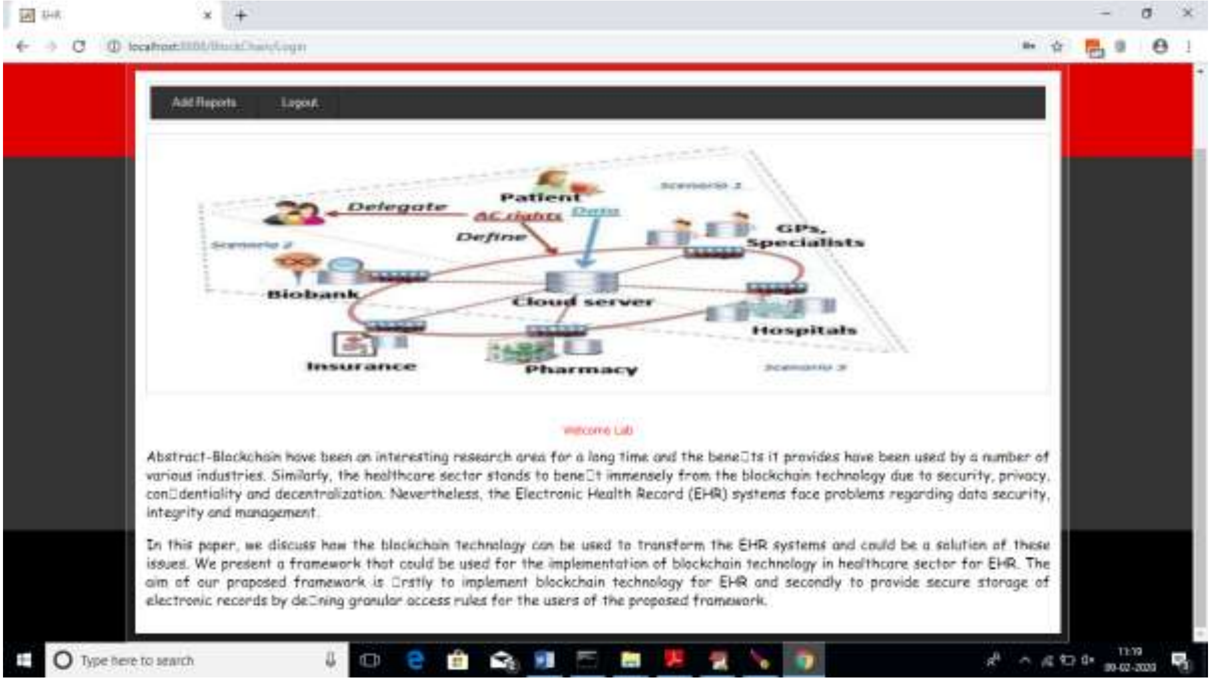
Username Lab

Password ···

Usertype Lab

Fig 5.18 : lab user login page

In above figure I am login as "Lab' user and after login will get below figure



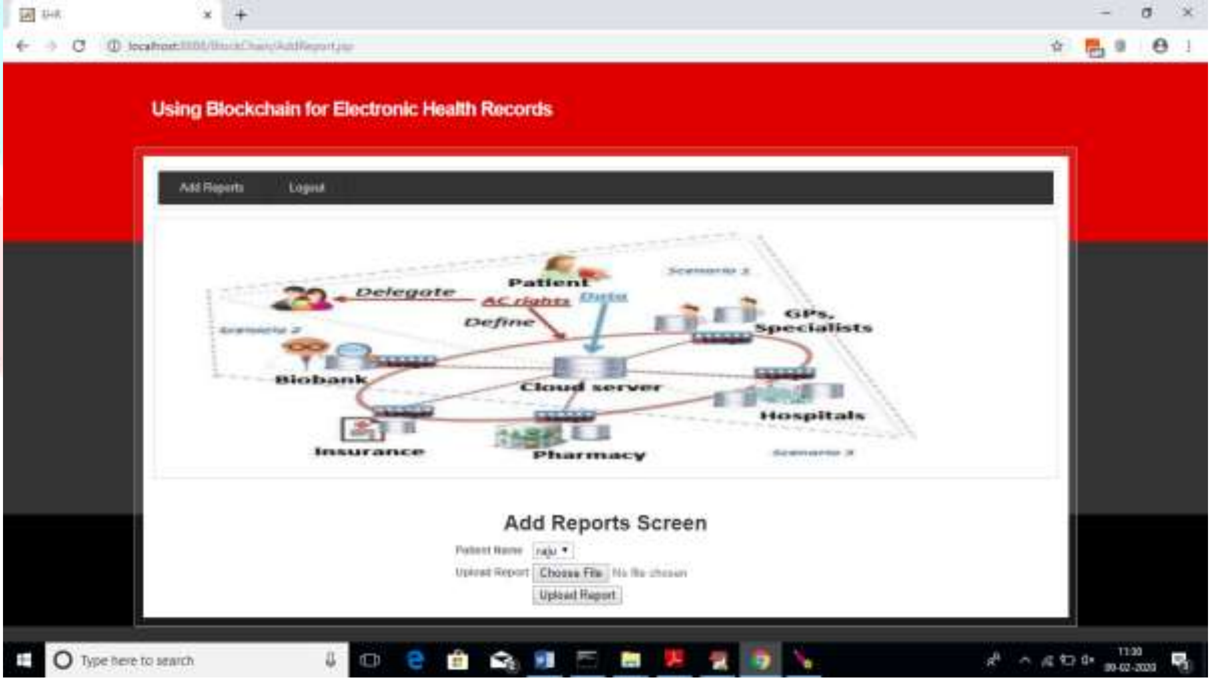
Welcome Lab

Abstract-Blockchain have been an interesting research area for a long time and the benefits it provides have been used by a number of various industries. Similarly, the healthcare sector stands to benefit immensely from the blockchain technology due to security, privacy, confidentiality and decentralization. Nevertheless, the Electronic Health Record (EHR) systems face problems regarding data security, integrity and management.

In this paper, we discuss how the blockchain technology can be used to transform the EHR systems and could be a solution of these issues. We present a framework that could be used for the implementation of blockchain technology in healthcare sector for EHR. The aim of our proposed framework is firstly to implement blockchain technology for EHR and secondly to provide secure storage of electronic records by defining granular access rules for the users of the proposed framework.

Fig 5.19:lab user welcome screen

In above figure click on ‘Add Reports’ link to get below figure



Using Blockchain for Electronic Health Records

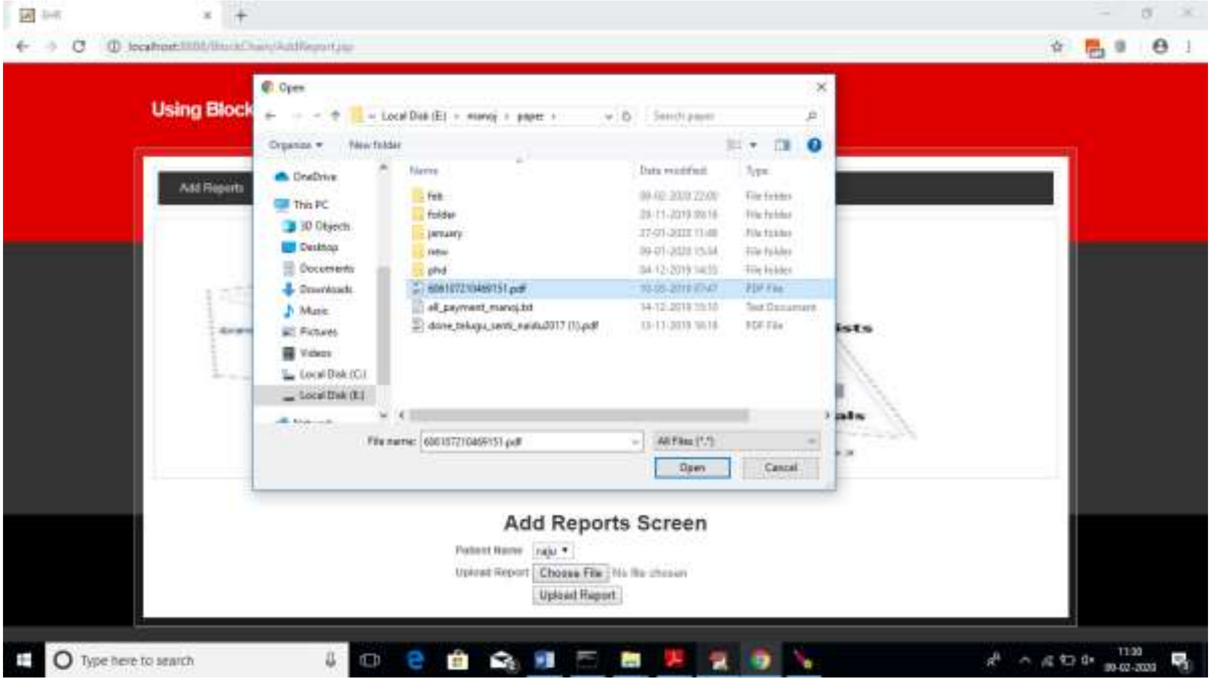
Add Reports Screen

Patient Name raju

Upload Report No file chosen

Fig 5.20 : adding reports by the lab user

In above screen lab person will select patient name and then upload report



Add Reports Screen

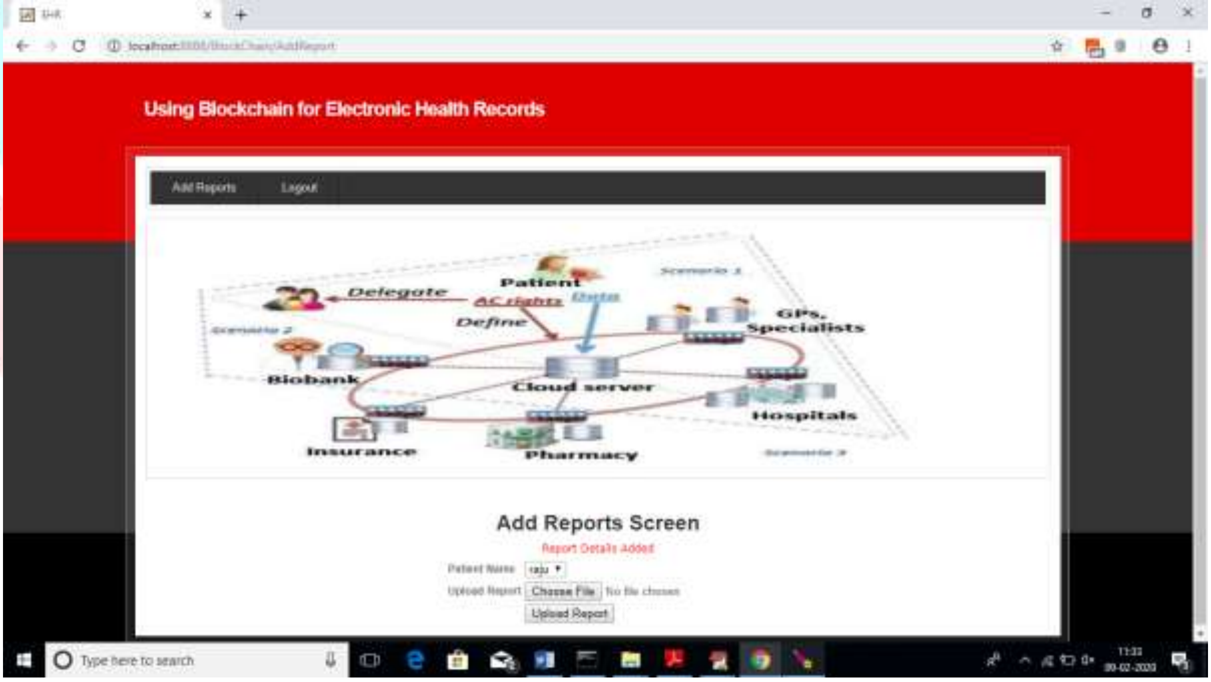
Patient Name raju

Upload Report Choose File No file chosen

Upload Report

Fig 5.21 : Uploading lab report

In above screen I am uploading one PDF file and you can upload any type of file and after upload will get below screen



Add Reports Screen

Report Details Added

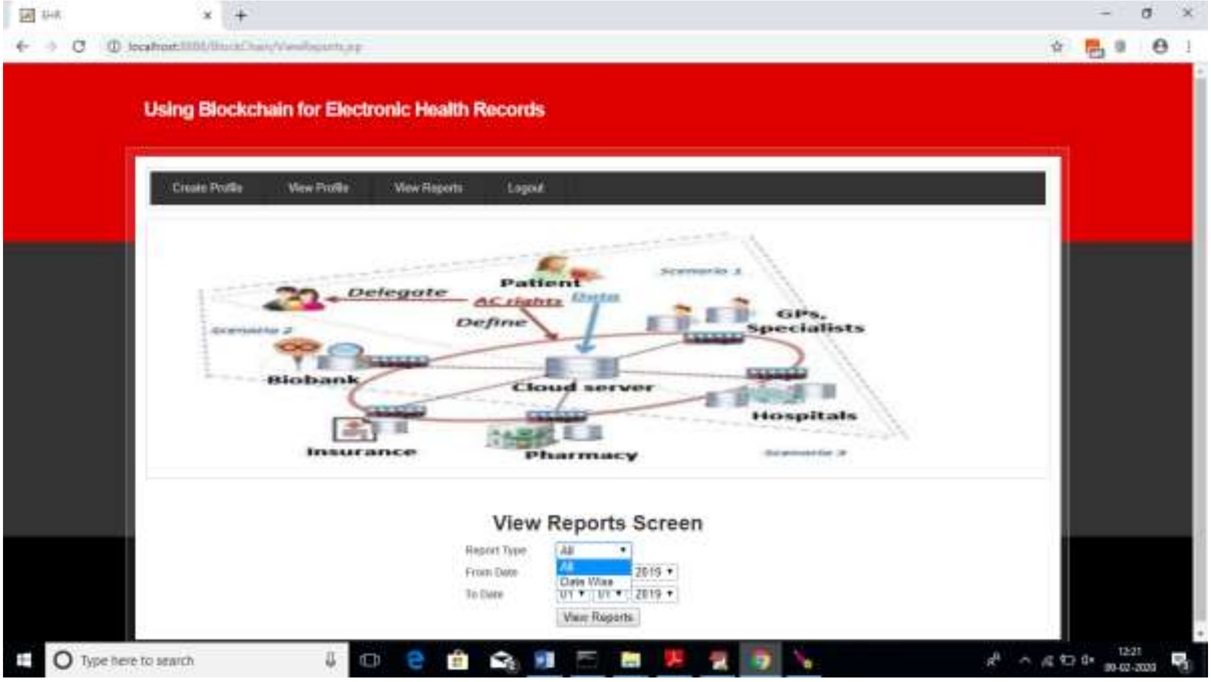
Patient Name raju

Upload Report Choose File No file chosen

Upload Report

Fig 5.22: Report added successfully message shown after uploading

In above screen we can see report details added and now patient can login by clicking ‘Data Owner’ link and access reports.



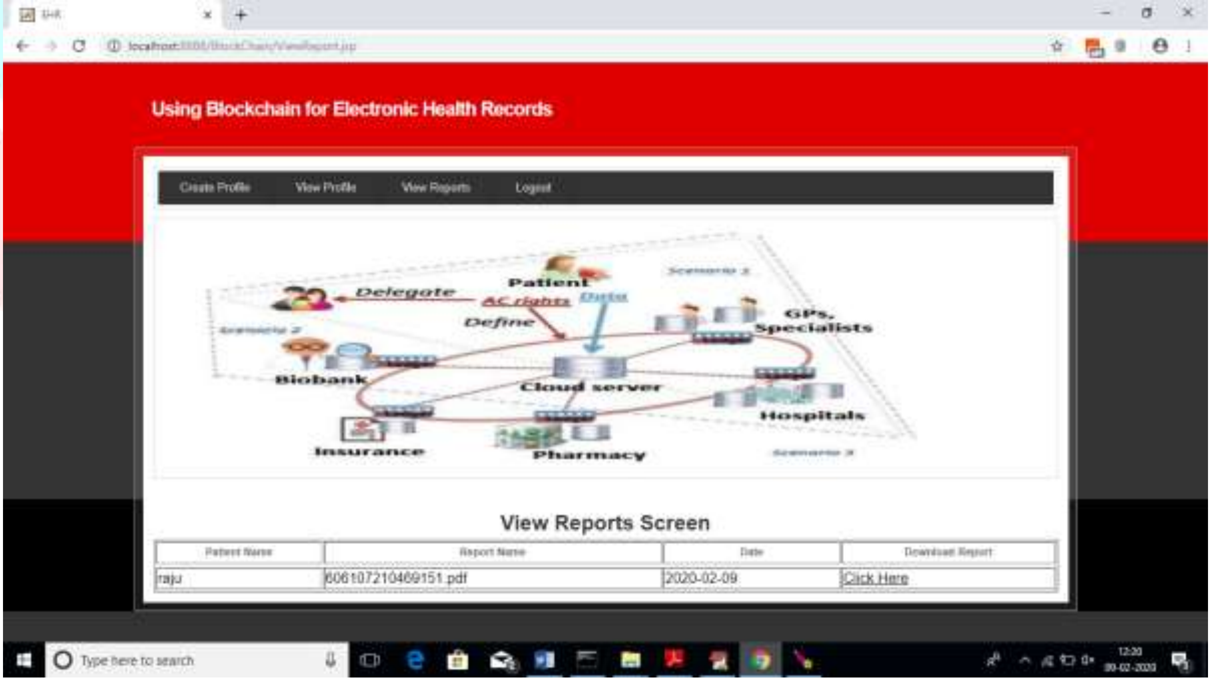
View Reports Screen

Report Type: All
All
Date Wise
From Date: 2019
To Date: 1/1 1/1 2019

View Reports

Fig 5.23 : view report of the patient

In above screen patient click on 'View Reports' link to get above screen and then select either option 'All' to get all reports or select from or to date option to select all reports between two date. After selecting 'All' Option user will get below screen upon click on 'View Reports' button

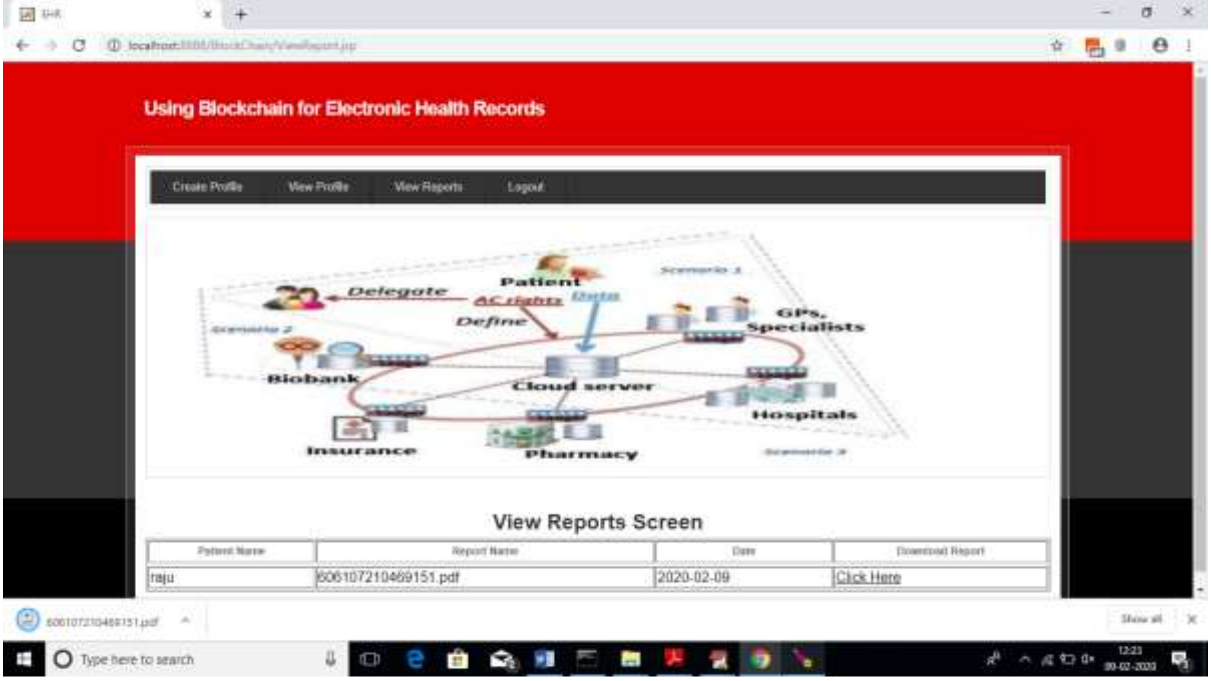


View Reports Screen

Patient Name	Report Name	Date	Download Report
raju	606107210469151.pdf	2020-02-09	Click Here

Fig 5.24 :View report screen

In above screen patient can click on 'Click Here' link to download report



View Reports Screen

Patient Name	Report Name	Date	Download Report
raju	606107210469151.pdf	2020-02-09	Click Here

Fig 5.25 : view reports screen downloaded the report

In above screen In browser status bar we can see file downloaded and similarly you can select date option and download files.

The section concludes with the successful experimental implementation of the concept. Finally the portal provides a secure scheme for patient data exchange.

V. CONCLUSION AND FUTURE ENHANCEMENT

Blockchain provides a tremendous potential of use in numerous industries, including healthcare. This technology has already become widespread within the monetary sector, but medical organizations still hesitate to implement it into their IT systems. This doesn't mean, however, that there are no healthcare companies currently using blockchain.

In this paper, I proposed a privacy-preserving scheme (Healthchain) for fine-grained access control of patient centric health data based on blockchain. We introduced two blockchains to ensure that both users' health data and doctors' diagnoses cannot be tampered to avoid medical disputes. We decoupled the encrypted data and the corresponding keys to achieve flexible key management. In addition, users can revoke the doctors at any time to ensure the privacy of the user. Implementation shows Healthchain is efficient and feasible in practice.

In future there can include data access from IoT Health devices so that a large number of data can be uploaded in the server and the performance evaluation can be done effectively.

REFERENCE

[1] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the internet of things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.

[2] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-things-based smart cities: Recent advances and challenges," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 16–24, 2017.

[3] L. Zhu, C. Zhang, C. Xu, X. Du, R. Xu, K. Sharif, and M. Guizani, "PRIF: A privacy-preserving interest-based forwarding scheme for social internet of vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2457–2466, 2018.

[4] S. Li, K. Xue, Q. Yang, and P. Hong, "PPMA: Privacypreserving multi-subset aggregation in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 462–471, 2018.

[5] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for IoT applications in smart homes," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1844–1852, 2017.

[6] A. Redondi, M. Chirico, L. Borsani, M. Cesana, and M. Tagliasacchi, "An integrated system based on wireless sensor networks for patient monitoring, localization and tracking," *Ad Hoc Networks*, vol. 11, no. 1, pp. 39–53, 2013.

[7] C. Zhang, L. Zhu, C. Xu, and R. Lu, "PPDP: An efficient and privacy-preserving disease prediction scheme in cloud-based e-Healthcare system," *Future Generation Computer Systems*, vol. 79, pp. 16–25, 2018.

[8] Z. Guan, Z. Lv, X. Du, L. Wu, and M. Guizani,

"Achieving data utility-privacy tradeoff in Internet of Medical Things: A machine learning approach," *Future Generation Computer Systems*, 2019.

[9] C. Zhang, L. Zhu, C. Xu, K. Sharif, X. Du, and

M. Guizani, "LPTD: Achieving lightweight and privacypreserving truth discovery in CIoT," *Future Generation Computer Systems*, vol. 90, pp. 175–184, 2019.

[10] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[11] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.

[12] N. Nizamuddin, H. R. Hasan, and K. Salah, "IPFSblockchain-based authenticity of online publications," in *International Conference on Blockchain*. Springer, 2018, pp. 199–212.

[13] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attributebased access control," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2130–2145, 2018.

[14] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.

[15] Y. Zhang, C. Xu, H. Li, K. Yang, J. Zhou, and

X. Lin, "HealthDep: An efficient and secure deduplication scheme for cloud-assisted ehealth systems," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4101–4112, 2018.

[16] J. Hua, H. Zhu, F. Wang, X. Liu, R. Lu, H. Li, and Y. Zhang, "CINEMA: Efficient and privacy-preserving online medical primary diagnosis with skyline query," *IEEE Internet of Things Journal*, 2018.

[17] K. Nikitin, E. Kokoris-Kogias, P. Jovanovic, N. Gailly, L. Gasser, I. Khoffi, J. Cappos, and B. Ford, "CHAINIAC: Proactive software-update transparency via collectively signed skipchains and verified builds," in *Proceedings of the 26th USENIX Security Symposium*. The Advanced Computing Systems Association, 2017, pp. 1271–1287.

[18] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing Bitcoin security and performance with strong consistency via collective signing," in *Proceedings of the 25th USENIX Security Symposium*. The Advanced Computing Systems Association, 2016, pp. 279–296.

[19] G. O. Karame, E. Androulaki, and S. Capkun, "Doublespending fast payments in Bitcoin," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 906–917.

[20] T. Ruffing, A. Kate, and D. Schroder, "Liar, Liar, Coins¨ on Fire!: Penalizing equivocation by loss of Bitcoins," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015, pp. 219–230.

[21] J. Chen, S. Yao, Q. Yuan, K. He, S. Ji, and R. Du,

"CertChain: Public and efficient certificate audit based on blockchain for TLS connections," in *Proceedings of the 37th IEEE International Conference on Computer Communications (INFOCOM '18)*.IEEE, 2018, pp. 2060–2068.

[22] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, 2018.

[23] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet of Things Journal*, 2018.

[24] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, 2018.

[25] Z. Shae and J. J. Tsai, "On the design of a blockchain platform for clinical trial and precision medicine," in *Proceedings of the 37th IEEE International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2017, pp. 1972–1980.