BLOCKCHAIN BASED APPROACH FOR SECURING HEALTH CARE DATA

Roshini R
Computer Science Engineering
Reva University
rroshini3@gmail.com
Dr. Farooque Azam
Associate Professor, Computer Science Engineering
Farooque.azam@reva.edu.in
Ramya Bhat
Computer Science Engineering
Reva University
ramyabhat325@gmail.com
S Anusha
Computer Science Engineering
Reva University
sanusha12720@gmail.com
Ramya M
Computer Science Engineering
Reva University
ramyamanjunath5878@gmail.com

Abstract

For a long time, Blockchain has been an exciting research topic, and many firms have benefited from its benefits. Likewise, Blockchain technology offers a lot of potential in the healthcare sector because of privacy, confidentiality, decentralization and security, Nonetheless, Electronic Health Record (EHR) systems are plagued by worries about data security, integrity, privacy and administration. We address how Blockchain technology may be utilized to improve EHR systems and how it could be a solution to these problems in this paper. We present a patient centric approach for integrating Blockchain technology for electronic health records in the healthcare sector. Also, to offer secure storage of electronic records for users of the proposed framework by specifying granular access controls. This framework gives the EHR system the advantages of a Scalable, secure, and integrated blockchain-based system.

Keywords – Blockchain, Decentralization, EHR, Patient Centric, Privacy, Security.

I. INTRODUCTION

The development of technology these days is influencing every aspect of fast-changing human life, as well as the way we previously used and interpreted things. As technology changes, it can also be found in various other areas of life. The essential blessings that development in era is supplying are to enhance protection, person enjoy and different factors of healthcare sector. We are residing in a generation wherein we're producing fitness information at an unparalleled price and storing this information on paper is technically impossible. This brought about the creation of Electronic Health Records (EHRs) withinside the last few years. However, its blessings have by no means been nicely used by healthcare carriers because of loss of protection and interoperability. The information saved in hospitals and different associated company is liable to diverse protection threats along with unmarried factor of failure and traditional DDos attacks. Furthermore, it is unnecessary to store the same patient's records in several institutions when a single database may be used [1].

Electronic Health Records (EHRs) are located in multiple hospitals and administered by centralised cloud providers in current healthcare systems. However, it creates a point of failure because patients, the genuine owners of their EHRs, lose track of them. [6].

The most critical matter of the day is a comprehensive solution which is dependable, secure, confidentiality-preserving, and economical cloud storage that can withstand the turbulence of the fast developing digital storage technologies.

[7]. One of the factors of our motivation is security, another is obtaining relevant data out of patient's large medical record in less time. They do, however, have worries about medical information privacy and security, user data ownership, data veracity, and other issues. The comparison and analysis of the systems reveal a significant disparity, which is due to a lack of scalability [8]. Implementing a revolutionary technology like Blockchain might be the solution to these issues. This invention promises to make always maintaining healthcare records and other health-related information a breeze. The main goal is to create temper-proof, secure medical records that can be shared over multiple platforms. In other words, Blockchain technology allows transactions to be completed without the involvement of any third party. [14].

Hence, the major purpose of our proposed system is to establish a framework based on Blockchain for Electronic Health System which protects the integrity and security of the data. The rest of the paper is organised as follows. Related work is described in Section II. Section III describes the architecture. Our methodology is detailed in Section IV. The end result is Section V. Finally, this article is concluded, and future work is given in Section VI.

II. RELATED WORK

In [1], IPFS's off-chain scaling method is used to construct a Blockchain-based DApp using the Solidity programming language to provide secure record storage and precise record access controls for those records. This framework facilitates Improved Scalability, Content-Addressability, Integrity, Access Control, and Information Confidentiality. IPFS, on the other hand, uses transport - encryption rather than content encryption (which implies that data is protected when being transferred from one IPFS node to another, but

anyone with the Content Identifier can download and see it) (CID). which is not much appreciable when privacy of data is concerned.

In [2], a Blockchain-based architecture is developed using Hyperledger Fabric supported by Java. While the incentive mechanism is implemented to build new blocks, On the Blockchain, smart contracts provide auditing and access control of Electronic Health Records. Ensures Integrity of the data, improves interoperability the systems. Along with SHA-256, Shamir's Secret Sharing Algorithm is used for access control.

In [3], The Hyperledger Fabric framework is used to implement a Blockchain-based approach to data access management. It comprises both of public and private Blockchains to which users have role-based permissions. RSA is being used to enable public key encryption I e., generate public and private keys which are used for authentication. Although this framework succeeds to implement a Patient-centric method identifies security breaches and information leaks by recognising the patient in his role as data owner, the confidentiality of personal data is being compromised due to the fact that the information is stored in external repositories instead of reliable cloud-based storage.

In [4], A permissioned Blockchain-based system built on a Hyperledger fabric is implemented for EHR integration and data sharing. Hybrid data management approach is used. EHR will be encrypted with a hybrid cryptographic system that incorporates the effectiveness of a symmetric-key cryptosystem with the ease of a public-key cryptosystem, and data will be housed in HIPAA-compliant cloud storage off-chain. The system, however, faces the danger of a SPOF.

[9] discusses the use of Blockchain technology to protect cloud-based healthcare data. However, while it ensures data security, it does not allow for efficient and safe sharing of digital information, and there is no data privacy because the records can be viewed and updated by any healthcare worker.

In [10] Blockchain based scalable and secure data source for medical care is proposed as a solution for accessing data during emergency. However, an ambulance client app user who is not a member of the fabric network may abuse their privileges. Because the data is organized in folders, only a single record cannot be shared or given access to.

Access control ensures the security of information systems by ensuring that users have the necessary permissions to access the services they demand. There are concerns about privacy and the presence of a third party in [11].

[12] Provides data privacy, security, and traceability, as well as low storage costs, low latency, and availability, for IoMT-based distributed healthcare systems. The app, however, is limited to wearable devices and does not leverage the intelligence by using AI/ML technology and NLP to extract critical insights and intuition from a patient's data.

[13] introduces a multi-cloud architecture with Blockchain-based immutable EHR storage, where transactions are timed to enable efficient block elimination, according to the patient's scheduled appointment. However, the doctor uploads the data to the EHR, the patient has no control over it.

[15] Med Bloc is a fully functional, Patients and healthcare professionals may easily access and exchange health information via a dedicated client service, which is powered

by people. Patients can grant and withdraw consent at any moment using smart contracts and cryptographic methods. They haven't used the cloud to store data for greater security in any event.

[16] The researchers employed MCDM's hybrid fuzzy-ANP TOPSIS system to assess Blockchain technology models' influence. The Private Blockchain model was recognised as the highest weighted choice, achieving the top place among the chosen Blockchain models for providing secure EHR services in healthcare organisations.

[17] Because any worker authorised to access the information has access to records, Blockchain allows for easy access to them. It can be accessible from anywhere because it is deployed on a distributed network. The system might be enhanced by giving rapid access to medical records in an emergency. Its structure could be changed to suit a specific condition or to follow industry best practises.

[18] They produce and transport files between computers using techniques they are acquainted with. To reduce client effort, the system combines Secured File Transfer Protocol (FTPS) for safe file transfers with Blockchain as the final source of data. Authorisation, accountability, access control, and Strong identity management are required by the permissioned Blockchain, which is based on pre-defined business logic and consensus.

III. BLOCKCHAIN BASED EHR ARCHITECTURE

A. Preliminaries

The preliminary work that went into the proposed architecture is formally summarised in this section. It elaborates the platform that was used to create this mechanism. In the following section, the most prominent aspects for the implementation of this mechanism are mentioned.

I. BLOCKCHAIN AND ITS DEPENDENCIES

Innovation on Blockchain was proposed by Nakamoto, for his popular work on advanced money or cryptocurrency, bitcoin. Nakamoto made use of Blockchain innovation to solve the bitcoin double investment problem, but in a short.

To understand the Blockchain architecture, consider Figure 1, this illustrates the full process of a transaction on the Blockchain network being sent from a user.

a. A transaction submitted by user on the network signals the creation of a new block. Transactions are stored in blocks on the Blockchain, which are then transacted to every affiliated node of the network. A transaction placed within a block is broadcasted to all network nodes. Every node within the network has an imprint of the complete Blockchain, that helps with verification. Whilst a block containing the user transaction is propagated to all connected nodes, they check to ensure that the block has not been tampered with, in any case.

b. The nodes develop an agreement on blocks that are valid to be attached to the Blockchain and which cannot be attached, during the whole process of adding a block to the Blockchain. The linked nodes perform this validation by checking the transaction and

confirming that the person making transaction is an authorized member of the system using well-known mechanisms.

When a node victoriously completes the validation, the node is rewarded with an incentive.

c. A block is added to the Blockchain only after it is verified.

d. Once the full validation procedure is done, the transaction is completed.

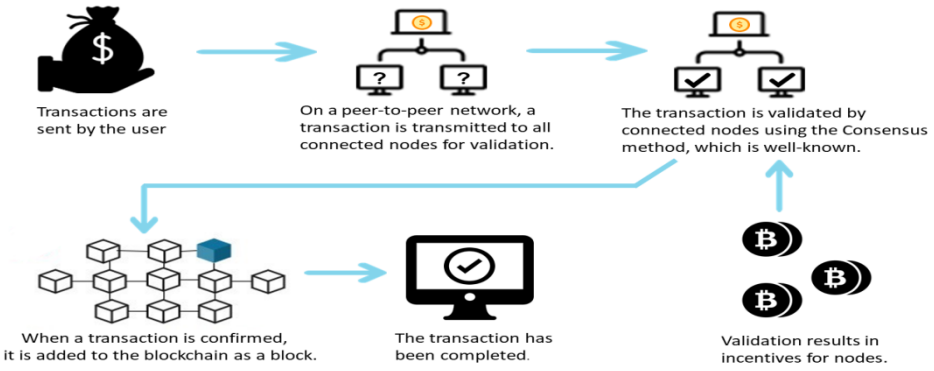


Figure 1. An Overview of Blockchain

The descriptions below explain some fundamental aspects of Blockchain technology.

- BLOCKS: A block has three elements: the data, hash of the current and the previous blocks. Depending on the type of Blockchain, the data could be anything. The data, like in the case of bitcoin, contains of coins that are truly electronic cash [13].
- IBM's HYPERLEDGER FABRIC BLOCKCHAIN PLATFORM: Hyperledger Fabric is Linux open source corporate Blockchain platform designed to serve as a premise for developing modular Blockchain solutions and applications.
- SMART CONTRACTS: Smart contract on Blockchain is basically a piece of code that may be used to do any action. When users send transactions, this code is performed. They are smart contracts that run directly on the Blockchain, keeping them secure from tampering and alterations of any kind.
- MEVN STACK: MEVN is an open-source JavaScript software stack that has emerged as a new and developing technique to construct powerful and dynamic online apps. By properly designing frontend and backend development, its software components may be leveraged to expand the functionality of your website or app.
- IDENTITY: A Blockchain network is made up of peers, orderers, client apps, administrators, and other organisations. An X.509 certificate protects the digital identity of each of these actors – active elements inside or outside of a network that can consume services. A trustworthy authority must verify an identity for it to be verifiable. This is accomplished in Fabric via a membership service provider (MSP). An MSP, to be more explicit, is a component that establishes the rules

that govern this organization's acceptable identities. Fabric's default MSP implementation employs X.509 certificates as identities and follows a standard PKI hierarchical paradigm.

A public key infrastructure (PKI) is a set of internet technologies that allows for secure network connections.

- *System architecture*

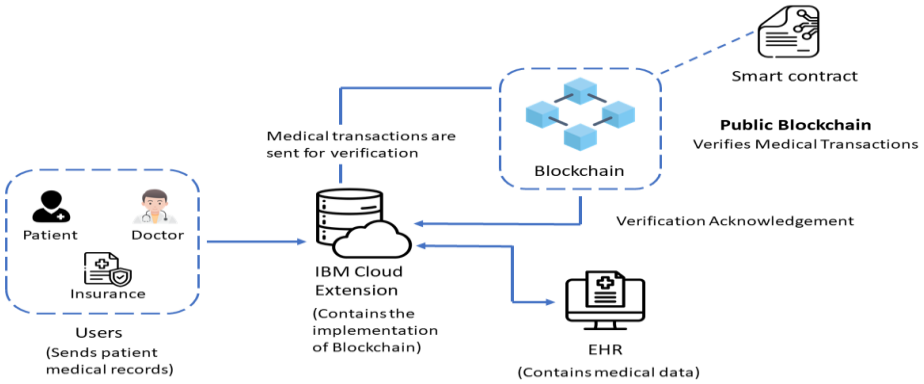


Figure 2. System Architecture

The web application provides a user interface that gives consumers quick access to the prototype's features and capabilities. The web portal can be viewed in three different ways: patient, doctor and insurance company. Patients can access the prototype's patient-specific features after they log in to the appropriate portal. Patients can access the prototype's patient-specific features after they log in to the appropriate portal. When a patient grants permission for the doctor to view their data, the data is encrypted and transferred to the cloud using the doctor's public key. Based on the permissions set by the patient, the doctor can read and update the data during the diagnosis period in the respective patient data files. Whereas the insurance agents can only view the data present in the EHR after authorization in order to offer protection against high medical costs.

The IBM Blockchain platform extensions produces smart contract in JavaScript that manages the assets. In the smart contract's source code, the extension creates a smart contract by combining the fabric-contract-api with a set of asset management functions. Information appended to the Blockchain will not alter once transactions are committed to the ledger since Hyperledger Fabric does not fork. A new transaction is the sole way to update the ledger. Due to the importance of data finality, the system employs a checks and balances protocol to ensure that transactions are legitimate, accurate, and verified. A transaction procedure in this case involves the following steps: initiation by an authorized client, user verification and signature, inspection and validation of user responses, and final validation of the transaction by all network peers. All of this must function successfully before a new block can be added to the network.

Users will receive the necessary credentials to connect to, access, and use the Fabric network resources after completing the registration and enrollment processes (peers, channels etc).The configuration allows network members to configure essential network components including identity verification and channel creation based on their agreement. This limits network access to only authorized users and that confidential transactions are conducted via channels. The user's access level determines whether they can view, update, or share the record.

C. Security basics

SHA 256

The public key cryptosystem, SHA-256 is being used to enable public key encryption I e., generate public and private key which are used for authentication.

Preparing and incorporating are the two main processes of SHA-256. The data is padded and then divided into subgroups. Subgroups are then merged with other subgroups and prime numbers. The subgroups are finally recombined to generate the final hash. This ensures that the registration process is encrypted, and user's personal information is safe.

Algorithm for Authentication:

STEP I: Start

STEP II: Input

read the entities [Patient, Doctor, Insurance]

STEP III: Registration using (Personal details)

Patient→ Name, age, Aadhar number, Phone number

Doctor→ Name, Age, License number, Phone number

Insurance→ Name, Age, License number, Phone number

STEP IV: Using SHA-256 to hash the personal details

STEP V: Generating unique ID

STEP VI: Authentication

The entities' claim of credentials will be verified by Wallet.

Step VIII: End

This system has two layers of security: first, Blockchain technology is safe and employs protocols and mechanisms to protect itself from third-party attacks. Second, our system employs role-based access, which restricts access to the system and its functions to users who have defined roles. As a result, our solution would secure not just the Access control of entities linked with patient records, as well as the security of patient information.

D. Proposed Methodology/work

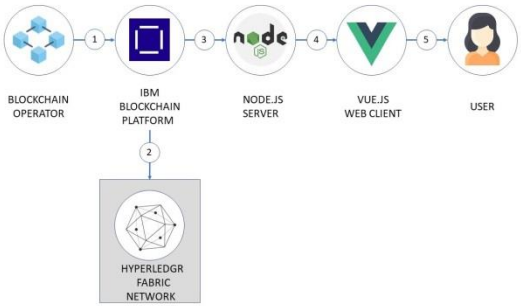


Figure 3. Overview of Proposed methodology

1. The IBM Blockchain Platform service is set up by the Blockchain operator.

2. The operator installs and instantiates the smart contract on the Hyperledger Fabric network created by the IBM Blockchain Platform.

3. The Fabric SDK is used by the Node.js application server to interface with the IBM Blockchain Platform network and generate APIs for a web client.

4. To connect with the network, the Vue.js client uses the Node.js application API.

5. The user uses the Vue.js web interface to register or login, as well as query the world state for records.

In Our proposed framework the application will be integrated with an Hyperledger Fabric to ensure that the patient's data is secure, and transactions are reliable. Hyperledger Fabric implements identity using public key infrastructure technology. Patients' hospital visits, reports, treatment details, physician's notes, laboratory results or reports, prescriptions, X-rays, and outcomes are all examples of transactions in our healthcare system. Patients will have data sharing choices with our system. They will now be able to choose which parts of their medical history are accessible to healthcare providers based on their needs, while keeping the rest of the data private and secure. To extract essential insights and intuition from a patient's medical history, machine learning and Natural Language Processing (NLP) is applied.

Each participant, such as a patient, doctor, or insurance company, is assumed to have a unique ID such as Aadhar number and licence number respectively. During the registration step, each entity must provide personal information and login with their username and password (Dpersonal). Our method uses SHA-256 to hash the Dpersonal and generates a unique ID from it. The patient's, doctor's, and insurance's unique IDs are Pid, Did, and Iid, respectively. The registration information (Dpersonal) is hashed and saved in an encrypted

format. After completing the registration procedure, each entity obtains a unique address in the Blockchain that correlates to its unique ID. The wallet will authenticate an entity's assertion of credentials once it has been registered.

A public and private key for the user with our certificate authority(CA) that is running on the IBM Blockchain cloud is created upon registration, and keys to the wallet.

When the doctor or insurance company receives access from the patient, they can log in with their respective credentials to download or see the records. They must provide an OTP sent to their registered mobile number before downloading it.

Workflow of proposed Scheme

Step 1: When a new Electronic health record file [EHR = Pid||Did|| Iid] is produced, the EHR is signed with the doctor's signature Dsig here in case of doctor, encrypted using the patient's public key SKpub, and then uploaded to the doctor's wallet [CipherEHR ESKpub (EHR||Dsig)]. Using asymmetric key encryption, we ensure that the patient and other entities have complete control over the accessibility of medical documents.

Step 2: The Blockchain saves the relevant reference index number and hash when encrypted EHR file is submitted to the wallet.

Step 3: When a patient visits a hospital, access to the patient's historical EHRs will be seeked, which will trigger a smart contract. The smart contract will authenticate the doctor's or insurance identity, EHR's index number and then provide access (allow or refuse) to them based on the patient's consent as established in access policies. If successful, patient uses his or her private key SKpriv, SKpriv,[EHR ← DSKpriv (CipherEHR)] to decode the CipherEHR.

Step 4: To compute the shared secret key, KES, both entities share ephemeral keys. To send the EHR file to the doctor B/ insurance, the patient re-encrypts it with KES, signs it with his Ksig, [ReCipherEHR EKES (EHR||Ksig)], and sends it to him. Doctor B utilises his KES, [EHR DKES (ReCipherEHR)], to decode it. Finally, it will check the EHR's integrity using doctor A's public key Dpub and patient EKpub's ephemeral public key EKpub to ensure that it has not been tampered with. When the access period expires, RC notifies the doctor and patient, and the keys expire at the same time, with the smart contracts updating the activity list. The doctor or insurance firm will lose access to the EHR and will have to request the patient view the file again.

This type of access control ensures that only authorised individuals have access to the EHR, prohibiting unauthorised access. Through encryption technology, our recommended access control solution enables protection of identity and data integrity while maintaining patient-centeredness. The wallet is in charge of confirming credentials of an entity. Because of the small block size and big size of the EHR file, it also serves as storage, with the EHR file's hash being uploaded to boost the efficiency of our method to the Blockchain.

When it comes to sending EHR data over Blockchain, scalability is a major concern, like as photographs, can be incredibly huge. Due to the network's distributed duplicated nature, it is impractical to store and copy EHR data on a Blockchain network for sharing. All metadata is stored on the chain (such as transactions, EHR information, and access control), while shared sensitive EHR data is saved and maintained in an IBM cloud. The shared EHR offers excellent scalability, durability, availability, and low latency, as well as near-perfect security (encrypted at both transmission and rest) and low cost.

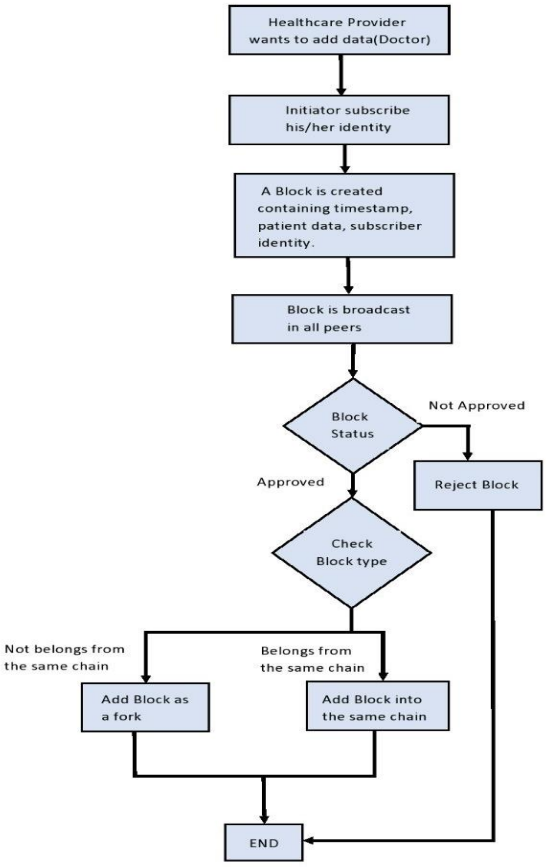


Figure 3. Access control Flowchart

Functioning of the smart contract approach

The approach explains how the smart contract for patient records works. The three functions of this method are to define add, view, and update records. Users of the system make advantage of these features. The doctor performs the first function, which is to add a

patient record. This function also ensures that the task is being carried out by the doctor's account's verified public address and not by a third party. After the doctor has completed the validity check, he or she can add the patient's records and then save the record to complete the function. View patient records is the second function, which requires the patient id that will be stored in a variable. The system would look for the patient's information using this id and then return the data to the user that had requested them. Validation for the given roles of patient, doctor, and insurance is also included in this function. Only authorized entities would be able to see the information. The third function is update patient records, which is utilized by the doctor to make any modifications to the patient's stored records. To guarantee that only authenticated users have access to this function, the validation procedure is repeated.

IV. RESULTS AND DISCUSSION

This section demonstrates our approach's practicality, and we discuss how healthcare industry, especially electronic health records, might benefit from Blockchain technology. Despite recent advancements in healthcare and in EHR systems, there were still some challenges that this unique technology, Blockchain, addressed. Our recommended solution combines secure document storage with precise access control constraints. Only trusted and related individuals have access to medical records, therefore the system benefits from role-based access as well. This also tackles the EHR system's information asymmetry problem. In the future we would like to create a database more tamperproof.

Paper	Cloud	Admin/ Hospital	Insurance	Role specific login/ Registration	Secured downloading
Blockchain based approach for securing health care data	✓	X	✓	✓	✓
Blockchain based EMR using smart contract	X	✓	X	X	X
E-health data access management	X	✓	X	X	X
Health Chain	X	X	X	✓	X
A Panacea for Healthcare	X	✓	X	✓	X
Securing Medical Data	✓	✓	X	✓	X

Table 1: Comparative analysis of features

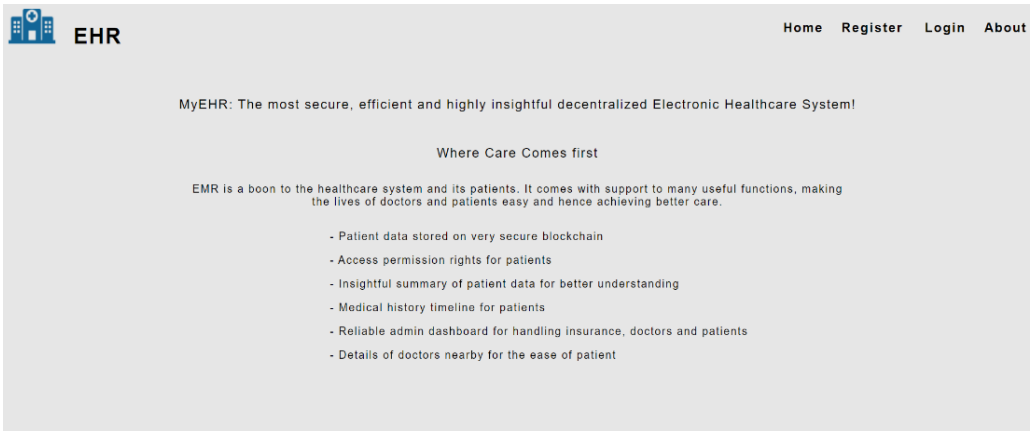
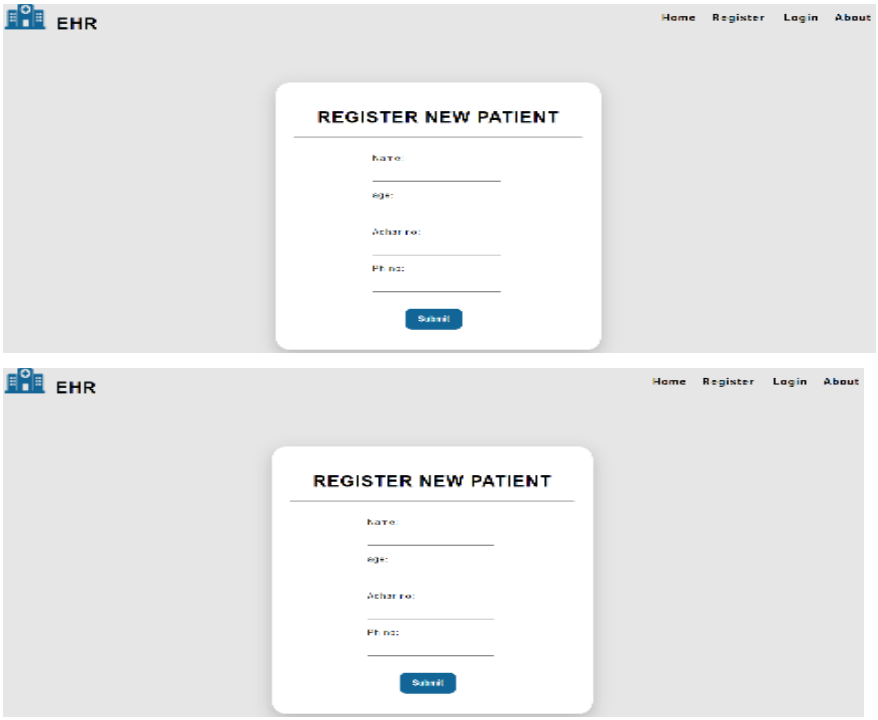


Figure 4. Home Page of the Web Portal



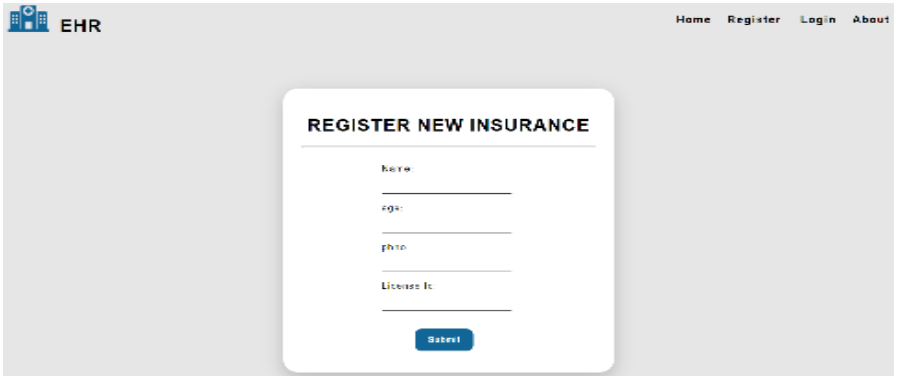
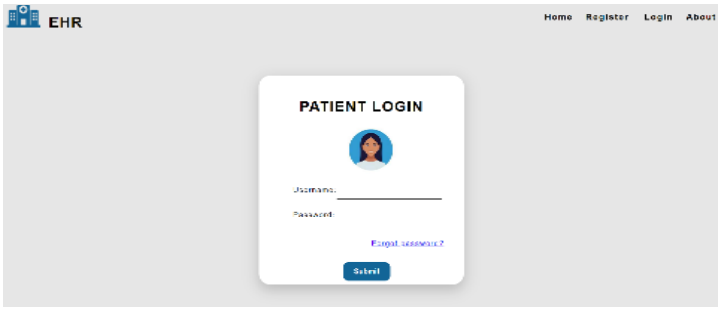
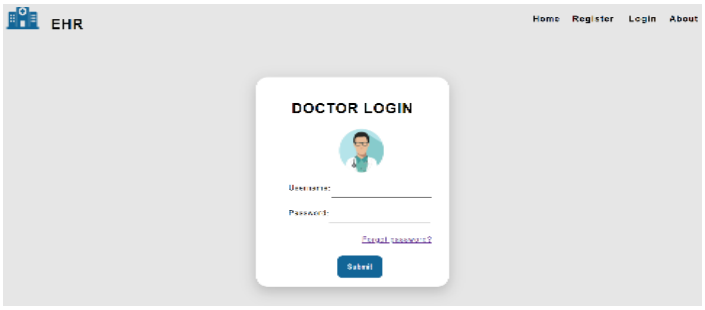


Figure 5. Registering new user





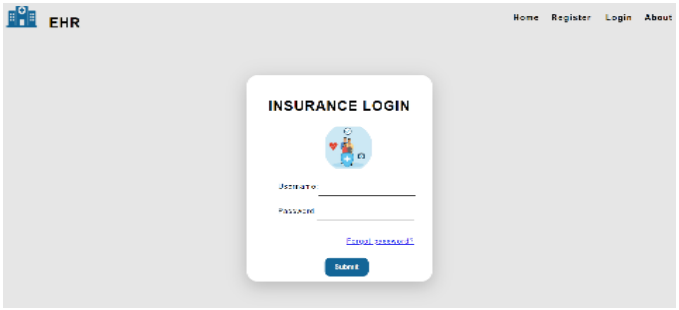


Figure 6. Access based Login

On registration the following will be generated which is used for further transactions.

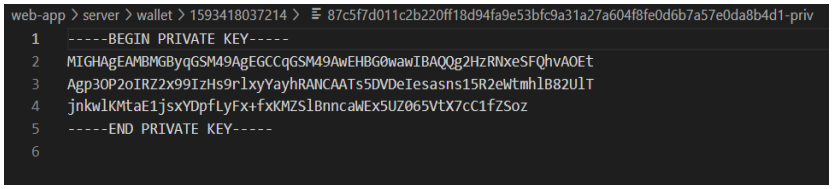


Figure 7. private key

Figure 8. public key

Figure 9. certificate

V. CONCLUSION

In this paper, a Blockchain based framework has been presented for secure storage of EHR using which the authorized entities can carry out respective transactions without intervention of any third party. This proposed system satisfies the criteria required by personal information protection rules. Because the data access is unambiguous, supplementary entities can obtain health information based solely on security regulations. The use of such a convention in real life would provide several benefits to all parties concerned. Patients must be able to easily manage their medical analyses and hospitals should be able to give better medical care, without causing patients to be concerned about the private information they are disclosing.

REFERENCES

[1] A. Shahnaz, U. Qamar, and A. Khalid, “Using Blockchain for Electronic Health Records,” in IEEE Access, , Volume. 7, pp. 147782 - 147795, 2019, doi: 10.1109/ACCESS.2019.2946373

[2] G. Yang, C. Li2, K. E. Marstein, “A Blockchain-based architecture for securing electronic health record systems,” in ResearhGate, pp. 1-13, 2019, doi: 10.1002/cpe.5479

[3] L. Hirtan, C. Dobre, P. Krawiec, J. Mongay Batalla, "Blockchain-based approach for e-health data access management with privacy protection," in IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2019, pp. 1-7, doi: 10.1109/CAMAD.2019.8858469

[4] A. Dubovitskaya, F. Baig, Z. Xu, R.Shukla, P. S. Zambani, A.Swaminathan, M. M. Jahangir, K. Chowdhry, R. Lachhani, N. Idnani, M. Schumacher, K. Aberer, S. D. Stoller, S. Ryu, F. Wang, "ACTION-EHR:Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care," in Journal of Medical Internet Research, pp. 1-15, 2020, doi: 10.2196/13598

[5] A. Henrique, M. C. André da Costa, R. da Rosa Righi, "Electronic health records in a Blockchain: A systematic review," , Volume: 26 issue: 2, page(s): 1273-1288, 2019, doi: 10.1177/1460458219866350

[6] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, and Y. Zhang "A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System," IEEE Internet of Things Journal, vol.8, pp. 5914 - 5925, 2021, doi: 10.1109/JIOT.2020.3032997

[7] J. Indumathi, A. Shankar, M. R. Ghalib, j. Gitanjali, Q. Hua, Z.Wen, and X. Qi "Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly, Unflappable, Unblemished, Unlimited Health Care Services" in special section on new advances in blockchain-based wireless networks, vol.8, pp. 216856 - 216872, 2020, doi: 10.1109/ACCESS.2020.3040240

[8] A. A. Jolfaei, S. F. Aghili, and D. Singelee "A Survey on Blockchain-based IoMT Systems: Towards Scalability," in IEEE Access, vol.4, pp. 1 - 28, 2021, doi: 10.1109/ACCESS.2021.3117662, IEEE Access

[9] C. Esposito, A. De Santis, G. Tortora, H. Chang, K. Raymond Choo "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy" in IEEE Cloud Computing, pp. 31- 37, 2018

[10] S. Hasavari and Y.Tae Song "A Secure and Scalable Data Source for Emergency Medical Care using Blockchain Technology" pp. 71 - 75,2019

[11] F. Safna, C. Meera , V. Mohan, S.L Sofia , L. Sumimol and P. Sajith "Securing Medical Data Using Blockchain and Cloud" International Journal of Advanced Science and Technology Vol. 29, No. 9s, (2020), pp. 3108-3114

[12] B. S. Egala , A. K. Pradhan , V. Badarla,and S. Mohanty "Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control" in IEEE Internet of things journal, vol. 8, no. 14, 2021, pp. 11717 - 11731

[13] R. Mishra, D. Ramesh and D. Edla "Deletable Blockchain based Secure EHR Storage Scheme in Multi-Cloud Environment" in 2020 IEEE 22nd International Conference on High Performance Computing and Communications, pp. 1057- 1064, 2020, doi: 10.1109/HPCC-SmartCity-DSS50907.2020.00142

[14] Ahmed, S. T. (2017, June). A study on multi objective optimal clustering techniques for medical datasets. In 2017 international conference on intelligent computing and control systems (ICICCS) (pp. 174-177). IEEE.

[15] J.Huang, Y.wei Qi, M.Rizwan Asghar, A.Meads, and Y.Tu, "MedBloc: A Blockchain-based Secure EHR System for Sharing and Accessing Medical Data" 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering TrustCom/BigDataSE), 2019, pp.5-8, Doi: 10.1109/TrustCom/BigDataSE.2019.00085

[16] M.Zarour1 , MD T.Jamal Ansari2 , M.Alenezi 1 , A.Krishna Sarkar, M.Faizan2 , A.Agrawal 2 , R. Kumar 2,4, AND R.Ahmad Khan, "Evaluating the Impact of Blockchain Models for Secure and Trustworthy Electronic Healthcare Records" IEEE Access (Volume: 8) , 2020, pp.2-3,12-15, Doi:10.1109/ACCESS.2020.3019829

[17] Vardhini B, S.N Dass, Sahana R, Dr.R.Chinnaiyan, "A Blockchain based Electronic Medical Health Records Framework using Smart Contracts" 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp.1-4, Doi:10.1109/ICCCI50826.2021.9402689

[18] Gowda NC, Manvi SS, Malakreddy B, "Blockchain-based Access Control Model with Privacy preservation in a Fog Computing Environment", IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), pp. 1-6, Jul 2022.