International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Blockchain Integrated IPFS-based System

Gajala Praveen [1*], Piyush Kumar Singh [2] and Prabhat Ranjan [3]

Submitted: 26/11/2023 **Revised:** 06/01/2024 **Accepted:** 16/01/2024

Abstract: The Data sharing is becoming more popular as a network technology. The management of electronic healthcare data has advanced in healthcare information systems. The information can be accessed at any time and from any location with patient-centric data. More social benefits, better healthcare, and fewer medical errors are all provided by e-healthcare. The global advancement of health and medical services is greatly impacted by the integration of blockchain technology and smart healthcare. Decentralization and quicker information access will make the medical system more effective. In this paper, we demonstrate how blockchain technology is being applied to the management and security of electronic health records in the healthcare sector. Secure healthcare systems have been established using a smart contract. On the ethereum blockchain, a smart contract has been developed to build secure healthcare systems. We conduct experiments in Interplanetary File System (IPFS) storage environments for a fully decentralized system that manages key generation for EHRs efficiently on the blockchain.

Keywords: *Blockchain, Smart Contracts, Secured health record, Information Sharing, Tamper-proof record management.*

1.Introduction

Blockchain technology opens up a world of possibilities for addressing difficulties in the healthcare industry. Blockchain technology could be one of the best methods for keeping track of electronic medical records (EMR) [1]. It assures that the patient records are authentic. When sharing healthcare data, the blockchain provides data integrity and patient privacy. Behind the patient-centric paradigm, the blockchain provides a trusted layer [2]. When blockchain records are employed in clinical research, the results will be precise and up to par. Blockchain technology would also be a good solution for money transactions such as insurance claims and bills. It aids in the elimination of important concerns such as claim duplications, manual errors, and pattern recognition. The Blockchain allows for the processing of financial data via smart contracts, which eliminate redundancies and inefficiencies in insurance claim administration [3]. Blockchain technology helps individuals, healthcare institutions, and healthcare providers overcome interoperability difficulties in the healthcare system. The public blockchain is used to regulate access to medical records. It offers scalability, data privacy, and access security. Every individual in the distributed healthcare blockchain network has access to a copy of everyone's record. As a result, an index is kept that contains information about records, such as their position and metadata. The process is simplified by the user's unique identity and access to the records [4]. Sharing data between healthcare organizations is difficult due to security and privacy concerns. Blockchain technology is frequently selected and used to secure data security and privacy efficiently. Data privacy has become a major topic of study as the extent of data exchange grows. Furthermore, when data is shared, it is often maintained by numerous parties, posing significant issues for protecting the privacy of this multi-party data. We employ blockchain to prohibit tampering with shared data, and the suggested approach allows for the trading of shared data while protecting transaction information. The fundamental goal is to ensure that data shared by various parties is kept private.

The amount of personal data is continually increasing as network technology advances [5]. The scalability and mobility of the cloud-based environment can provide several benefits [6-8], but there are some challenges to overcome [9]. Abuse, leakage, loss, or theft of EHR in cloud-based management systems can be exposed [10]. Health insurance and electronic health records are closely

[1,2,3] *Department of Computer Science, Central University of South Bihar, Gaya, India*

linked. Several cryptographic methods have been proposed to ensure the security of EHRs [11-14].

Data for e-Health systems can come from a variety of places, including clinics, hospitals, and pathologies. All patient data is maintained on a distributed ledger. Smart contracts, a core idea in blockchain, enable trustless features across multiple entities in the HER administration system [15]. In this paper, compared to traditional systems, blockchain technology uses a different platform.

Contribution of this work: The following contribution of this work:

(1) A novel architecture for integrating blockchain with IPFS-based EHR management systems has been proposed. Each component in the proposed architecture is discussed in terms of its functionality.
(2) We used an off chain scaling method that stores the data to address the scalability issue.
(3) EHR combined with ethereum blockchain platform, smart contract. To demonstrate the blockchain integration with IPFS-based EHR management systems, a prototype is created using the ethereum public blockchain.
(4) Front-end platform design and implementation for the EHR web portal.

Paper organization: The remainder of the paper is organized as follows: In the second section, a full analysis and discussion of the linked work of blockchain in healthcare are discussed. In Section 3, some preliminary concepts are introduced. Section 4 describes our proposed system design. The implementation details are presented in Section 5. The experimental outputs are discussed in section 6. This paper finishes with Section 7.

2. A Review of Blockchain Healthcare Applications

The research on blockchain-based techniques in healthcare is discussed in this section. Blockchain technology will reduce paperwork, costs, wait times, and overheads by delivering medical records that can be accessed from anywhere [16].

The MedRec [17] system does not keep track of patient's medical records. To store the record's signature, the system employs blockchain technology. The signature ensures that an original copy of the record is obtained.

Some scholars have proposed some solutions to overcome the problem of blockchain storage capacity. Zhang et al. [10] describe a blockchain-based safe and privacy-preserving PHI sharing (BSPP) approach for e-Health system diagnosis improvements. The PHI is stored on a private blockchain, while the safe indexes of the PHI are kept on a consortium blockchain.

Xia et al. [18] proposed Medshare as a solution to the problem of exchanging medical data. By utilizing blockchain technology for transaction authentication and verification, this startup aims to empower patients to have complete ownership over their data.

Yue et al. suggest a three-layered system [19], with a data usage layer, a data management layer, and a data storage layer. The private blockchain, according to this research, serves as a cloud.

The paper [20] uses a Merkle tree-based structure for blocks, which is comparable to Bitcoin's technique. They used Uniform Resource Locators (URLs) to refer to Fast Healthcare Interoperability Resources (FHIR).

[21] Proposes a key negotiation for blockchain key management methods. It creates a lightweight backup and recovery mechanism for health blockchain keys using body sensor networks.

The authors of [22] describe a patient-centric healthcare data management system that enforces privacy by using blockchain as storage. This research employs cryptographic methods to protect patient data and achieve pseudonymity.

MedChain is a technique proposed by Shen et al. [23] for sharing medical data using blockchain. They created this system to collect patient data from IoT sensors.

In Zhang et al.'s [24] work, they took some initial steps towards adopting blockchain technology for various healthcare use cases, as well as pointing out some of the challenges associated with its implementation.

Another article [25] describes Ethereum and blockchain as secure platforms for handling all types of sensitive data. A smart contract is a secure method of preventing third-party disruption.

The cloud services scenario is used by Xueping Liang et al. [26]. According to performance evaluation results, ProvChain provides security features for cloud storage systems, such as misleading provenance, consumer privacy, and minimal overhead reliability.

According to Mackey et al. [27], blockchain is being intensively investigated in the healthcare industry by several business stakeholders. It

reduces expenses and standardizes the entire process. They conducted a poll of several practitioners to learn more about blockchain conceptualization and application in healthcare facilities.

Blockchain technology has shown some promise in the healthcare field as a way to solve problems with data security, sharing, privacy, and storage [28, 29].

Ancile is a blockchain-based architecture for EHR management that employs smart contracts to offer patients ownership and control of their medical records. It securely limits document access.

The paper [30] presented another permissioned blockchain system for exchanging and maintaining cancer patients' medical records. A username/password method was used in the design of a membership service to authenticate registered users. Blockchain was used for EHRs, but it failed to satisfy expectations [31]. It was discovered that EHR systems had issues with reliability and user friendliness [32].

3. Preliminaries

The preliminary steps employed in the proposed architecture are formally described in this section.

3.1 Blockchain

The concept of blockchain was born on October 31, 2008, when Nakamoto published a white paper [33]. The blockchain establishes trust relationships among distributed nodes. Decentration, data timeliness, collaborative maintenance, programmability, security, and trust are all characteristics of blockchain [34]. Users can utilize the blockchain to develop powerful smart contracts and decentralized applications. For transactions to be completed and computed, blockchain technology in general follows specific consensus norms. The consensus algorithm adds the new block to the blockchain. Consensus techniques are chosen based on the application's requirements [35]. Blockchain offers a powerful abstraction for developing distributed protocols. To encrypt data, blockchain uses the asymmetric cryptography principle. Users can decipher the encrypted data. The cloud delivers encrypted data. The cloud can write and read data from the blockchain.

3.2 Ethereum

Ethereum is more than just a digital asset. Using smart contracts, it is a distributed platform that makes it easier to create decentralized applications. Turing-complete smart contracts are supported. It is extremely well-liked for developing decentralized apps based on smart contracts, like medical applications. It allows programmers to customize their blockchain [36]. When it comes to establishing a medical blockchain, it's important to estimate the cost involved. Gas is consumed during an EVM process. EVM Gas is an ether-based virtual fuel that drives the EVM. The gas needed for a transaction is a charge for running the transaction's code. The gas used during transaction execution is added to a miner's account. The ethereum blockchain charges some fees. The network miners determine the precise price of gas. They may refuse to accept the transaction. All of these actions on the EVM require gas for creation, deployment, and storage. Medical smart contracts have been compiled. Gas is a cost associated with running an operation on the ethereum network.

Ethereum became a fully distributed and decentralized computational system with the Ethereum Virtual Machine (EVM). It involves computing and data storage processes. The processing power used to execute transaction code, such as that for the cryptocurrency ether, is rewarded by miners [37, 38].

3.3 Smart Contract

The phrase "Smart Contracts" was coined for the first time by Nick Szabo [39]. They are computer programs that execute on their own when particular conditions in the system are met. They're utilized to transfer any form of value between peers in a blockchain without the need for a trusted third party [40, 41]. A smart contract is a contract with computerized computational logic. After fulfilling the program's logic, it automatically initiates transactions between parties. Smart contracts are designed to help with management and administration [42-44]. Clinical trials normally consist of a series of dependent phases that must be completed to obtain certain results. It will be invoked once network nodes have reached consensus [45, 46]. As a result, smart contracts may be able to keep track of and be transparent while giving people complete control over the processes involved.

Smart contracts are a set of instructions written in the Solidity, Go, or Vyper programming languages that are used to complete a specific task in the blockchain network. These little scripts are kept on each blockchain network's ledger and are called when a transaction or function needs to be

committed. As a result, the patient's information is kept secure.

3.4 Interplanatery File System (IPFS)

The IPFS protocol is a good option for storing important and sensitive data because of its safe storage technique. It is unique and is used for the identification of stored data files on the IPFS [47, 48]. IPFS makes use of cryptographic hashes that are kept in a decentralized manner via a peer-to-peer network. The created cryptographic hash could be stored on the decentralized application, reducing the number of computational processes on the blockchain. The IPFS protocol works as follows:

• IPFS files are assigned a unique cryptographic hash.
• On the IPFS network, duplicate files are not permitted.
• A network node stores the node's content and index information.

4. System Design of the Proposed Architecture

This section focuses on the framework aspects that determine how technology is used in healthcare. The proposed framework is implemented using three layers: the user layer, the blockchain layer, and the implementation layer, as shown in Figure 1.

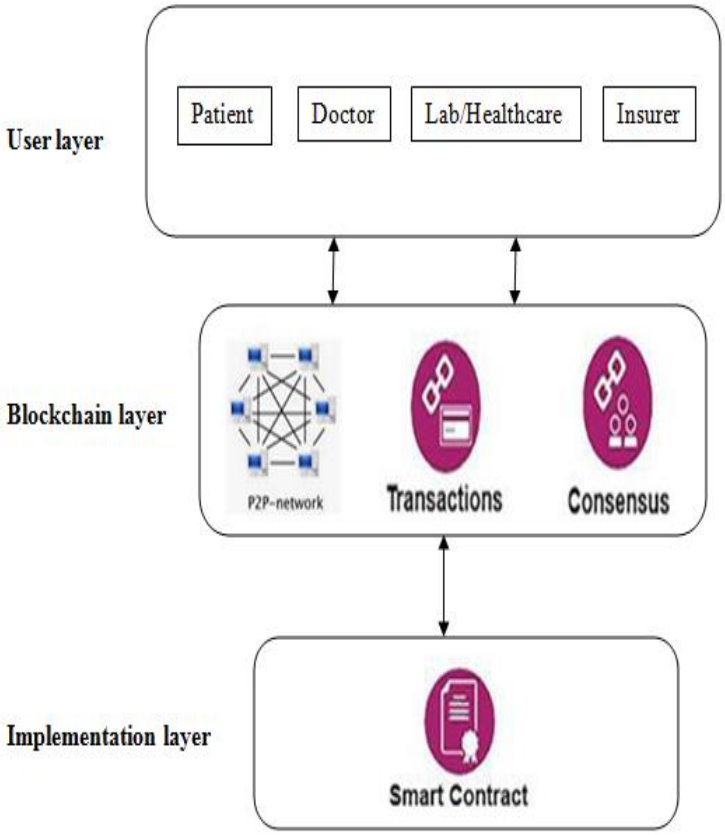

Fig 1 General System Design of the Proposed Framework

Users include patients, doctors, labs, and insurers. A user can be identified in the system by his role. A user can communicate with a blockchain-based DApp via the method included in the blockchain layer. The smart contract was used to implement the system. The processing of smart contracts is shown by an algorithm below.

Algorithm: Processing Algorithm for Smart Contract

```
Assign Roles for individual:
    Roles (New Role, New Account)
          Add new role and account in roles mapping
     End
Add Patient Record:
 Add (contains variables to add data)
   if (msg.sender = = doctor) then
       add data to particular patient's record
   else Abort session
  end if
  end

View Patient Record:
View (patient id)
if (msg.sender = = doctor || patient) then
   if (patient id) = = true then
    retrieve data from specified patient (id)
         return (patient record)
  else Abort session
 end if
end if
end

 Add lab Record:
  Add (contains variables to add data)
if (msg.sender = = lab) then
add lab report to particular patient's record
else Abort session
end if
end
Provide insurance:
Insurer (patient id)
if (msg.sender = = insurer) then
    if (patient id) = = true then
     Provide insurance to specified patient (id)
   else Abort session
 end if
end if
end
```

Our proposed architecture for an EHR management system based on blockchain is shown in Figure 2.

We specify the entities and activities to be performed in our blockchain-based storage. The administrator and User are the two main entities in the system. For our suggested structure, users are further separated into three categories: Doctor, Patient, and Insurer. The system administrator, who is a member of the hospital's administrative staff, assigns roles to these users. The suggested framework or system contains different modules. Our system will continue to function when these components are merged. Additional concepts that must be understood in these modules are described below.

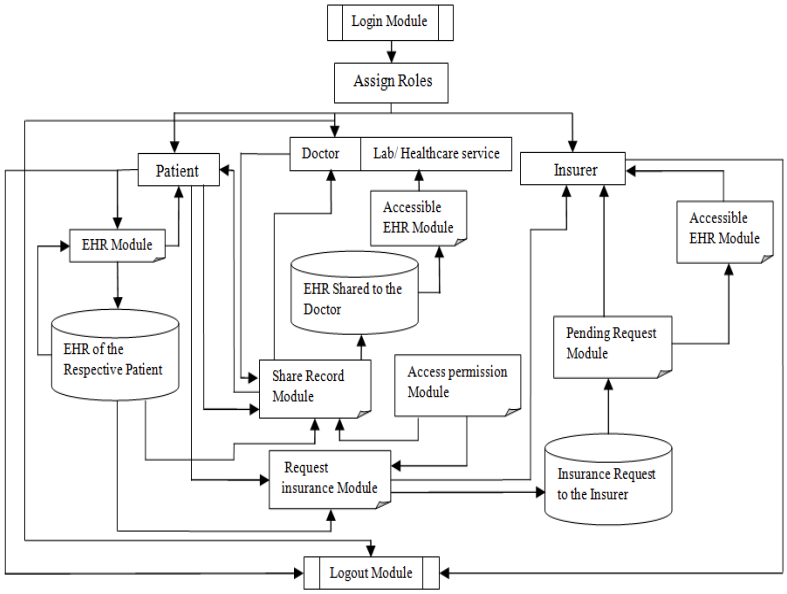

Fig 2 System Design of the Proposed Architecture

4.1 The Actor's Role:

The application logic for the framework is divided into three roles. The three are:

The Patient Role: A user who is registered as a patient has all their respective EHRs saved in IPFS. The user will be able to view their EHRs and can decide to share any of them with the doctor, healthcare provider, or insurer. Every user will also have the utility to 'unshare' their EHRs, essentially meaning that they will be able to remove the doctor's or insurer's access to their EHRs whenever necessary.

The Doctor/Healthcare Services Role: Users who register themselves as doctors can either send or receive EHRs from their patients. This would mean that the doctor role enables the users to issue EHRs or review the EHRs that are shared by the patient role user.

The Insurer Role: The insurer role enables users to view the EHRs shared by patients with them. They can decide whether or not they should provide insurance as per the request of the 'patients' based on their shared EHR. The insurer will also be shown a list of all pending requests through the EHRs that have not been reviewed.

4.2 System Architecture

The system focuses on the establishment of blockchain, user interfaces, and smart contracts. As shown in Figure 2, the research framework was built in three stages: login, different actor roles, and the logout stage. The first stage begins with the login module. The second stage involves categorizing and separating the different roles of healthcare providers that influence the use of blockchain in healthcare systems. In the final stage, all the users log out with the help of the logout module.

Figure 2 shows our system architecture. Entities in our architecture are as follows:

Login/Register: The architecture of the framework begins with the login module. This module is responsible for differentiating the various roles users may want to log into the system. The roles would include patient, doctor, lab/health service, and insurer. All roles are discussed in the previous section. All user registries are linked to the user's Metamask account.

The Patient Portal: This part of the architecture handles the following modules:

(a) The EHR Module: This module is used to access the user's (here, patient's) EHRs from the IPFS. This would allow the users to view their history of EHRs that were issued to them and stored in the IPFS.

(b) The Share Record Module: This module allows users to share their EHRs for review with doctors or healthcare services. It also facilitates the storage of records in IPFS and the addition of the generated hash values through IPFS to the blockchain. The blockchain transaction is then handled by Metamask.

(c) The Request Insurance Module: This module lets the user request insurance from the insurer. When a request is made, the selected EHR is sent to the insurer for review.

(d) The Access Permission Module: The user can share their EHRs with doctors, healthcare services, or insurers via the 'Share Request' and 'Request

Insurance' modules. This module will let the user (here: the patient) revoke the permission of doctors, healthcare services, or insurers to view their EHRs.

The Doctor/Healthcare Portal: This part of the architecture lets the Doctor and Healthcare Service roles access their modules, which include:

(a) The Share Record Module: The same module as the patient portal. Let the user share EHRs with the selected patient, which are then stored in the IPFS. The hash value generated by IPFS is added to the blockchain. This blockchain transaction will be handled by Metamask.

(b) The Accessible EHR module: This allows the user (in this case, doctors or healthcare services) to view all of the EHRs that patients have shared with them and that are accessible to them.

The Insurer Portal: This part of the architecture lets the users who have the role of 'insurer' access their modules, which include:

(a) The Pending Request module: This module would allow the user (here: insurer) to view all the insurance requests made by the patients, which will remain pending unless the insurer decides to take action (i.e., decides to provide insurance or not) for the particular request or until the patient decides to revoke the insurer's access to the EHR.

(b) The Accessible EHR Module: When a patient files a request for insurance with an insurer, the patient is required to provide their EHR to the insurer. The EHR shared by the patient with the insurer will be accessible to the insurer through this module.

Logout: Users from all roles, with the help of the Logout functionality, will be able to log out of the blockchain network after finishing a session. This will reset the login credentials and require the user to log in again to use the services and connect to the blockchain network.

5. Implementation Details

The blockchain smart contract system has been used to create and implement several medical workflows. In contrast to other alternatives, our proposed framework uses the IPFS scaling technique to overcome the scalability challenge. Furthermore, Ethereum is employed to implement the proposed framework in its entirety.

5.1 Flow of the Application

A flow diagram of the application of doctor, insurer, and patient is shown in Figures 3, 4, and 5.

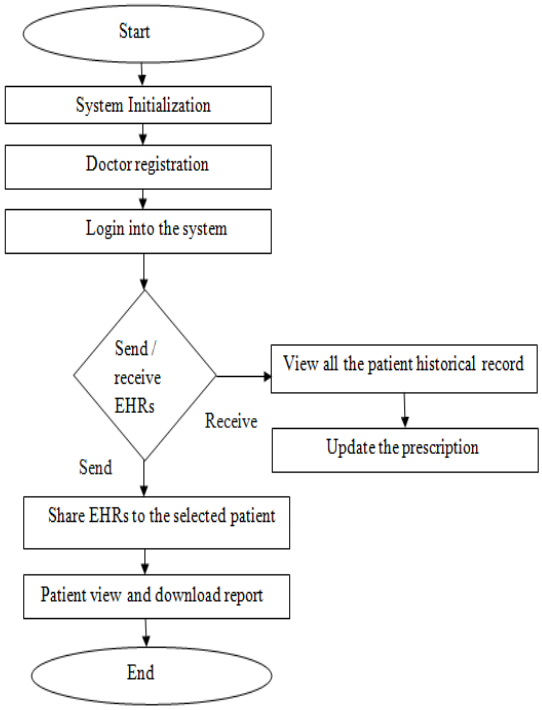

Fig 3 Flowchart of the doctor

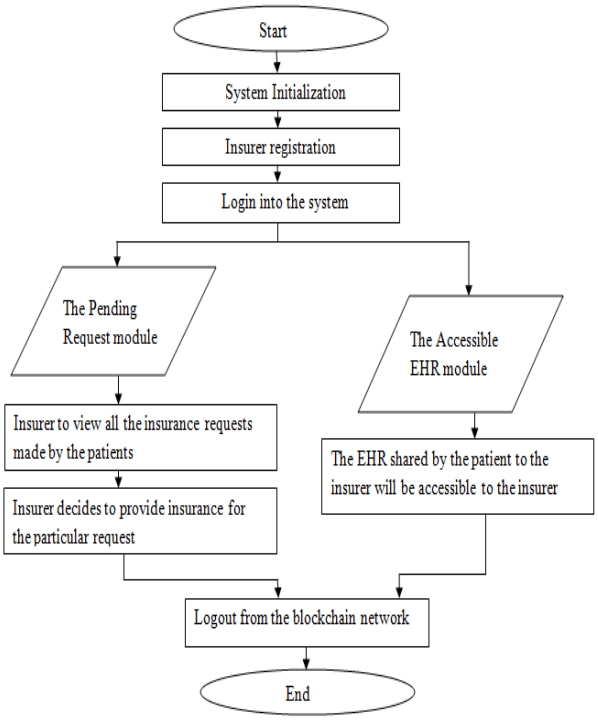

Fig 4 Flowchart of the Insurer dashboard.

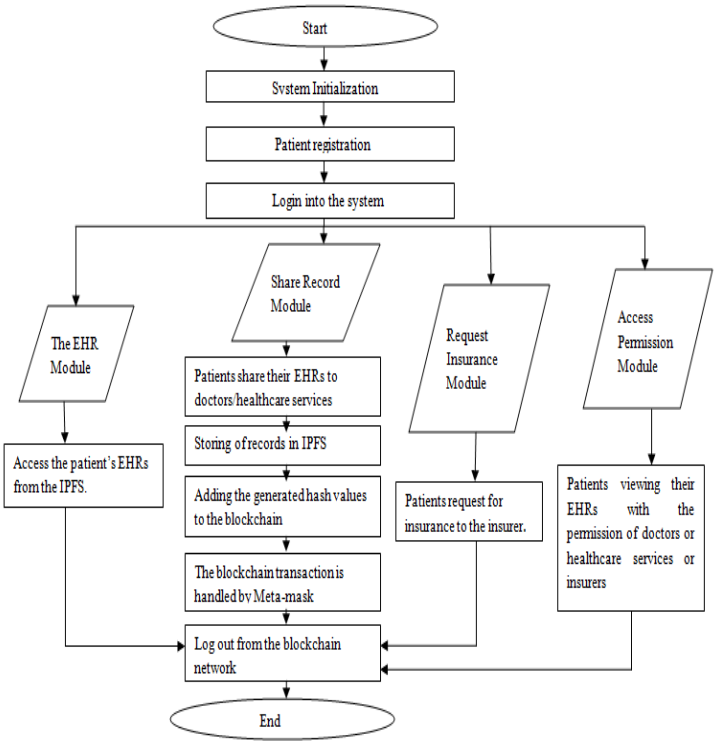

Fig 5 Flowchart of the patient

Our project consists of three parts: a client application, a blockchain, and a cloud-based EHR management system. The public blockchain platform we're using is ethereum. In place of the live blockchain, we use a local version of ethereum called Ganache. We use Windows 10 for configuring Ganache. We use web3js to interface with Ganache, which is a set of libraries for interacting with Ganache. To communicate with Ganache, Web3JS uses an HTTP or IPC

connection. Our smart contracts were built in Solidity, a programming language designed to work with the ethereum platform. Solidity is a computer language similar to JavaScript. Remix, an online text editor for Solidity, is used to write and compile smart contracts. The Metamask, a Google Chrome extension that should be enabled on the client system to communicate with the ethereum platform, is used to simulate the ethereum network.

We use HTML5 and JavaScript to create client applications. Java is used to create the cloud-based EHR management system. We have used IPFS for storage as our cloud database. Through the Web3 provider, HTML functions are linked to Solidity functions. The Web3 provider will be connected to an external ethereum node. In solidity, the contract is created and assembled. The user-supplied parameters are provided to the solidity function. The value can be retrieved and sent using Solidity's functions. The prerequisite environment must be selected before the contract produced in Solidity can be deployed. In the HTML program, the deployment address of the solidity file is added. As a result, a connection is made. An Application Binary Interface (ABI) is created by default for each contract generated in Solidity. As a result, the HTML software understands the structure of the contract. There are default accounts available in Solidity. It is also possible to create new accounts. Each account has a unique account address. An HTML application can be used to assign a specific account address. Only authorized doctors will be able to get information from the patient in this manner. Any other individual attempting to retrieve the content will be denied access since the address does not match.

An end-to-end transaction occurs if the connections are successful. No one in the middle could intercede and collect the contents. The blocks are constructed by default, and the remix IDE keeps track of transaction details. The details of the transaction are now visible in the user interface.

6. Output

This section shares implementation steps and a few screen scraps as shown in Figure 6-10. We are using the ethereum blockchain tool and a solidity-written smart contract to store information. Figure 2 depicts the overall workflow of our prototype development. Figure 6 shows the contract creation on the Ganache platform.

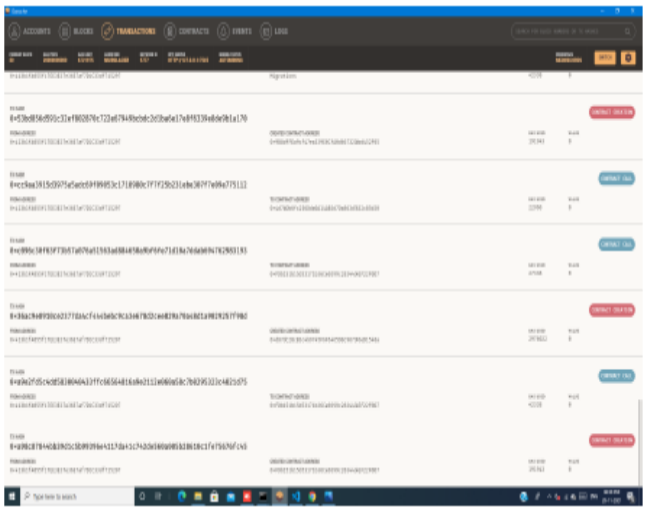

Fig 6 Contract Creation on the Ganache Platform

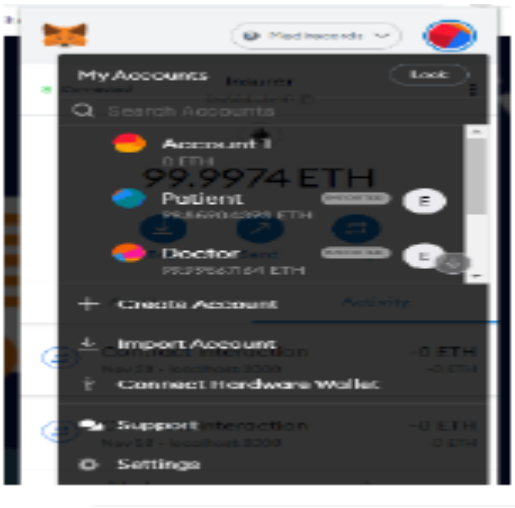

Fig 7 Ganache Interaction of Patient and Doctor with Metamask

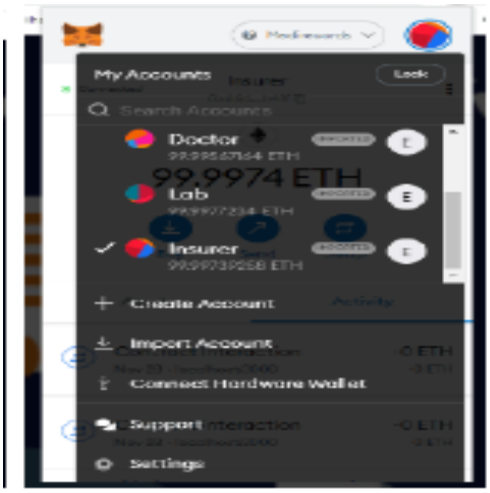

Fig 8 Ganache Interaction of Lab Person and Insurer with Metamask

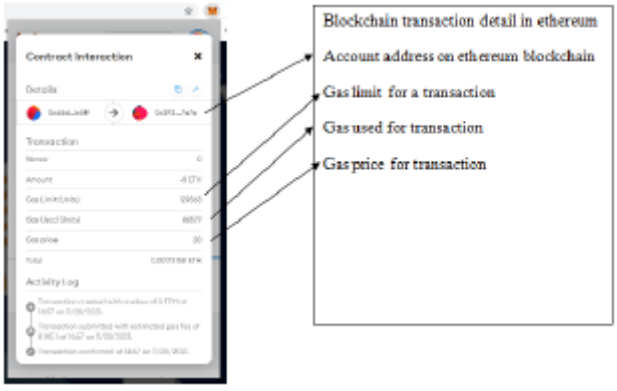

Fig 9 Blockchain transaction details in ethereum

On the DApp browser, users can view the entire proposed framework.

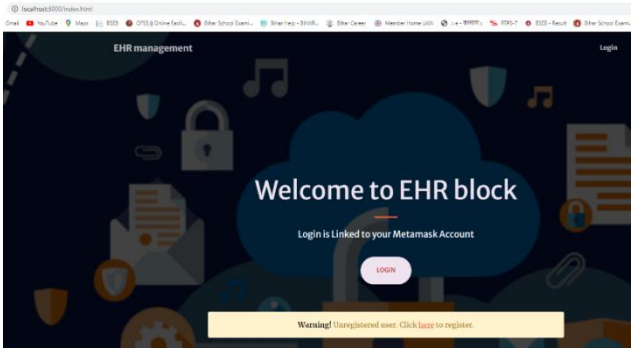

Fig 10: Web app index page loading

7. Conclusion

Patients find it difficult to obtain their medical records in traditional healthcare systems. The goal of new healthcare information technologies is to provide a pathway for the health industry. In the healthcare industry, data handling inefficiencies have been a problem. Many patients and healthcare practitioners are dissatisfied with the multiple obstacles that must be overcome to acquire current, real-time patient data. Patients frequently require their medical records to be updated. On the other hand, data privacy and security are in grave danger. To address this issue, a secure blockchain network has been established, to which only approved doctors and patients have access.

We present a novel approach to medical record management that uses smart contracts. Based on the needs from a medical perspective, we created a system for data management and sharing. This study gives a workable solution and implements it. This paper on code deployment is comprehensive and covers every part of the method and result. Finally, blockchain may be a viable option for safeguarding patient health information. This approach might be developed further in the future to create a complete blockchain-based healthcare system with more healthcare stakeholders.

References

[1] Esposito, C., Santis, A.D., Tortora, G., Chang, H., & Choo, K. (2018) 'Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?', IEEE Cloud Computing, Vol. 5, pp.31–37.

[2] Kish L.J, Topol E.J. (2015) 'Unpatients why patients should own their medical data', Nature Biotechnology, Vol. 33, No. 9, pp.921–924.

[3] Katuwal, G.J., Pandey, S., Hennessey, M., & Lamichhane, B. (2018) 'Applications of Blockchain in Healthcare: Current Landscape & Challenges', ArXiv, abs/1812.02776.

[4] Linn, L.A. and Koo M.B. (2016) 'Blockchain for health data and its potential use in health it and health care related research', InONC/NIST Use of Blockchain for Healthcare and Research Workshop, Gaithersburg, Maryland, United States: ONC/NIST, pp.1–10.

[5] Sharma S. (2016) 'Expanded cloud plumes hiding big data ecosystem', Future Generation Computer Systems, Vol. 59, No. C, pp.63–92.

[6] Chen, Y., Lu, J., & Jan, J. (2012) 'A Secure EHR System Based on Hybrid Clouds', Journal of Medical Systems, Vol. 36, No. 12, pp.3375–3384.

[7] Kuo A. M. (2011) 'Opportunities and challenges of cloud computing to improve health care services, Journal of Medical Internet Research, Vol. 13, No. 3, e67, https://doi.org/10.2196/jmir.1867

[8] Poulymenopoulou, M., Malamateniou, F., & Vassilacopoulos, G. (2012) 'Emergency healthcare process automation using mobile computing and cloud services', Journal of Medical Systems, Vol. 36, No. 5, pp.3233–3241.

[9] Anderson, N. R., Lee, E. S., Brockenbrough, J. S., Minie, M. E., Fuller, S., Brinkley, J., & Tarczy-Hornoch, P. (2007) 'Issues in biomedical research data management and analysis: needs and barriers', Journal of the American Medical Informatics Association: JAMIA, Vol. 14, No. 4, pp.478–488.

[10] Zhang, A., & Lin, X. (2018) 'Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain', Journal of Medical Systems, Vol. 42, No. 8, pp.1–18.

[11] Abbas, A., & Khan, S. U. (2014) 'A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds', IEEE Journal of Biomedical

and Health Informatics, Vol. 18, No. 4, pp.1431–1441.

[12] Shen, Q., Liang, X., Shen, X., Lin, X. and Luo, H. Y. (2014) 'Exploiting Geo-Distributed Clouds for an E-Health Monitoring System With Minimum Service Delay and Privacy Preservation', IEEE Journal of Biomedical and Health Informatics, Vol. 18, No. 2, pp.430–439.

[13] Yang, Y. and Ma, M. (2016) 'Conjunctive Keyword Search With Designated Tester and Timing Enabled Proxy Re-Encryption Function for E-Health Clouds', IEEE Transactions on Information Forensics and Security, Vol. 11, No. 4, pp.746–759.

[14] Zhou, J., Cao, Z., Dong, X., & Lin, X. (2015) 'PPDM: A Privacy-Preserving Protocol for Cloud-Assisted e-Healthcare Systems', IEEE Journal of Selected Topics in Signal Processing, Vol. 9, No. 7, pp.1332–1334.

[15] Wright, C.S., & Serguieva, A. (2017) 'Sustainable blockchain-enabled services: Smart contracts', IEEE International Conference on Big Data (Big Data), pp.4255–4264.

[16] Rabah, K. (2017) 'Challenges & opportunities for blockchain-powered healthcare systems: A review', Mara Research Journal of Medicine & Health Sciences, Vol. 1, No. 1, pp.45–52.

[17] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016) 'MedRec: Using Blockchain for Medical Data Access and Permission Management', International Conference on Open and Big Data (OBD), pp.25–30.

[18] Xia, Q., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X., & Guizani, M. (2017) 'MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain', IEEE Access, Vol. 5, pp.14757–14767.

[19] Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016) 'Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control', Journal of Medical Systems, Vol. 40, pp.1–8.

[20] Peterson, K.J., Deeduvanu, R., Kanjamala, P., & Mayo, K.B. (2016) 'A Blockchain-Based Approach to Health Information Exchange Networks'.

[21] Zhao, H., Zhang, Y., Peng, Y., & Xu, R. (2017) 'Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys', IEEE 13th International Symposium on Autonomous Decentralized System (ISADS), pp.229–234.

[22] Omar, A.A., Rahman, M.S., Basu, A., & Kiyomoto, S. (2017) 'MediBchain: A Blockchain-Based Privacy Preserving Platform for Healthcare Data', in International conference on security, privacy, and anonymity in computation, communication, and storage, Springer, 534–543.

[23] Shen, B., Guo, J., Yang, Y. (2019) 'MedChain: Efficient Healthcare Data Sharing via Blockchain', Applied Sciences, Vol. 9, No. 6.

[24] Zhang, P., White, J., Schmidt, D.C., & Lenz, G. (2017) 'Applying Software Patterns to Address Interoperability in Blockchain-based Healthcare Apps', ArXiv, Vol. abs/1706.03700.

[25] Stephen, R., Alex, A. (2018) 'A Review on BlockChain Security', Conference Series: Materials Science and Engineering; IOP Publishing, Vol. 396, No. 1, Available online: https://iopscience.iop.org/article/10.1088/1757-899X/396/1/012030/meta (accessed on 21 may 2022).

[26] Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., Njilla, L. (2017) 'Provchain: A blockchain-based data provenance architecture in the cloud environment with enhanced privacy and availability', in Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, Madrid, Spain, 14–17 May 2017.

[27] Mackey, T.K., Kuo, T.T., Gummadi, B., Clauson, K.A., Church, G., Grishin, D., Obbad, K., Barkovich, R., Palombini, M. (2019) ' 'Fit-for-purpose?'–Challenges and opportunities for applications of blockchain technology in the future of healthcare', BMC medicine, Vol. 17.

[28] Terry, M. (2009) 'Medical identity theft and telemedicine security', Telemedicine and e-Health, Vol. 15, No. 10, pp.928–933.

[29] Engelhardt, M. A. (2017) 'Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector', Technology Innovation Management Review, Vol. 7, No. 10.

[30] Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017) 'Secure and trustable electronic medical records sharing using blockchain', AMIA Annual Symposium Proceedings.

[31] Hochman, M. (2018) 'Electronic health records: A "Quadruple win," a "quadruple failure," or simply time for a reboot?', Journal of General Internal Medicine, Vol. 33, No. 4, pp.397–399.

[32] Vehko, T., HyppÃ¶nen, H., Puttonen, S., Kujala, S., Ketola, E., Tuukkanen, J., Aalto A. M., and Heponiemi, T. (2019) 'Experienced time pressure and stress: Electronic health records usability and information technology competence play a role',

BMC Medical Informatics and Decision Making, Vol. 19, No. 1.

[33] Nakamoto, S. (2008) 'Bitcoin: A Peer-To-Peer Electronic Cash System', [online] https://bitcoin.org/bitcoin.pdf (accessed 15 June 2021).

[34] Antonopoulos A M. (2014) 'Mastering Bitcoin: Unlocking Digital Crypto-Currencies', O'Reilly Media.

[35] Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D.T., Wang, P., Wen, Y., & Kim, D.I. (2019) 'A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks', IEEE Access, Vol. 7, pp.22328–22370.

[36] Gupta, S., & Sadoghi, M. (2019) 'Blockchain transaction processing', in Encyclopedia of Big Data Technologies, ArXiv, abs/2107.11592, pp.366–376.

[37] Chohan, U.W. (2017) "Cryptocurrencies: A Brief Thematic Review", IRPN: Innovation and Finance (Topic).

[38] Dannen C. (2017) 'Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners', Apress, ISBN: 9781484225356.

[39] Szabo, N. (1997) 'Formalizing and securing relationships on public networks', First Monday, Vol. 2, No. 9, [Online]. Available: https://firstmonday.org/ojs/index.php/fm/article/view/548

[40] Christidis, K.,&Devetsikiotis, M. (2016) 'Blockchains and Smart Contracts for the Internet of Things, IEEE Access, Vol. 4, pp.2292–2303.

[41] Atzei, N., Bartoletti, M., Cimoli, T., Lande, S. and Zunino, R. (2018) 'SoK: Unraveling bitcoin smart contracts', In book: Principles of Security and Trust, Thessaloniki, Greece, pp.217–242.

[42] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017) 'An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends', IEEE International Congress on Big Data (BigData Congress), pp.557–564.

[43] Mamoshina, P., Ojomoko, L., Yanovich, Y., Ostrovski, A., Botezatu, A., Prikhodko, P., Izumchenko, E., Aliper, A., Romantsov, K., Zhebrak, A., Ogu, I. O., & Zhavoronkov, A. (2017) 'Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare', Oncotarget, Vol. 9, No. 5, pp.5665–5690.

[44] Xia, Q., Sifah, E.B., Smahi, A., Amofa, S., & Zhang, X. (2017) 'BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments', Information, Vol. 8, No. 2.

[45] Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., & Hayajneh, T. (2018) 'Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring', Journal of Medical Systems, Vol. 42, pp.1–7.

[46] Benchoufi, M.,&Ravaud, P. (2017) 'Blockchain technology for improving clinical research quality', Trials, Vol. 18, No. 1.

[47] Dey, T., Jaiswal, S., Sunderkrishnan, S., & Katre, N. (2017) 'HealthSense: A medical use case of Internet of Things and blockchain', International Conference on Intelligent Sustainable Systems (ICISS), Vol. 9, No. 7, pp.486–491.

[48] InterPlanatery File System (IPFS), Accessed: march. 18, 2022, [Online]. Available: https://ipfs.io/.

Gajala Praveen is pursuing her PhD in the Department of Computer Science at the Central University of South Bihar, Gaya, India. She received her MTech degree in Computer Engineering from Jamia Millia Islamia (a central university), New Delhi, India. Her research interests include blockchain technology, natural language processing, and distributed computing. She has published research papers in international journals, conference proceedings, and book chapters. Email: gajalapraveen@cusb.ac.in

Piyush Kumar Singh is an Assistant Professor in the Department of Computer Science, Central University of South Bihar, Gaya, India. His research field interests are in image processing, wavelets, and blockchain technology. He has published research papers in national and international journals, conference proceedings, and book chapters. Email: piyush@cusb.ac.in

Prabhat Ranjan is an Assistant Professor in the Department of Computer Science, Central University of South Bihar, Gaya, India. His research field interests are in big data, distributed systems, software engineering, and blockchain technology. He has published research papers in national and international journals, conference proceedings, and book chapters. Email: prabhatranjan@cub.ac.in