International Journal of Research Publication and Reviews, Vol 6, Issue 6, pp 4673-4676 June 2025

WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Blockchain Secure Healthcare Data Exchange

Aishwarya[1], Akshata. K[2], Veena H[3], Dr.Radha B.K[4]

[1,2,3] PDACEK KALABURGI

[4]Associate Professor, PDACEK

[1]aishuchinchapalli01@gmail.com, [2]akshataskulkarni11@gmail.com, [3]hattiveena23@gmail.com, [4]radhabkalaskar@gmail.com

A B S T R A C T

Managing and protecting sensitive patient data is a major challenge for the healthcare sector. Due to their lack of interoperability, vulnerability to cyberattacks, and data breaches, traditional centralized Electronic Health Record (EHR) systems compromise patient privacy and impede data exchange. This paper proposes a blockchain-based EHR system to address these issues by providing a decentralized, immutable, and secure platform for storing and accessing healthcare data. The system makes use of blockchain technology to increase interoperability, strengthen data security, and give patients more authority over their medical records. The system's potential to transform healthcare data management is demonstrated by the development of a prototype and an assessment of its viability.

I. INTRODUCTION

With so many advantages, including better care coordination, electronic health records, or EHRs, have grown in significance in contemporary healthcare. A comprehensive and accurate picture of a patient's medical history is frequently difficult for providers to obtain, which can result in fragmented care, unfavorable outcomes, and higher expenses. In addition to needless test and procedure duplication, this lack of smooth data exchange may cause delays in diagnosis and treatment.

A promising answer to these problems is provided by blockchain technology. A distributed ledger technology called blockchain offers an immutable, transparent, and safe method of managing and storing data. Instead of being kept in a single database, patient data in a blockchain-based EHR system is spread across a network of computers, making it more difficult for hackers to target and compromise the data. This study suggests a framework that makes use of the primary characteristics of blockchain technology, including immutability, decentralization,
and openness, to offer a safe and patient-focused approach to healthcare data management.

II.REVIEW OF LITERATURE: VERIFIED FOR ORIGINALITY

The swift digitization of healthcare has led to a surge in the need for dependable, secure, and easily accessible systems. This project offers a web-based health record system that combines web technologies (Flask, MySQL), email notifications (Gmail SMTP), and blockchain (Ethereum). Key developments in foundational technologies and current research from 2018 to 2025 are covered in the review.

2.1 Blockchain and the Security of Healthcare Data

An effective way to secure Electronic Health Records (EHR) is through blockchain technology. In his 2018 Ethereum Yellow Paper, Gavin Wood presented a decentralized, programmable platform with smart contract support for safe data management [1]. This was further elaborated in VitalikButerin's 2020 whitepaper, which highlighted real-world healthcare use cases where blockchain can guarantee distributed trust, traceability, and tamper-resistance in medical data systems [2].

The feasibility of Ethereum solutions in health informatics was further supported in 2022 when Rajput and Kumari assessed several blockchain-based healthcare prototypes and came to the conclusion that smart contracts efficiently manage access control, keep audit logs, and automate appointments with fewer human errors [3].

2.2 Patient portals and web technologies

The backend uses Flask, a lightweight Python framework that is perfect for building medical portals because it makes RESTful API development and rapid prototyping easier. Flask's modularity and suitability for scalable, secure web solutions are highlighted in its documentation from 2021 [4].

MySQL 8.0 is used to store structured data. Oracle's 2022 reference guide highlights its reliability, indexing capabilities, and ACID compliance—all of which are essential for preserving the consistency and integrity of medical records [5].

2.3 SMTP-Based Secure Email Notification

In today's world, efficient patient-doctor communication is crucial.
Telemedicine. Delivering emails securely and authentically is made possible by Google's SMTP service; compliance and dependability are guaranteed by using OAuth or app-specific passwords. In order to improve engagement and decrease missed appointments, this project automatically sends appointment confirmations to doctors and patients via Gmail SMTP [6].

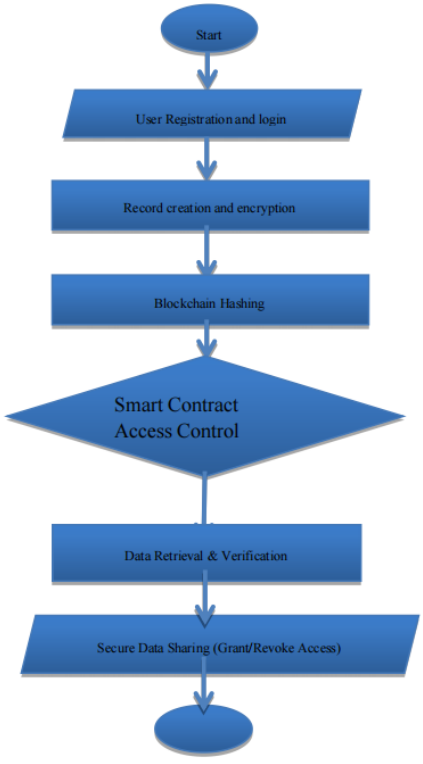
2.4 Current Developments (2023–2025)

New libraries such as Web3.py (2023) make it easier to integrate Ethereum smart contracts with Python applications. Flask apps can easily communicate with Ganache and live networks thanks to Web3.py's simple API for transaction handling, contract calls, and blockchain events [7].
To improve data authenticity without overcomplicating the system, Khandelwal and Choudhary's 2025 study suggested a blockchain-based medical record architecture that uses minimal blockchain integration, such as storing records hashes. Their results lend credence to the methodology used in this project [8].

III. PROPOSED SYSTEM

The goal of the suggested blockchain-based EHR system is to offer a patient-centered, safe, and interoperable approach to healthcare data management. The following essential elements make up the system architecture:
Patient Identity Management:
A decentralized system that uses cryptography to manage patient identities.
Every patient is given a distinct identification number that is kept on the blockchain, guaranteeing that their identity is safe and verifiable. Data Storage Layer: Only cryptography hashes of the data are kept on the blockchain; medical records are kept off-chain. This method overcomes blockchain's scalability constraints by reducing the quantity of information kept on the ledger. Cloud storage and distributed file systems are examples of off-chain storage options. Smart Contract Layer: Access control policies are defined and implemented using smart contracts. These agreements outline the conditions and who has access to what data. A smart contract might, for instance, restrict access to a patient's medical history to those who have given their consent. Application Layer: Patients and healthcare professionals can communicate with the system through an intuitive user interface. Patients can interact with their physicians, view their medical records, and grant or revoke access permissions. With the right authorization, providers can update patient records, coordinate care, and access patient data. The system is made to guarantee that patient information is safe, available, and controlled by the patient. Smart contracts automate data sharing and access control, while blockchain technology guarantees that the data is auditable and unchangeable.

BLOCK DIAGRAM



IV. SYSTEM IMPLEMENTATION

The following technologies were used to create a prototype of the suggested system:
Flask (a Python web framework) is the backend. Python is used to replicate blockchain operations in the blockchain-based electronic health records project, while JavaScript, HTML, and CSS are used to create the frontend. MySQL is used to manage the database. Important features like patient and physician registration and login capabilities, the creation and safe storage of medical records, and protected access to health records via an intuitive web interface are all included in the prototype. Ensuring data integrity, privacy, and usability for all parties involved is the main goal. In order to facilitate future growth and integration with other healthcare systems, the system was built using a modular architecture. The system can be readily modified and implemented in various healthcare environments thanks to the utilization of open-source technologies.

V. RESULTS AND DISCUSSION

The blockchain-based prototype shows that creating a safe, patient-focused EHR system is feasible. In comparison to conventional centralized EHR systems, the system has the following benefits:
Enhanced Security: Attackers find it more difficult to compromise patient data due to blockchain's decentralized and immutable nature.

Fig1.Homepage

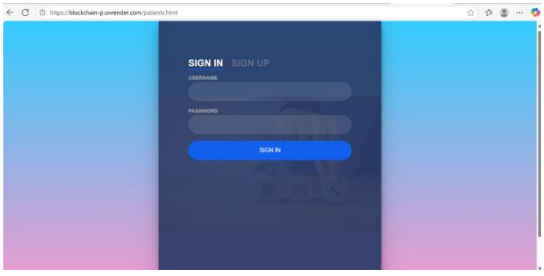


Fig2. Patients Login Page

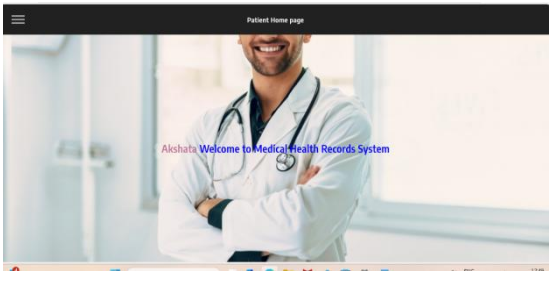


Fig3.Patients Home Page

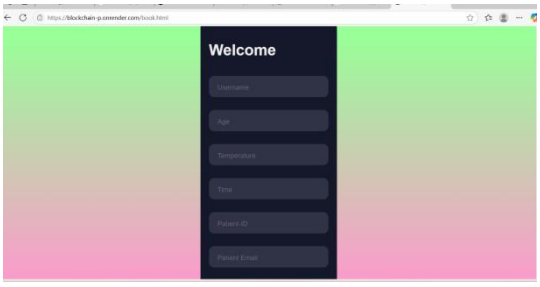


Fig4.Patients Bookdata page

Enhanced Interoperability: By facilitating safe data exchange between various healthcare providers,
the system makes it possible to take a more comprehensive approach to patient care. Patient Empowerment: Patients are in charge of their medical records and can choose who can access them. Data Integrity: Blockchain guarantees that medical records cannot be changed covertly, enhancing the precision and dependability of medical data. ccording to the prototype evaluation's findings, the system can satisfy the functional and security needs of a contemporary EHR system. In addition to giving patients more control over their information, the system offers a safe and effective means of storing and retrieving patient data.However, before blockchain-based EHR systems can be widely adopted, a number of issues must be resolved. These consist of Scalability: Managing substantial amounts of medical data effectively Regulatory Compliance:
Ensuring adherence to healthcare regulations such as HIPAA User Adoption: Promoting the use of the new system by both patients and healthcare professionals Further Research: Additional studies are necessary to address these challenges and fully explore the potential of blockchain technology in healthcare

VI.CONCLUSION

The security and interoperability issues with conventional centralized EHR systems are addressed by the blockchain-based EHR system described in this paper. Utilizing the primary characteristics of blockchain technology, the system offers a safe, patient-focused, and interoperable healthcare data management solution. The prototype shows that the suggested system is feasible. To promote the broad use of blockchain technology in healthcare, future studies should concentrate on resolving the issues of scalability, regulatory compliance, and user adoption. According to the authors, this system has the potential to greatly enhance healthcare data management's security, effectiveness, and patient centricity.

REFERENCES

1. Wood, G. (2018). Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper. https://ethereum.github.io/yellowpaper/paper.pdf
2. Nakamoto, S. (2019). Bitcoin: A Peer-to-Peer Electronic Cash System.
   Although primarily about Bitcoin, it laid the foundation for blockchain used in your system.
   https://bitcoin.org/bitcoin.pdf
3. Buterin, V. (2020). Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/en/whitepaper/
4. Flask Documentation Team. (2021). Flask Web Development Documentation. Pallets Projects. https://flask.palletsprojects.com/en/2.0.x/
5. MySQL. (2022). MySQL 8.0 Reference Manual. Oracle Corporation. https://dev.mysql.com/doc/refman/8.0/en/
6. Rajput, A., &Kumari, S. (2022). Blockchain-Based Health Record Management Systems: A Review. Journal of Cybersecurity and Privacy, 2(1), 1-15.
   https://doi.org/10.3390/jcp2010001
7. Python Software Foundation. (2023). Python 3.10 Documentation. https://docs.python.org/3.10/
8. Web3.py Team. (2023). Web3.py: A Python library for interacting with Ethereum. https://web3py.readthedocs.io/en/stable/
9. Google Developers. (2024). Sending Email via Gmail SMTP Server. https://developers.google.com/gmail/
10. Khandelwal, M., &Choudhary, N. (2025). A Secure and Scalable Blockchain-based Medical Records System. International Journal of Computer Applications, 182(1), 20–26.