Organ Donation And Transplantation System Using Hashing Algorithm

S Syedali Fathima[1], Mrs. S.Mamitha,M.E.[2]
[1, 2] Dept of CSE
[1, 2] Stella Mary's College of Engineering

Abstract- *In the current era of smart cities and smart homes, the patient's data like name, personal details and disease description are highly insecure and violated most often. These details are stored digitally in a network called Electronic Health Record (EHR). The EHR can be useful for future medical researches to enhance patients' healthcare and the performance of clinical practices. These data cannot be accessible for the patients and their caretakers, but they are readily available for unauthorized external agencies and are easily breached by hackers. This creates an imbalance in data accessibility and security. This can be resolved by using blockchain technology. The blockchain creates an immutable ledger and makes the transaction to be decentralized. The blockchain has three key features namely Security, Transparency, and Decentralization. These key features make the system to be highly secured, prevent data manipulation, and can only be accessible by authorized persons. In this paper, a blockchain-based security framework has been proposed to secure the EHR and provide a safe way of accessing the clinical data of the patients for the patients and their caretakers, doctors, and insurance agents using cryptography and decentralization. The proposed system also maintains the balance between data accessibility and security. This paper also establishes how the proposed framework helps doctors, patients, caretakers, and external authorities to securely store and access patients' medical data in EHR.*

Keywords- Blockchain; electronic health record (EHR); storage; security; accessibility; cryptography; decentralization.

I. INTRODUCTION

Medical practitioners often remotely access data for patients requiring regular observation using Internet of Medical Things (IoMT). Relying on the weak security protocols of IoT devices for healthcare data exchange can result in patient's information leakage, information alteration during communication, and other privacy concerns, which can result in health and safety issues. Blockchain is a Distributed Ledger Technology (DLT) with each transaction stored in decentralised blocks replicated across different nodes. This avoids the security and data management issues of centralized storage of healthcare data, which can be vulnerable to external threats and has a single point-of-failure. However, this integration requires careful planning as the IoT devices have limited resources . Blockchain has revolutionised the way the data exchange takes place. Healthcare is a data intensive field and requires managing data for patient monitoring, clinical records and research, managing pharmaceuticals, and processing medical insurance claims.

The data management is facilitated through the immutable nature of blockchain, and these records can then be extracted and analysed through big data analysis for meaningful insights and decision-making . The patients' data has very high security and privacy requirements, and the blockchain application must comply with the General Data Protection Act (GDPR). Blockchain technologies can also provide data immutability, and trustworthy data between organisations. A blockchain, peer-to-peer (P2P) network, and digest chain, termed MedChain was proposed for efficient sharing of the healthcare data from IoT and wearable devices. An architecture for healthcare data sharing was proposed and a prototype implementation was developed with wearable devices for air quality sensors, Ethereum, IOTA distributed ledger and Tangle (a directed acyclic graph). A Hyperledger fabric-based solution was proposed for healthcare secure storage system to address the risks of data sharing and privacy leakage, allowing a fine-grained access to the stored data. A cloud-based environment of secure and privacy preserving data gathering and analysis from patient wearable devices was used to make the data available to doctors and insurance agents.

A survey of blockchain applications to ensure privacy and security of medical data in Electronic Health Records (EHR) systems highlighted the research opportunities in edge computing, machine learning, and big data for better integration of blockchain and EHR systems. The data interoperability is often required for the medical records where different entities, such as insurance companies, and other hospitals, require access to the data. A patient centric blockchain framework termed HealthChain was proposed for sharing of patients' health records. Similarly, a patientcentric architecture for data interoperability was considered highlighting the patient's consent in deciding the nature of the data to be shared with other stakeholders. A patient controlled system for health record exchange and communication can increase the participation of healthcare stakeholders in the development of patient-focused applications. The data sharing can also provide for associated incentives, and various incentivization schemes were considered for the data sharing on blockchain platforms. The healthcare industry is at a larger potential risk of severe cyberattacks than ever before. The healthcare data breaches reported to the Health and Human Services (HHS) Office for Civil Rights, between 2009 and 2021 had resulted in the impermissible disclosure, loss, and theft of 314,063,186 healthcare records. An average of 1.95 healthcare data breaches were reported each day in 2021. Blockchain technology may be used in conjunction with healthcare to boost the sector's capacity and protect the integrity and privacy of patients' information. The patients can also have access to their healthcare history and be aware of decisions affecting their health.

The benefits of using blockchain compared to conventional methods of healthcare database management systems, include decentralized management, and tamper-proof database records, while securing it from unauthorized users through encryption. The use of smart contracts, which are executable code scripts to be executed based on certain conditions, can help restrict access by thirdparties and intermediaries. Blockchain technology has a lot of applications in healthcare. Blockchain can be used for interoperable Electronic Health Records (EHRs) , healthcare asset management to keep track of the medical equipment , audit trail of pharmaceutical supplies health insurance claims and tracking diseases . One of the issues with blockchain technologies is that these tend to be complex and due to this usability could be a problem that can be addressed by providing simple interfaces to the user. Data management is an important area and has enormous improvement potential, however its most critical requirements are centred around data privacy and security. The focus of this paper is to investigate the use of blockchain technologies to facilitate the secure sharing of healthcare data through the implementation of a prototype application. To the best of our knowledge this is the first use of Substrate and Polkadot ecosystem for implementing secure data management solution for a healthcare application.

II. LITERATURE SURVEY

Organ donation being the most noble deed requires revolutionization. One cannot imagine the urgency and desperation a person feels when his/her loved one is in need of such act and they could not locate an appropriate donor. On the other hand, people who wish to donate worries about the privacy, security and authenticity. The Proposed System is a web-based Application which uses FIFO approach to select an organ donor for each genuine patient requiring a transplant and if there is an emergency case then the priority is given to that patient. It provides an efficient platform for potential organ doners and those who need the organs to connect. It uses Blockchain as its underlying Technology. Blockchain Technology is as it is known a decentralized and distributed network which stores records that are immutable as in cannot be altered once saved.

The organ donation system in the United States is centralized and difficult to audit by the general public. This centralized approach may lead to data integrity issues in the future. The Organ Procurement and Transplant Network (OPTN) was built and maintained by a non-governmental organization called the United Network for Organ Sharing (UNOS) under its proprietary UNetSM umbrella platform. This platform is made up of proprietary closed source software and does not provide the general public easy access to the organ transplant data for auditing. This study investigates the feasibility, challenges, and advantages of a blockchain-based OPTN. A prototype of a blockchain-based OPTN was created using the Hyperledger Fabric framework. The policies and guidelines issued by the United States Department of Health and Human Services for UNOS and the OPTN were used as the basis of this prototype. Four factors were identified to have a direct effect on the performance of this system, viz. max batch time out, max block size, endorsement policy, and transaction rate. Additionally, two variants of the blockchain chaincode were also developed.

WThis study proposes an approach to track unethically procured organs in particular in countries or regions where investigations cannot be performed by utilizing forensic DNA methodology. Using China as an example, previous research has concluded that organs in China are in part unethically and extra-legally procured (so called "forced organ harvesting") from living prisoners of conscience without consent. Using forensic DNA-analysis, propose building a DNA data bank from missing prisoners of conscience in China and comparing these results with DNA from donor organs in patients who received transplants in China. Biological materials collected in China will provide DNA directly or indirectly from potential victims of forced organ harvesting. Archival biopsies from transplant recipients’ donor organs will provide DNA profiles of donors. Verified match between DNA profiles of transplanted organs and missing victims will establish proof of such connection, thus provides evidence despite a lack of transparency.

Internet of Things have brought exciting changes in the social norms, work environments and the prospects for future generations. These devices (Things) have already changed the way our networks are used for communication. With the introduction of machine to machine communication (M2M), where devices communicate without human involvement to perform routine day to day tasks. These tasks on one hand, include services that provide convenience to the device owners such as setting off alarms, acting as personal assistant for reminders, keeping track of daily activities etc. On the other hand, there are certain tasks where these devices perform Transactions on behalf of the owners i.e. financial transactions/ online ordering etc. These transactional tasks have significant legal implications if some problem / dispute arises due to such action performed by these devices on behalf of the owners. To ensure that these interactions take place under observation of the owners and to keep track of their occurrence, there is a need to keep record of all such communication. Propose use of Blockchain for tracking all these transactions without compromising secrecy of data by keeping its integrity intact for medico-legal requirements and prevent risk of fraud.

In today's era of digitisation, many technologies have evolved that every manual work can be digitally automatized. In the digital automatizing process, security and privacy are the most important and highly demanding aspects. Blockchain offers many features that can be used in almost every sphere of life. Features like decentralisation, transparency, privacy makes it an extremely useful technology. Therefore, by making use of all these features, several problems in healthcare sector can be solved like removing complex network of third parties and lack of traceability of transactions. This paper presents a decentralised, secure and transparent organ and tissue transplant web application (also called DApp), which not only nullifies the role of any third party involved in the organ transplantation, but also is a cost effective solution that saves the patient's from high cost of transplantation.

III. PROPOSED SYSTEM

In this project, proposed blockchain technology may be used in conjunction with healthcare to boost the sector's capacity and protect the integrity and privacy of patients' information. The patients can also have access to their healthcare history and be aware of decisions affecting their health. The benefits of using blockchain compared to conventional methods of healthcare database management systems, include decentralized management, and tamper-proof database records, while securing it from unauthorized users through encryption. The use of smart contracts, which are executable code scripts to be executed based on certain conditions, can help restrict access by third parties and intermediaries. Blockchain technology has a lot of applications in healthcare. Blockchain can be used for interoperable Electronic Health Records (EHRs) , healthcare asset management to keep track of the medical equipment, audit trail of pharmaceutical supplies , health insurance claims , and tracking disease.

In our blockchain network, every device (cellphones, laptops, PCs) will act as a node and will be able to connect to the decentralized blockchain network using their public and private keys. In every blockchain system, an account consists of a set of public/private key pairs. Some of the nodes will be authority nodes that can assign public and private keys to any other node, to be used for joining the network. These public and private keys are generated using the Substrate's utility called Subkey. But since it was still in production phase, we also used Polkadot's extensions for this purpose. This is also important for block production and block finalization. After joining, a role-based sign-up determines the node authority, e.g., a doctor will sign up as a doctor, a patient as a patient, and all these nodes will have different authorities according to the assigned role. Every node in the blockchain will have restricted access to the data, that is, a doctor will be able to alter data only for his patients, and the patient will be able to view the altered data. Besides this, we also built an interface for medical equipment tracking.

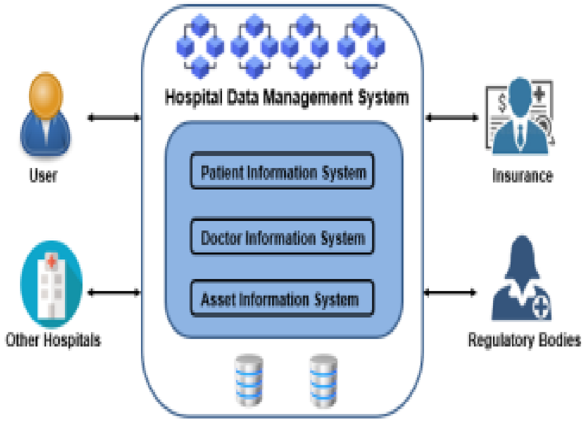

Hospital Data Management System
User
Insurance
Patient Information System
Doctor Information System
Asset Information System
Other Hospitals
Regulatory Bodies

Fig.1. System Architecture

First, the donor is examined by the hospital transplant team, and if the donor is deceased, a brain death test is performed. Meanwhile, if the donor is still alive, doctors examine the donor and ensure that the donor is fit for live donation. Then, all medical records are reported to the procurement organizer. The procurement organizer is responsible for evaluating the donor's condition to decide if he is a fit donor and ensuring that the donor is properly registered in the medical system. Next, if the evaluation shows that the donor is eligible for donation, the procurement organizer sends all the data to the organ transplantation organizer. This step can be performed only if the donor gives consent to donate to an anonymous person. After that, the matching process between the available donors and patients on the waiting list is performed by the organ transplantation organizer. As a result, a ranked list is generated as an output and provided to the transplantation surgeons. Next, the transplant surgeon decides whether the organ is appropriate for the patient based on various considerations, such as the donor's medical records and the current health of the prospective recipient. Later, when a transplant surgeon accepts the donated organ, the donor's surgeon is notified to remove the donated organ. Finally, the donated organ is trans ported to the patient's hospital and received by the transplant surgeon.

SYSTEM MODULES

- Blockchain Network Configuration
- Configuration through the Web Interface
- Creating a Blockchain based Healthcare Network
- Avoiding Runtime Upgrades
- Application Security

MODULE DESCRIPTION

Blockchain Network Configuration

For this purpose, a node-authorization pallet was created to manage a configurable set of nodes for a permissioned network. Each node is identified by a PeerId and each PeerId is owned by an AccountId that claims it. With this pallet, the following actions are possible: • Join the set of well-known nodes that allow connections. • Make another connection from a specific node. A node associated with a PeerId must have one and only one owner. If it is a normal node, any user can claim a PeerId as its owner. The owner of a node can then add and remove connections for that node. The connections between well-known nodes cannot be changed as these are always allowed to connect to each other. However, the connection between a well- known node and a normal node.

Configuration through the Web Interface

The developed web interface provides ease of access in interacting with the healthcare application using the React framework. We divided the whole application into modular components in React to mirror the application functionality, such as Hospital creation form, and Patient Registration form. We implemented a signup function using Polkadot's JS Apps extension. Using this, a user can generate unique private and public keys along with a mnemonic seed, to be securely kept by the user. For developmental purposes we set some default accounts in our blockchain named Alice, Bob, Dave, Eve, and Fredie. We built different pallets on Substrate to define the runtime logic of our blockchain node, for example, a pallet for patient registration, a pallet for doctor's registration, etc.

Creating a Blockchain based Healthcare Network

After creating the pallets, we can implement their traits, and the runtime logic of the chain so that the functionality of that pallet is available. The following pallets were built:

- Hospital Registration
- Patient/Doctor Registration
- Role Definition
- Healthcare Asset Registration
- Healthcare Asset Tracking

1) Hospital Registration: An authorized medical entity, for example, a hospital or any healthcare organization would register as a hospital and are subsequently able to add members to it. Each hospital would be allocated a specific and unique public address and only the authorized members will be able to modify the data.

2) Patient/Doctor Registration: After finalization, every transaction was stored in a block and an identifier for that block was generated. The identifier is called a hash and the record of transaction in that particular block can be traced using the given hash. The doctor registration interface was similar. We were able to register and store the data in the blockchain and the hash of that data was updated across all the nodes in the distributed ledger.

3) Role Definition: This feature in our blockchain is built on the Role-Based Access Control (RBAC) protocol, which is designed to manage access to resources based on user roles. It is a pallet that stores a record of roles and the users to which those roles are allotted by the authority node on the chain. This pallet allows an authority node to grant access to other users having different root privileges, for instance, balances pallet, which essentially provides functionality for handling accounts and balances, or democracy pallet, which handles the administration of general stakeholder voting. In the chain, Alice was pre-allocated the Execute permission on the RBAC pallet, which allowed Alice to use the RBAC pallet to create roles. Alice was also granted the Manage permission on a few other pallets, to bootstrap the blockchain.

4) Healthcare Asset Registration: Modern day healthcare facilities hold a lot of critical equipment and assets, comprising of patient monitors, mobile x-ray units, ECG monitors, ultrasound units and other diagnostic equipment. The availability of these assets needs to be ensured at the right place and the right time to ensure patients' health and safety.

5) Healthcare Asset Tracking: After the assets are registered, these can be tracked and traced. This interface keeps a detailed record of all the assets stored on the chain, and helps to maintain transparency, making the asset handling process foolproof.

Avoiding Runtime Upgrades

The most common method of updating a blockchain network is to replace the rules of the rudimentary protocol. This is mostly done to implement new features or modify the existing ones. If the runtime upgrade does not have compatibility with older versions, this will force the blockchain nodes to upgrade to continue participating to the newest version of the network. Nodes which do not update are not able to comprehend the new rules and features, and they would be discarded from the network, forming an alternative network. This problem can be solved by using the Substrate framework. With Substrate, if a block is produced and spread through the network, the blockchain nodes will be executing that block after performing various generic checks on it. Once the block is declared valid by the consensus mechanism, all the nodes in the chain would start to execute the blockchain state transitions it might contains. Thus, using forkless upgrade feature of Substrate, we were able to upgrade the runtime of our running healthcare blockchain network, without creating any forks of the chain.

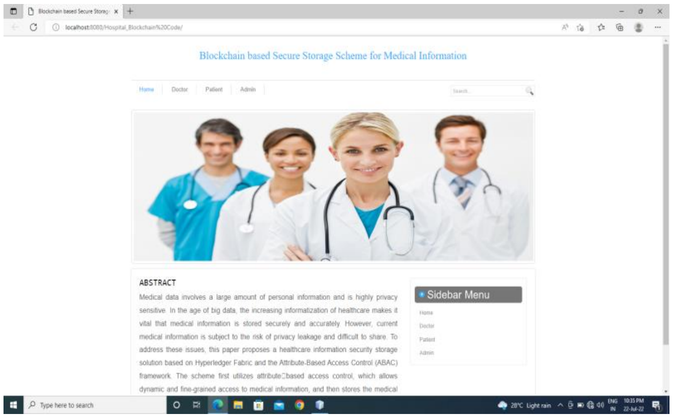
Application Security

1) Denial-of-service attacks: A denial-of-service (DoS) attack is primarily focused on temporarily making a network service unavailable to the users. This is a common attack type for the blockchain networks where an attacker makes many transactions to a targeted network node in an attempt to disrupt its operation and to make it unavailable to its users. We used the Proof of Authority (PoA) consensus mechanism to provide a safeguard against this attack. As authority nodes are preauthenticated in blockchain, block finalization rights are only given to nodes that are able to withstand a DoS attack. We conducted a comprehensive audit and stress test to evaluate the resilience of the Substrate based healthcare blockchain application against DoS attacks. The audit process involved a systematic examination of the application's security protocols and configurations, while the stress test was aimed to assess the system's ability to handle a high volume of transactions and requests.

2) 51% Attack: A 51% attack occurs when a malicious user in a blockchain network has more than 50% control over the blockchain, and can therefore alter the entire system. The attackers can stop the finalization and request for new transactions, and can also alter and rewrite blocks in a blockchain and even reverse the transactions. It is a common attack in the blockchains using the Proof of Work (PoW) consensus algorithm. We instead used Proof of Authority (PoA) consensus in our blockchain healthcare system. In PoA consensus mechanism, the 51% attack requires a malicious user or an attacker to gain control over 51% of nodes present in the network. Thus 51% attack is much harder for PoA network as compared to PoW network. However, for added protection, we used the concept of balances and transaction units. This helped to prevent bots and malicious users from spamming the blockchain network through spam transactions.

IV. RESULT AND DISCUSSION

4.1 SIMULATION OUTPUT

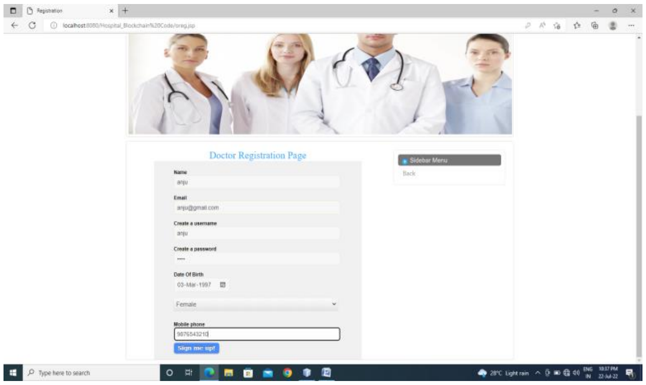


Blockchain based Secure Storage Scheme for Medical Information

ABSTRACT

Medical data involves a large amount of personal information and is highly privacy sensitive. In the age of big data, the increasing informatization of healthcare makes it vital that medical information is stored securely and accurately. However, current medical information is subject to the risk of privacy leakage and difficult to share. To address these issues, this paper proposes a healthcare information security storage solution based on Hyperledger Fabric and the Attribute-Based Access Control (ABAC) framework. The scheme first utilizes attribute□based access control, which allows dynamic and fine-grained access to medical information, and then stores the medical

Fig.2. Home Page



Doctor Registration Page

Name
anju

Email
anju@gmail.com

Create a username
anju

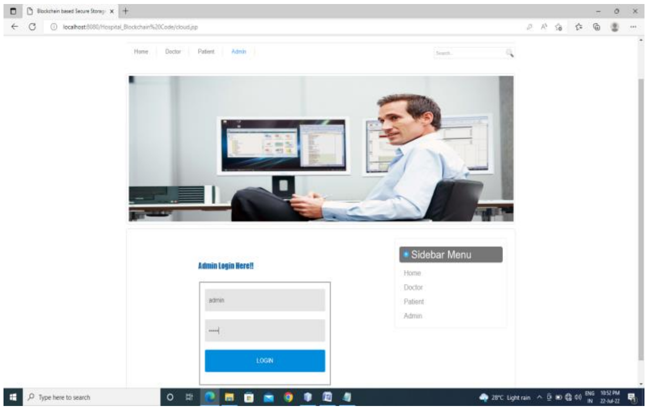
Create a password
····

Date Of Birth
03-Mar-1997

Female

Mobile phone
9876543210

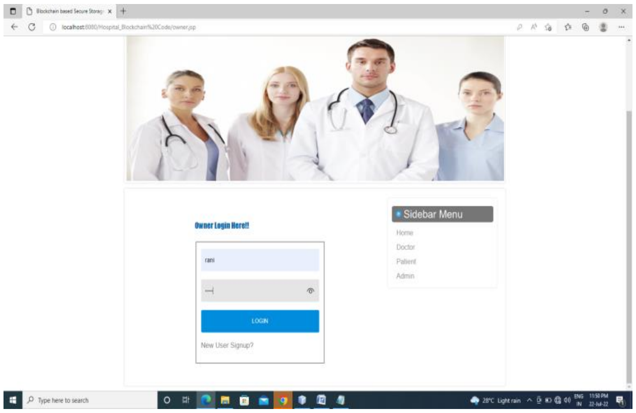
Fig.3. Doctor Registration Page



Admin Login Here!!

admin

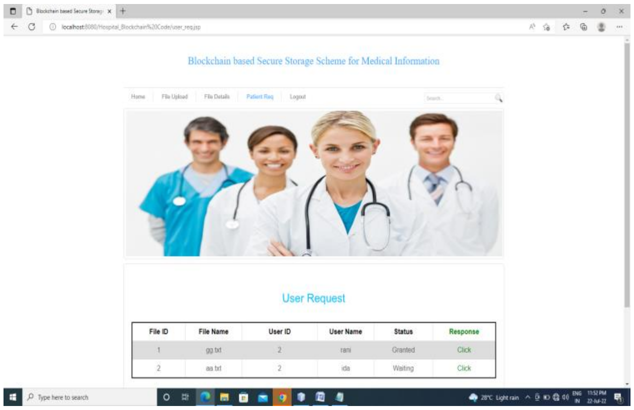
Fig.4. Admin login Page



Owner Login Here!!

rani

Fig.5. Owner Login Page

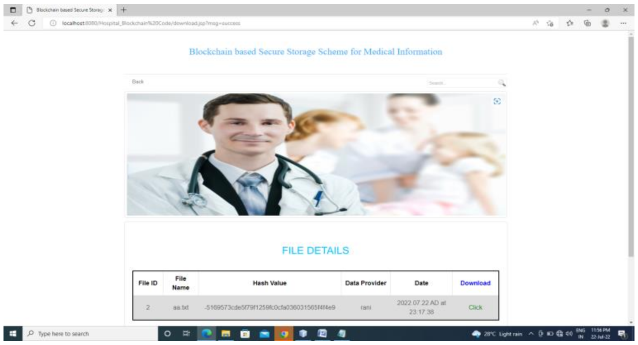


Blockchain based Secure Storage Scheme for Medical Information

User Request

File ID	File Name	User ID	User Name	Status	Response
1	gg.txt	2	rani	Granted	Click
2	aa.txt	2	ida	Waiting	Click

Fig.6. User Request

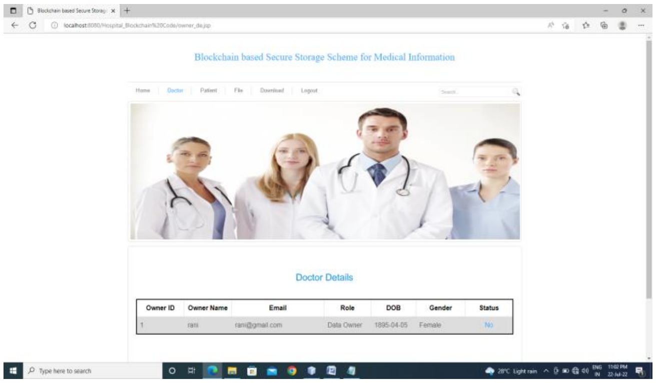


Blockchain based Secure Storage Scheme for Medical Information

FILE DETAILS

File ID	File Name	Hash Value	Data Provider	Date	Download
2	aa.txt	-5169573cde5f79f1259fc0cfa036031565f4f4e9	rani	2022.07.22 AD at 23:17:38	Click

Fig.7. File Details

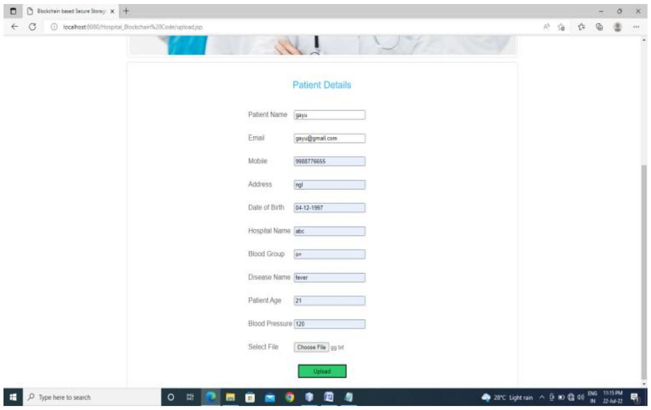


Blockchain based Secure Storage Scheme for Medical Information

Doctor Details

Owner ID	Owner Name	Email	Role	DOB	Gender	Status
1	rani	rani@gmail.com	Data Owner	1895-04-05	Female	No

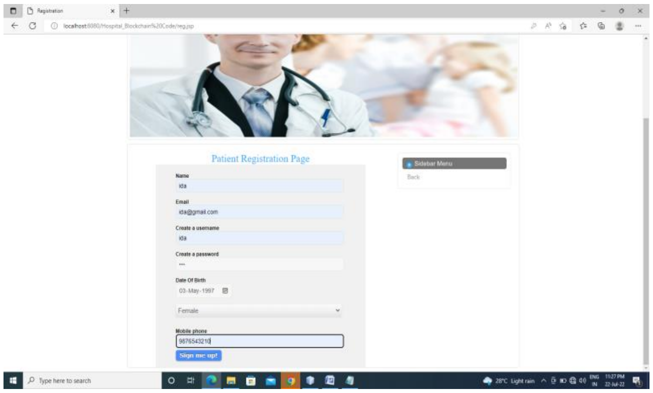
Fig.8. Doctor Details



Patient Details

Patient Name	gayu
Email	gayu@gmail.com
Mobile	9988776655
Address	ngl
Date of Birth	04-12-1997
Hospital Name	abc
Blood Group	o+
Disease Name	fever
Patient Age	21
Blood Pressure	120
Select File	gg.txt

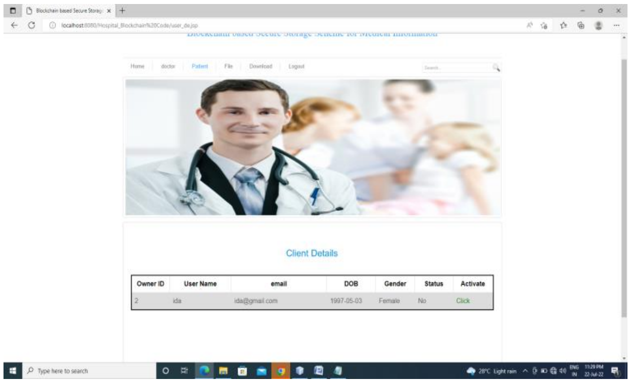
Fig.9. Patient Details



Patient Registration Page

Name	ida
Email	ida@gmail.com
Create a username	ida
Create a password	***
Date Of Birth	03-May-1997
	Female
Mobile phone	9876543210

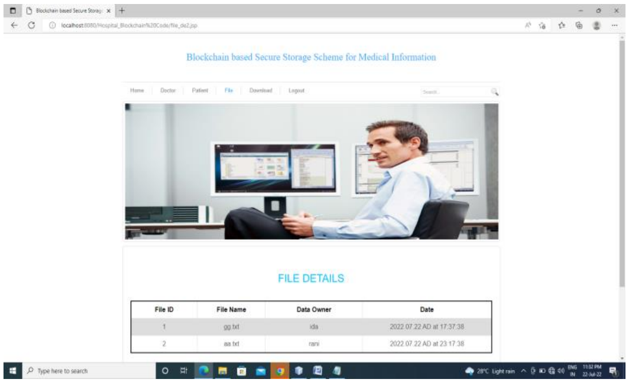
Fig.10. Patient Registration Page



Client Details

Owner ID	User Name	email	DOB	Gender	Status	Activate
2	ida	ida@gmail.com	1997-05-03	Female	No	Click

Fig.11. Client Details

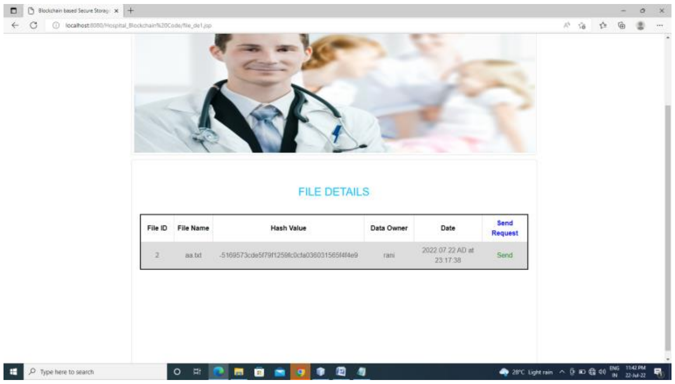


Blockchain based Secure Storage Scheme for Medical Information

FILE DETAILS

File ID	File Name	Data Owner	Date
1	gg.txt	ida	2022.07.22 AD at 17:37:38
2	aa.txt	rani	2022.07.22 AD at 23:17:38

Fig.12. Data owner details


Blockchain based Secure Storag
localhost:8080/Hospital_Blockchain%20Code/file_de1.jsp
Type here to search
28°C Light rain
ENG IN
11:42 PM 22-Jul-22

FILE DETAILS

File ID	File Name	Hash Value	Data Owner	Date	Send Request
2	aa.txt	-5169573cde5f79f1259fc0cfa036031565f4f4e9	rani	2022.07.22 AD at 23:17:38	Send

Fig.13. File Details

V. CONCLUSION

The blockchain technology can revolutionize the way data is managed, stored, and shared. The prototype blockchain-based healthcare data management system presented in this paper, was built on the Substrate framework. It demonstrates the potential of this technology in providing security, data reliability, traceability, and reduced server costs. The system includes features such as patient/doctor registration, healthcare asset registration and tracking, and role-based access control. The Proof of Authority consensus mechanism and protection methods against 51% and Denial of Service attacks further enhances the security of the system. The forkless upgrades, allow the system to be upgraded without compromising the data stored in the blockchain.

Overall, the prototype system presented in this paper provides a strong foundation for blockchain-based healthcare data management systems and opens up new possibilities for the future of healthcare.

REFERENCES

[1] Diana Hawashin , Raja Jayaraman , Khaled Salah "Blockchain-Based Management for Organ Donation Transplantation" and, https://ieeexplore.ieee.org/document/9787401 volume 10 June 8, 2022

[2] V. Puggioni. (Feb. 26, 2022). An Overview of the Blockchain Development Lifecycle. Cointelegraph. Accessed: Apr. 8, 2022.

[3] E. J. De Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," ACM Computing Surveys (CSUR), vol. 53, no. 2, pp. 1-27, Mar 2022.

[4] Z. Sun, D. Han, D. Li, X. Wang, C. C. Chang, and Z. Wu, "A blockchainbased secure storage scheme for medical information," EURASIP Journal on Wireless Communications and Networking, pp. 1-25, Dec 2022.

[5] V. Jaiman, L. Pernice, and V. Urovi, "User incentives for blockchainbased data sharing platforms," Plos one, vol. 17, no. 4, Apr. 2022.

[6] A. Soni and S. G. Kumar, ''Creating organ donation system with blockchain technology,'' Eur. J. Mol. Clin. Med., vol. 8, no. 3, pp. 2387–2395, Apr. 2021.

[7] Harvard Business Review. (Dec. 13, 2021). Electronic Health Records Can Improve the Organ Donation Process. Accessed: Apr. 8, 2022.

[8] A. O. Almagrabi, R. Ali, D. Alghazzawi, A. AlBarakati, and T. Khurshaid, "Blockchain-as-a-utility for next-generation healthcare internet of things," CMC-Computers Materials & Continua, vol. 68, no. 1, pp. 359-76, Jan 2021.

[9] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. BaniHani, "Blockchain smart contracts: Applications, challenges, and future trends," Peer-to-peer Networking and Applications," vol. 14, no. 5, pp. 2901-25, Sep 2021.

[10] Livemint. The Illegal Organ Trade Thrives in India-and it isn't Likely to End Soon. Accessed: Dec. 21, 2021.

[11] M. He, A. Corson, J. Russo, and T. Trey, ''Use of forensic DNA testing to trace unethical organ procurement and organ trafficking practices in regions that block transparent access to their transplant data,'' SSRN Electron. J., 2020.

[12] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K. K. Choo "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," Computers & security, Oct 2020.

[13] P. Ranjan, S. Srivastava, V. Gupta, S. Tapaswi, and N. Kumar, ''Decentralised and distributed system for organ/tissue donation and transplantation,'' in Proc. IEEE Conf. Inf. Commun. Technol., Dec. 2019.

[14] L. A. Dajim, S. A. Al-Farras, B. S. Al-Shahrani, A. A. Al-Zuraib, and R. M. Mathew, ''Organ donation decentralized application using blockchain technology,'' in Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS), May 2019.

[15] G. Alandjani, ‘‘Blockchain based auditable medical transaction scheme for organ transplant services,’’ Tech. Rep., 2019.

[16] M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, ‘‘A systematic review of the use of blockchain in healthcare,’’ Symmetry, vol. 10, no. 10, p. 470, Oct. 2018.

[17] M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, ‘‘A systematic review of the use of blockchain in healthcare,’’ Symmetry, vol. 10, no. 10, p. 470, Oct. 2018,

[18] N. Mattei, A. Saffidine, and T. Walsh, ‘‘Mechanisms for online organ matching,’’ in Proc. 26th Int. Joint Conf. Artif. Intell., Aug. 2017.

[19] S. Zouarhi, ‘‘Kidner-A worldwide decentralised matching system for kidney transplants,’’ J. Int. Soc. Telemed. E-Health, vol. 5, Apr. 2017.

[20] V. Ferraza, G. Oliveira, P. Viera-Marques, and R. Cruz-Correia, ‘‘Organs transplantation - How to improve the process ?’’ Eur. Fed. Med. Inform., Cardiff, U.K., Tech. Rep., 2011.