A Privacy Preserving Blockchain Framework for Healthcare Data Based on EHR (Electronic Health Records)

Sheel Srivastava[1] Mr. Suyash Srivastava[2]
[1]Student [2]Professor
[1,2]Department of Computer Science and Engineering
[1,2]SR Institute of Management and Technology, Lucknow, India

Abstract — Healthcare information is highly sensitive because it includes details such as patient prescriptions, medical history, treatments, and clinical activities. This data is often shared among different stakeholders within the healthcare system, including doctors, laboratories, and other medical professionals. Since patient information is critical, it must be kept accurate, up-to-date, confidential, and accessible only to authorized individuals. Traditional centralized systems used for storing healthcare records can increase security risks, as they create a single point of vulnerability. Therefore, ensuring the privacy and security of medical data while sharing it across multiple entities has become a major concern. This study proposes a privacy-preserving access control framework based on blockchain technology. The framework uses a decentralized approach, where data is managed across distributed systems through consensus mechanisms. This ensures better security, transparency, and integrity of healthcare data. One of the key advantages of blockchain is its immutability, which prevents unauthorized modification of records and protects transactions from tampering. Furthermore, the proposed system considers different participants in the healthcare ecosystem, such as patients, doctors, researchers, and pathology labs, allowing them to share information securely through authorized channels. The framework is implemented and evaluated using Laravel and Hyperledger Fabric, and the results demonstrate improvements in security, regulatory compliance, reliability, scalability, and data accuracy.

Keywords: Blockchain, Electronic Health Record, Medical Hashing Control, Security and privacy of data.

I. Introduction

Over the past decade, the healthcare sector—including hospitals, pharmaceutical institutions, and insurance organizations—has been handling patient records with increasing care and responsibility. These records, commonly referred to as Electronic Health Records (EHRs), are considered highly valuable assets due to their sensitive nature and the need for strict privacy and security measures.

EHRs store detailed and confidential information about patients, such as personal details (name, address, and unique identification), medical history, family medical background, treatment plans, prescribed medications, and other related data. This information is often shared among various stakeholders within the healthcare system to support timely and effective decision-making. Therefore, it is essential that the shared data remains accurate, consistent, and accessible only to authorized individuals.

Despite their importance, maintaining the security and privacy of EHRs remains a major challenge. Over the years, healthcare organizations have increasingly become targets of cyberattacks, where attackers attempt to steal sensitive patient data. One of the key reasons behind this is the high value of medical records on illegal markets, which is significantly higher than that of financial data like credit card information.

To address these concerns, governments and regulatory bodies have introduced strict frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the General Data Protection Regulation (GDPR) of 2018. These regulations define guidelines for securely storing, processing, and sharing healthcare data to prevent misuse and data breaches.

However, security risks still persist. In some cases, internal misuse of data has been reported, although such incidents have reduced due to stricter legal actions. External threats such as phishing, ransomware, and social engineering attacks continue to compromise healthcare systems. For example, attackers have successfully accessed sensitive information through deceptive emails or disrupted services by encrypting critical records, leading to operational failures and service delays.

Another limitation of traditional healthcare systems is the lack of proper audit mechanisms to track who accessed patient records and when. This lack of transparency increases the risk of unauthorized access and reduces accountability. Such security breaches not only violate patient privacy but also damage the reputation of healthcare organizations and even impact national trust.

According to modern data protection regulations like GDPR, patient data must be handled by authorized entities and shared only with proper consent. Therefore, implementing strong access control mechanisms is essential to ensure that sensitive healthcare data remains secure, private, and protected from unauthorized access.

II. Related Work

This segment presents the current examinations connected with our proposed work to recognize the meaning of blockchain innovation in medical services applications and figure out the conceivable exploration holes that should be tended to. In the writing, various systems have been proposed to counter the security issues to shield the EHRs from unapproved access; these structures are named Cloud-based and Blockchain-based outline works / designs / arrangements. At first, cloud-based solutions have been proposed to oversee patient records in the medical services industry to limit cost and improve- demonstrate effectiveness and security.

Title	Description
The work process should be according to shaped regulations	Patients' data should be gotten against a privacy break.

Should upholds Turing Fulfilment Operation	The medical services application in view of blockchain ought to support Turing Culmination Tasks by keeping programming element to take care of any calculation issue.
The blockchain platform ought to enable user identification & authentication	Patients and Experts ought to be recognized/validate in the medical care application. Support interpretability by requiring a structural format for the interpretation of exchanged clinical data.
Adaptability for huge populations	The application should be versatile and upholds quite a few clients.
Cost-effectiveness	For a large number of participants, the blockchain solution must be affordable.
Ought to show restraint focused care model	Ought to show restraint focused care model
E-Mail Alert for Access Data	When Admin or Doctor access any data like patient prescription or lab report, patient got email alert for grant permission to access data.

Table 1: 2.1: Description of the Related Work

III. BLOCKCHAIN TECHNOLOGY

The blockchain is decentralized (i.e., no concentrated authority to control) and disseminated design, known as a shared stage, distributes undertakings to a large group of hubs and works in a gathering to frame choices for the benefit of the organization[3][4][6][15]. Every hub is permitted to per-structure works that are known as exchanges and every one of the approved exchanges are kept in a circulated and unchanging record as a block. Blockchain accomplished prominence fundamentally from the digital money, i.e., Spot COIN, in the realm of money. In the blockchain, various tasks are being handled at each moment; every client is conveying his/her appropriated record to distinguish fakes and confirm the separate transac-tions anytime of time. The blockchain network continues to add new approved blocks of exchanges in the disseminated record[17]. All members or hubs have equivalent open doors for bookkeeping record in the net-work and it guarantees a total agreement inside all hubs in the closely resembling blockchain. Blockchain innovation shapes a trust layer without hosting any third gathering for different deals. In the mongrel lease situation, blockchain applications have broadened and turned into the spine for various applications. In the medical services space, blockchain innovation assumes an imperative part to construct platform for putting away, assessing, and keeping up with classified medical services data with a full- evidence framework.

A blockchain organization can be delegated public (Permission less), private (Permissioned), cross breed, and combined/consortium blockchain; the reasonable blockchain organization can be selected based on the necessities of the utilization case[24]. The private blockchain network is focal sized and overseen by an individual/association, while, the public blockchain network is totally decentral-sized and oversaw by various clients/associations. The half breed blockchain network consolidates the highlights of both public and private blockchain networks, and different clients are permitted to control their information and just the subset of the information is accessible in the public space or for a particular gathering.

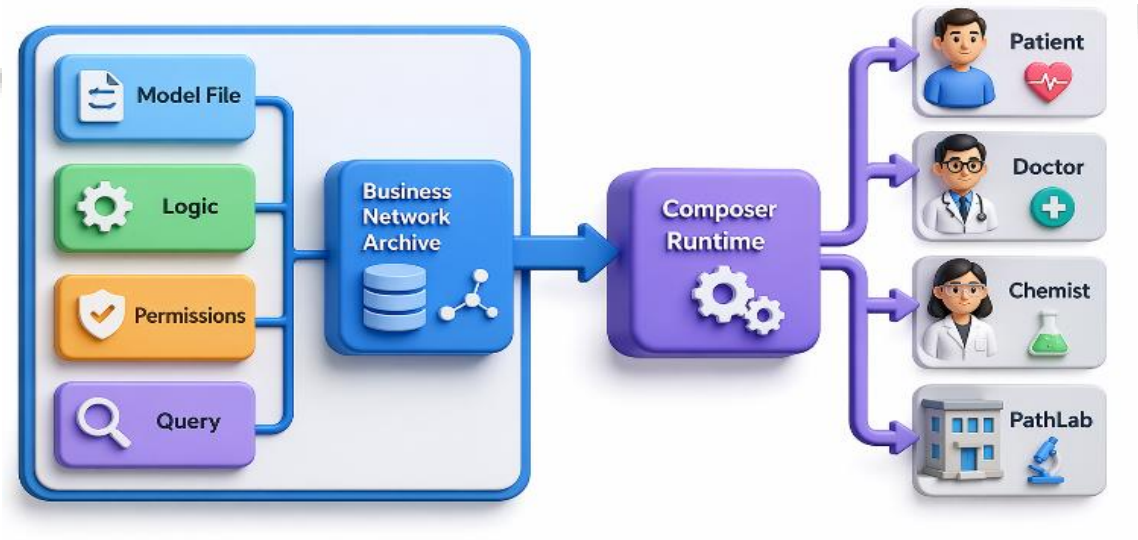

Fig. 3.1: Business Network Architecture

IV. FRAMEWORK & IMPLEMENTATION

This segment portrays the fundamental devices and procedures used to construct our proposed medical services system. Laravel Framework assume an imperative part in the execution of a blockchain-based system. Hashing Alga is a system that permits no change while any other want to change a blockchain application

This project developed by Framework Laravel 9.0 Laravel is one of the most popular server-side scripting languages running today[27]. It is used for creating dynamic cloud-based pages that interact with the user offering customized information. Laravel offers many advantages; it is fast, stable, secure, easy to use and open source Email alert active while anyone want to change data of health record and Hashing code implemented for encrypt data of health records

V. SECURITY REQUIREMENTS

The information should stay classified, exact, and accessible just to approved clients. Despite the fact that it becomes difficult when various substances are mentioned to peruse and alter data sets whenever. Accordingly, it is an important perspective to guarantee security by sticking to the appropriate channel of sharing data[26]. A proficient medical services application ought to help the accompanying important features Find Medicines by Keywords

VI. DIAGRAM

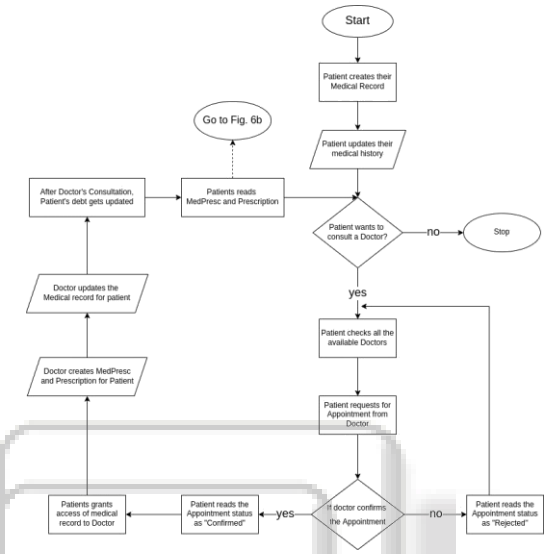

Fig. 2: (6A)

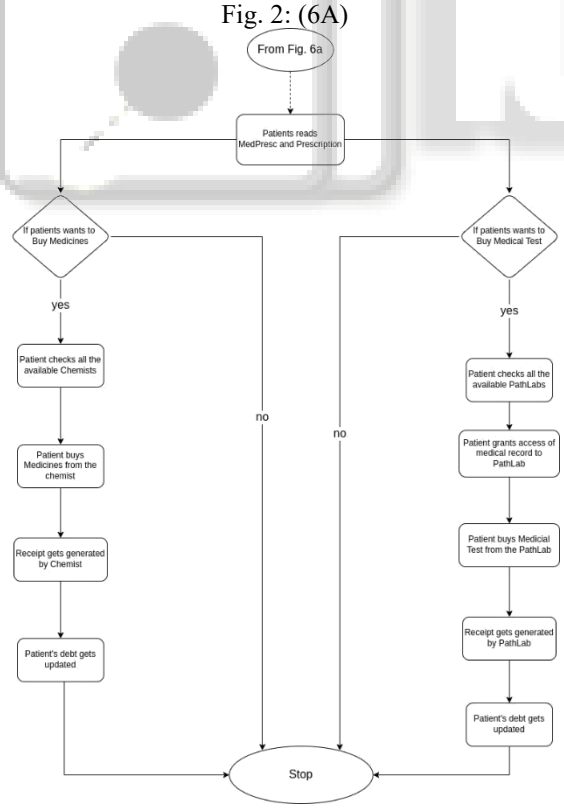

Fig. 3: (6B)

Fig. 6A & 6B: is Flow Chart of the proposed framework for healthcare application

A. Proposed Framework

The proposed framework for healthcare data management is explained in this section. The proposed framework's flowchart, which depicts the overall operation of a healthcare application with various participants—patients, doctors, pathologists, and chemists and their respective transactions, is shown in Fig. 6. The exchanges help to refresh the resources inside the system.

Roles / Module	Access Rights & Control
Admin	– Has full admittance to all clients and framework assets – Adds Members to the blockchain network. – Peruse, Make, Update, and Erase all members' data
Doctor	– Access, Edit, Create, and Delete their data – A Specialist sees just the rundown of patients they are approved to change. – Read and update medical records that they have authorized. – All Members can see all specialists. – Read, Create, Update Appointment. – Read, Create, Update Prescription. – Confirm an Appointment with the patient.
Patient	– Access to, creation of, modification to, and deletion of their own participant data. – Access, edit, and read medical records. – Permit Doctor and PathLab Access to Medical Records – Renounce Admittance to Clinical records from Specialist and PathLab. – Read all of the assets, including the receipt, prescription, and appointment. – Schedule a Visit with the Doctor. – Purchase Medication from the Scientific expert. – Purchase Medication from the Scientific expert. – Purchase a medical test from PathLab

Table 2: (7.1) Access Right & Control of the Modules

VII. HASHING ALGORITHM

procedure CREATEANDUPDATEMR(D_x, D_{pkx})
The procedure of creating and updating Medical records
P_x with P_{prkx} creates MR_x ▷ Patient with his private key creates a medical record
$P_x \rightarrow MR_x(D_{pkx})$ ▷ Patient Grants access to medical records using Doctor public key
For each user u, given access to MR_x
if (Permission == "ALLOWED" and Role = "Doctor" or "PathLab") **then** ▷ Algorithm checks whether Access Control permission is ALLOWED or DENIED to access MR_x
$D_x \leftarrow$ Decrypt $(D_{prkx}(MR_x))$ ▷ Doctor decrypts Medical Record with his Private key
$D_x \rightarrow$ Update $MR_x(P_{pkx})$ ▷ Doctor encrypts updated Medical Record with patient public key
$P_x \leftarrow$ Decrypt$(P_{prkx}(UHR_x)$ ▷ Patient decrypts updated Medical Record with his Private Key
else if (Permission == "DENY") **then**
D_x cannot view MR_x
else
Nothing is happened
end if
end procedure

VIII. RESULTS AND DISCUSSION

This segment presents a logical conversation on vari- ous executed situations in the blockchain climate for medical services application. We have approved our supportive of acted structure on various situations like portrayed in the past area. We have developed and deployed our prototype on a system Intel Core i5 processor with 16GB of memory and Window 11 OS. The prerequisites for installing Xampp Server and Composer. The components necessary to set up the development environment are composer and other components like VS- Code are installed in order to create and execute a business network.

A. Discussion on Privacy & Security

Presently, awe discuss the assessed results based on various execution boundaries like protection and security, adherence of guidelines, and accessibility and afterward contrast our proposed structure and the current framework/systems.

The blockchain-based system guarantees a patient's security by giving the adaptability to indicate ing granular access control across his/her EHRs. More- finished, it considers access control systems between the clients of the organization by including shrewd agreements. It is basically impossible to get to clinical information by any substance of the blockchain or pernicious clients without approaching honors. Indeed, specialists can see the rundown of patients, who have been conceded admittance privileges to their clinical records in the organization.

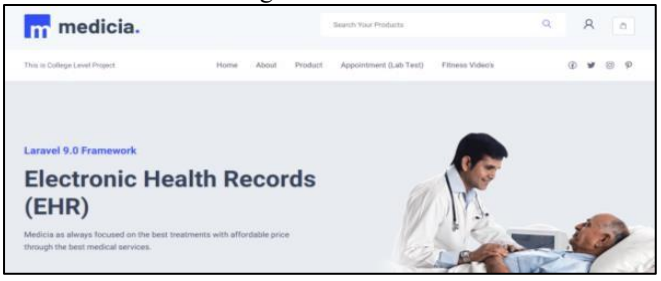

Fig 4 (8A) – Welcome Page

Fig 5 (8B) – Appointment for Lab Test

IX. CONCLUSION AND FUTURE SCOPE

In this work, we proposed another entrance control outline work for the medical care information the executives framework utilizing access control systems and encryption methods. The proposed system is safer, proficient, and available between various members, for example, dad patients, specialists, physicists, and pathology labs. We have carried out this permissioned blockchain network using laravel and writer in an orderly way. Utilizing the consortium model, we sent brilliant agreements in blockchain innovation to make security strategies so patients have control of the entrance rules of different partners in the medical services framework. Besides, it offers huge potential for guaranteeing the protection, security, uprightness, time productivity, and secrecy of medical services information, and granular access control the board. The model favorable to vides a blockchain-based application for medical care information the executives and satisfies specific principal prerequisites. Later on we, first and foremost, plan to make our edge work more easy to understand by incorporating it with a proposal framework, to relegate a position to specialists and pathology labs based on their patients' insight or fulfillment. From there on, the patients' criticism uncovers to all partners on the blockchain network for successful suggestion to the patients. We can likewise consolidate the strategies to get to EHRs in crisis circumstances to concede access freedoms to specialists or different partners by the designated individuals from the patient.

ACKNOWLEDGEMENT

Certainly this project could not have completed without guidance and moral support from other staff member of the college.

Last but least we are thankful to our guide for his moral support for this project and we are thankful to faculties for their expert guidance.

Finally we are thankful to our all-other well-wisher and those people who are directly or indirectly related with this project for their valuable and precious help during this project.

REFERENCES

[1] H. Abrar, S. J. Hussain, J. Chaudhry, K. Saleem, M. A. Orgun, J. Al-Muhtadi, and C. Valli. Risk analysis of cloud sourcing in healthcare and public health industry. IEEE Access, 6:19140– 19150, 2018.
[2] L. Adefala. Healthcare experiences twice the number of cyber attacks as other industries. CSO ONLINE, Mar, 6, 2018.
[3] F. Ahmad, Z. Ahmad, C. A. Kerrache, F. Kurugollu, Adnane, and E. Barka. Blockchain in internet-of- things: Architecture, applications and research direc- tions. In 2019 International conference on computer and information sciences (ICCIS), pages 1–6. IEEE, 2019.
[4] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani. Applications of blockchains in the internet of things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 21(2):1676–1717, 2018.
[5] M. Antwi, A. Adnane, F. Ahmad, R. Hussain, M. H. ur Rehman, and C. A. Kerrache. The case of hy- perledger fabric as a blockchain solution for healthcare applications. Blockchain: Research and Applications, 2(1):100012, 2021.
[6] S. T. Argaw, N.-E. Bempong, B. Eshaya-Chauvin, and Flahault. The state of research on cyberattacks against hospitals and available best practice recommen- dations: a scoping review. BMC medical informatics and decision making, 19(1):1–11, 2019.
[7] T. Q. Ban, B. N. Anh, N. T. Son, and T. Van Dinh. Survey of Laravel blockchain frameworks: case study in fpt university's cryptocurrency wallets. In Proceedings of the 2019 8th International Conference on Software and Computer Applications, pages 472–480, 2019.
[8] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W.-C. Hong. A survey on decentralized consensus mechanisms for cyber physical systems. IEEE Ac- cess, 8:54371–54401, 2020.
[9] V. Buterin et al. A next-generation smart contract and decentralized application platform. white paper, 3(37):2–1, 2014.
[10] M. Castro and B. Liskov. Practical byzantine fault tolerance and proactive recovery. ACM Transactions on Computer Systems (TOCS), 20(4):398–461, 2002.
[11] U. Chelladurai and S. Pandian. A novel blockchain based electronic health record automation system for healthcare. Journal of Ambient Intelligence and Humanized Computing, 13(1):693–703, 2022.
[12] T. K. Dasaklis, F. Casino, and C. Patsakis. Blockchain meets smart health: Towards next generation healthcare services. In 2018 9th International conference on information, intelligence, systems and applications (IISA), pages 1–8. IEEE, 2018.
[13] N. Fikri, M. Rida, N. Abghour, K. Moussaid, A. El Omri, and M. Myara. A blockchain architecture for trusted subledger operations and financial audit using decentralized microservices. IEEE Access, 2022.
[14] J. Gao, H. Liu, Y. Li, C. Liu, Z. Yang, Q. Li, Z. Guan, and Z. Chen. Towards automated testing of blockchain-based decentralized applications. In 2019 IEEE/ACM 27th International Conference on Program Comprehension (ICPC), pages 294–299. IEEE, 2019.
[15] W. Gao, W. G. Hatcher, and W. Yu. A survey of blockchain: Techniques, applications, and challenges. In 2018 27th international conference on computer communication and networks (ICCCN), pages 1–11. IEEE, 2018.
[16] W. J. Gordon and C. Catalini. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Computational and structural biotechnology journal, 16:224–230, 2018.
[17] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini,
[18] E. A. Howson, and T. Hayajneh. Healthcare Blockchain system using smart contracts for secure automated remote patient monitoring. Journal of medical systems, 42(7):1–7, 2018.
[19] H. Guo, W. Li, M. Nejad, and C.-C. Shen. A hybrid blockchain-edge architecture for electronic health record management with attribute-based cryptographic mechanisms. IEEE Transactions on Network and Service Management, 2022.
[20] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and B. Sadoun. Habits: Blockchain- based telesurgery framework for healthcare 4.0. In 2019 international con- ference on computer, information and telecommunica- tion systems (CITS), pages 1–5. IEEE, 2019.
[21] J. Hathaliya, P. Sharma, S. Tanwar, and R. Gupta. Blockchain-based remote patient monitoring in healthcare 4.0. In 2019 IEEE 9th international conference on advanced computing (IACC), pages 87–91. IEEE, 2019.
[22] H. Honar Pajooh, M. A. Rashid, F. Alam, and S. Demidenko. Experimental performance analysis of a scal- able distributed Laravel. Sensors, 22(13):4868, 2022.
[23] K. M. Hossein, M. E. Esmaeili, T. Dargahi, et al. Blockchain-based privacy-preserving healthcare architec- ture. In 2019 IEEE Canadian conference of electrical and computer engineering (CCECE), pages 1–4. IEEE, 2019.
[24] Laravel Framework 9.0. Web Tech Solution docs. 2023.

