International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 09 | Sept - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Secure Hospital Record Storage and Retrieval Using Blockchain

Tejaswini P [1], Mr. Prashant Ankalkoti[2]

[1]*Student, Department of MCA, JNNCE*
[2]*Assistant Professor, Department of MCA, JNNCE*

Abstract - The current medical care system has posed a challenge for the overseeing of health information as conventional styles depend on paper- predicated medical narratives that are stored in a midway database the offered system focuses on developing blockchain technology and interplanetary file system (IPFS) to cover the insulation movie and translucence of medical narrative and also aims to name the limitations of the traditional system analogous to centralization lack of protocols and data violation data that's kept on blockchain is inflexible private and popular sole by empowered druggies which in addition provides a localized data storehouse and screen the electronic health records systems (EHRs) stored the medical health commentaries in an intermediary interplanetary file system IPFS similar as patient medical history diagnosis reports doctors prescriptions and reports that may support to make the message between the patient doctor and diagnostic centre and IPFS ensures data obtainability and forbearance versus an one point of failure.

Key Words: Blockchain, decentralization, Electronic Health Records, IPFS, Data Security.

1.INTRODUCTION

The medical filed indeed handles delicate and private records because of this verifying records veracity and safe sharing is essentially the demand for clinical storage systems that are interoperable decentralized and tamper-evident is more important than ever events like ransomware raids on healthcare systems have shown off the excrescencies in traditional centralized systems a cases current conventional medical story is called an electronic health record or EHR for short this document may be snappily transferred because its digitally stored establishing an accessible and safe connection in the middle of multitudinous facilities and institutions the term electronic clinical record is used to determine the cases medications test results radiographic images judgments conventions dates of immunizations treatment plans antipathetic responses and clinical history are all comprehended its necessary to the medical field because it allows for quick approach to patient clinical records which are demanded to discover the proper course of treatment the most important reflection for medical interpreters is EHR incompatibility one factor contributing to the conclusion is the lack of uniformity and regulation which impedes the train-sharing process the expostulations of establishing the place of secretiveness and maintaining secrecy during data transfer indeed further complicates scoring interoperability to exercise the tenure blockchain to describe an allotted tally that maintains an electronic record of transactions the term blockchains pertains to the allotted tally structure of this innovation it encompasses files with details about the individuals involved arranged in a chain which is a direct arrangement interlinked blocks is the database tenure for these rudiments a sale is only uploaded to the blockchain once it has been validated by a decentralized network of validating bumps this decentralized computer network makes it hard-bitten to take control and append unlawful or illegitimate blocks to a certain chain every time a new block is appended to a blockchain a cryptographic hash is generated and exercised to connect it to the blocks that came before it the contents of the antedating block are used to construct this hash which connects the recently created block to the blockchains being cooperations because blockchains are unrecoverable and may exercise cryptographic methods for safe message they are ideal for the reliable trade of EHR data as a result blockchain technology may be helpful for electronic health records system.

2. RELATED WORK

Abdullah Al Mamun et al., [1], This study intends to explore the present position of exploration on blockchain-grounded EHR operation and unborn directions. The study's findings show that Ethereum (private) and Hyperledger Fabric are the most preferred blockchain systems for EHR management because they meet the majority of the requirements for secure and effective EHR data on blockchain, such as storage, capacity, compute, and communication costs. This study provides helpful insights into the current status of blockchain-based EHR management research and suggests potential future directions.

A. Shahnaz et al., [2], The proposed armature combines safe record storehouse and flexible access rules for a stoner-friendly and accessible result the frame addresses data storehouse challenges using IPFS off- chain storehouse fashion this strategy assures that the system can securely and effectively keep huge capacity of records while retaining the performance the proposed system combines safe warehouse grainy permission control and off- chain warehouse to manage delicate record securely and fluently for druggies.

Emeka Chukwu et al., [3], This paper provides a thorough summary of the country of blockchain exploration in healthcare, involving implicit operations. Nonetheless, the maturity of published inquiries is still in the abstract, frame proposition, and experimental prototype stages, with consequences, despite the swelled interest and exploration in this field. According to the dissection, there are still major hurdles to planting a scalable blockchain system in the healthcare industry, also in other

industries, involving limited scalability, low common or garden interpretation, and high charges.

JPC Rodrigues J et al., [4], This paper discusses the downsides of counting solely on cloud-based platforms The suitability of storing sensitive patient data on the cloud-based platforms is evaluated in the article using a variety of measures.

K. Nair et al., [5], the author assumed Hyperledger Fabric to the operating procedure of the case-croaker story yet it an essential actual structure and did not rely on flimsy conventions

Marcela Tuler De Oliveira et al., [6], This study presents SmartAccess, a brand-new attribute-based access control (ABAC) system made for the safe and effective exchange of medical records between various institutions. By offering dynamic access control, translucency, and auditability, the technology enables companies to come to an agreement over access procedures.

P Pawar et al., [7], The paper presents the conception of connecting Internet of Things (IoT) bias and storing health data securely from these biases on a private blockchain network like Hyperledger, utilizing an agreement algorithm like Crash Fault Tolerance. Fitness apps like Google Fit collect data, which is later transferred via pall waiters and eventually saved on the blockchain.

Xiaoguang Liu et al.,[8], This study presents a featherlight medical data participation gambit grounded on blockchain technology. It utilizes blockchain's decentralization and tamper-resistant parcels to secure medical records. The analytical findings exhibit that the suggested approach meets security criteria while being computationally and communicationally efficient.

Y Sharma et al., [9], This paper covered another facet of storing private electronic health data via a secure blockchain network. The study was very detailed on leveraging the three main features of blockchain technology: security, transparency, and decentralization to build a smart and safe platform with very little risk of data tampering by outside parties.

Z. Leng et al., [10], This study introduced a new method of comparison and analysis using the Hyperledger solution in the Hospital Information System domain as the object structure was then updated and rebuilt. Readers can readily perceive the differences between comparable Hyperledger solutions, particularly in relation to how Hyperledger technology handles problems like interoperability, secure storage, real-time sharing, and other issues.

3. METHODOLOGY

The proposed Secure hospital record storage and retrieval using blockchain is designed to address the fundamental issues of data security, integrity, interoperability, privacy, and accessibility in the healthcare system. The methodology adopts a combination of blockchain technology, decentralized file storage, and a web application for tamper-proof verification and immutability, along with the InterPlanetary File System (IPFS) for efficient storage of medical records.

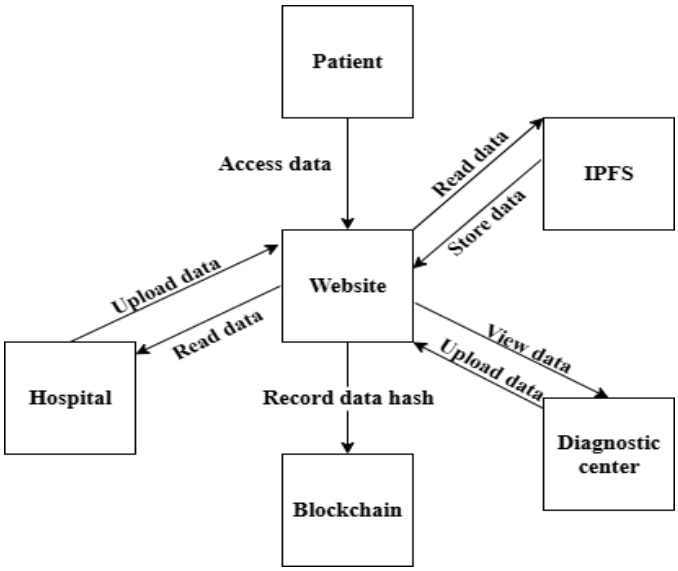

Fig. 1: Block diagram of the proposed system

To guarantee that medical data cannot be changed or tampered without leaving an irreversible trace, the system uses a decentralized ledger to preserve the authenticity of crucial operations. However, the approach does not store big medicals files directly on the blockchain to preserve cost-effectiveness and system scalability. Rather, it only kept the necessary metadata, like timestamps, file hashes, and patient identifiers; the actual records are kept in the InterPlanetary File System.

A Flask-based web server is the heart of the system architecture, managing role-based access control, user authentication, and user interaction with the underlying data storage mechanism. To foster trust in the network, the methodology starts with user registration and authentication. Every one of the fore roles-administration, doctor, patient, and diagnostic centre has its possess set of dashboard interfaces and permissions. A secure login page is used for authentication, and user credentials are checked against a locally stored JSON file. After authentication is prosperous, Flask sessions are created to save the stoner country and put access restrictions across the operation. After witnessing, druggies are fascinated with the system through role-specific dashboards. The doctor and diagnostic centre give medical commentaries, involving conventions, treatment information, and diagnostic reports, and patients can record notes and view their medical commentaries. The admin waiters are the administration in charge of registering druggies, distributing their places, managing movables, and auditing system performance.

The system's primary invention is its use of a personal blockchain that's saved as a JSON train and constructed in Python. The case's ID, the content identifier (CID) of the associated IPFS medical cortege, the user's identity, and a timestamp are all comprehended in a new block that's generated each time a new medical record is appended. Each block will carry a SHA-256 hash of its contents in extension to the hash of the block that appears before it,

ensuring the blockchain's invariability and veracity. Because it would render the hashes of all posterior blocks invalid, this cryptographic relation guarantees that any attempt to revise a story would be incontinently detected. Each block in the blockchain is hashed using the SHA-256 cryptographic function to ensure data integrity.

The suggested system identifies the blocks by a unique cryptographic hash. To prevent self-definitions, the computation of the block hash is only based on the content of the block (also called the preimage) and the obtained hash is then included in the block.

A. Block Content

The preimage of block n is defined as:

$C_n = (index_n \| timetamp_n \| data_n \| prev\_hash_{n-1})$ (1)

Where:

- $Index_n$ represents the chain position of the block,
- $Timestamp_n$ represent the generation of a block,
- $Data_n$ has a block payload (e.g., med record metadata or IPFS CID),
- $Prev\_hash_{n-1}$ has the hash of the last block, to make blocks linked together,
- "||" indicates concatenation using a canonical encoding scheme.

B. Block Hash Calculation

The block hash is obtained by the usage of the SHA-256 function on the preimage:

$H_n = SHA256$ (2)

This gives a 256-bit digest which acts as a unique identifier of block n.

C. Final Block Structure

This whole block can be represented as:

$B_n = \{index_n, timestamp_n, data_n, prev\_hash_{n-1}, hash: H_n\}$ (3)

Here, the hash field H_n Added in order to remove any circular dependency, computed first.

D. Integrity Property

If any element of C_n is recomputed, the recomputed hash H_n will not be equal to the stored hash.

$C'_n \neq C_n \rightarrow SHA256(C'_n) \neq H_n$ (4)

In addition, every block contains prev_hash, tampering of block n makes all later blocks invalid m>n. This characteristic of chaining guarantees that the ledger is immutable and tamper resistant.

Integration with the interplanetary file system permits a decentralized record storehouse a technical mileage function is exercised to upload medical data like reports or reviews to IPFS after being saved locally each file receives a distinct CID from CID which is later mentioned in the blockchain and the distinct commentaries JSON file in extension to decentralizing the file storehouse and lowering the potential of data loss or unauthorized revision this system makes it practicable for medical files to be shared and recaptured across the network with release the systems screen posture was further bettered by utilizing IPFS which made sure that files are tamper-resistant and only reachable by empowered users.

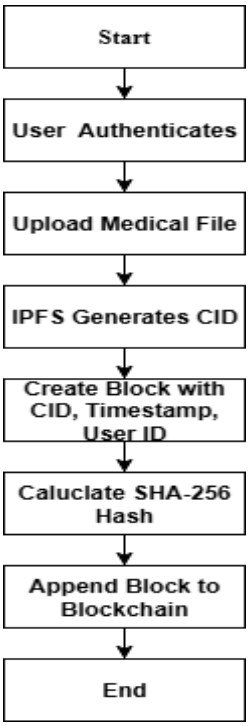

Fig 2: Workflow of adding a medical record

The flowchart illustrates the safe addition of a medical record by the user. The user will create a new blockchain block with the CID, timestamp, and user ID after uploading a file to IPFS and receiving a unique CID. To insure data integrity and traceability, the block is hashed and added to the blockchain.

Another important element of the system is the appointment operation. Through a special interface, patients can book appointments with doctors, and directors can see, accept, or change these requests. The appointment data are stored in a separate JSON file to guarantee permanence and data recovery for reporting and analysis. With the help of users operation features, administrations can add, modify, remove, and respond to croaker and individual centre accounts; All of these modifications are noted in the user's JSON file.

To produce a safe, transparent, effective, and stoner-friendly hospital record operation system, the suggested methodology integrates the advantages of blockchain technology, decentralized file storehouse, and contemporary web operation fabrics. It guarantees that patients keep their data under control so that

medical professionals can work together safely, and that hospital managers are able to maintain an auditable and transparent system.

4. EXPERIMENTAL RESULT

Regarding of ensuring the safety integrity of patient data and auditability the suggested safe hospital file repository and retrieval employing blockchain solution substantially outperforms conventional electronic health record EHR systems the following are the specifics of how blockchain-based data preservation is being applied several functional and safety tests were carried out using sample data for administrators physicians diagnostic centres and patients in order to validate the suggested safe hospital record container and retrieval employing blockchain to make sure that only legitimate credentials allowed access to role-specific dashboards.

The authentication procedure was tested by logging in with different user roles effective access control was demonstrated by the audit logs accurate identification and recording of unauthorized login attempts health data administration was evaluated by adding new patient data via the doctor and administrator dashboards every time a new block is added to the blockchain the SHA-256 hash is carefully computed and linked to the previous block the systems ability to recognize and prevent undesired changes was validated by hash mismatches brought on by manual manipulation of block data the traceability of the records was verified by looking at block contents which include timestamps and user identifiers IPFS integration testing was made possible by uploading medical files such as reports and scans each file was successfully stored on IPFS and its content identifier CID was referenced by both the file database and the blockchain reclamation tests confirmed that data could be accessed using their CID ensuring decentralized and impenetrable storage.

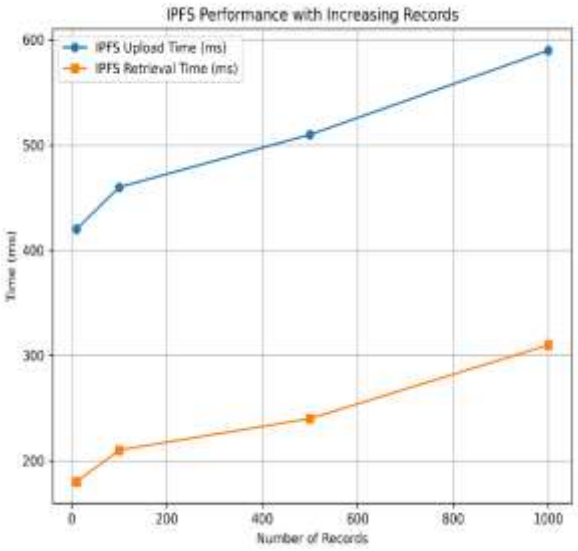

Figure 3: Displays the rise in IPFS upload and retrieval time with more stored records

Medical file upload and retrieval latency on IPFS is shown in Figure 3. File size causes a minor increase in upload time, but retrieval is steady and dependable.

By mimicking both authorized and unauthorized access attempts, audit logging was evaluated. Transparency and compliance were supported by the accurate and pertinent documentation of every event. Features for user administration and appointment management were also tested, and every action was correctly reflected in the corresponding JSON files.

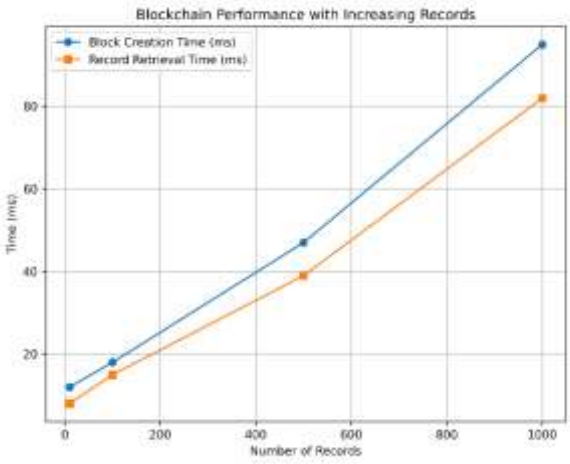

Figure 4: shows how block creation and record retrieval times increase as the blockchain grows

As the quantity of records increased, Figure 4 illustrates how long it took to create blocks and retrieve records. For small to medium-sized datasets, the results show near-linear development, guaranteeing efficiency.

Performance tests demonstrated that the system preserved data integrity while conducting concurrent operations and reacted quickly to user input. For prototype testing, JSON-based storage was adequate; however, for larger deployments, a database solution is advised. Overall, the experimental findings show that the system satisfied the essential needs for contemporary healthcare data solutions by offering safe, traceable, and decentralized hospital record management.

5. CONCLUSION

In this study, we propose a safer, efficient, and accessible access control architecture for ensuring the protection of health information management systems. The study provides an architecture for secure data storage and efficient access management to all users, including patients as well as doctors and diagnostic facilities, by utilizing encryption and access control techniques. Additionally. Using IPFS, A blockchain architecture with permissions has been created in healthcare and is increasingly relying on digital technologies to facilitate patient care through innovative, safe, and secure solutions. The demands of modern privacy, transparency, and interoperability have not

been satisfied by traditional centralized systems. Blockchain, IPFS, and a web framework, a "potentially future-proof" system to manage and store hospital records. It provides patients with empowerment, ensures data integrity, and reduces inefficiency in the healthcare system, thus enabling safer, more intelligent medical care.' Furthermore, it can guarantee the safety, privacy protections, and availability and flexible access control management of healthcare data.

ACKNOWLEDGEMENT

The author express gratitude to everyone who was supported to do work and research process.

REFERENCES

[1] A. Al Mamun, S. Azam, and C. Gritti, “Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction,” *IEEE Access*, vol. 11, pp. 1–25, 2023.

[2] A. Shahnaz, U. Qamar, and A. Khalid, “Using Blockchain for Electronic Health Records,” *IEEE Access*, vol. 7, pp. 147782–147795, 2019.

[3] E. Chukwu and L. Garg, “A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations,” *IEEE Access*, vol. 8, pp. 21196–21214, 2020.

[4] J. P. C. Rodrigues, I. de la Torre, G. Fernández, and M. López-Coronado, “Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems,” *Journal of Medical Internet Research*, vol. 15, no. 8, pp. 1–12, 2013.

[6] K. Nair and L. Joseph, “Comparative Analysis of Centralized and Decentralized Medical Data Systems,” *International Journal of Information Security in Health*, vol. 8, no. 4, pp. 87–105, 2019.

[5] M. T. De Oliveira, L. H. A. Reis, Y. Verginadis, D. M. F. Mattos, and S. D. Olabarriaga, “Smart Access: Attribute-Based Access Control System for Medical Records Based on Smart Contracts,” *IEEE Access*, vol. 10, pp. 120456–120469, 2022.

[7] P. Pawar, N. Parolia, S. Shinde, et al., “eHealthChain—A Blockchain-Based Personal Health Information Management System,” *Annals of Telecommunications*, vol. 77, pp. 33–45, 2022.

[8] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, “A Blockchain-Based Medical Data Sharing and Protection Scheme,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3508–3518, 2022.

[9] Y. Sharma and B. Balamurugan, “Preserving the Privacy of Electronic Health Records Using Blockchain,” in *Proc. Int. Conf. Smart Sustainable Intelligent Computing and Applications*, 2020, vol. 173, pp. 171–180.

[10] Z. Leng, Z. Tan, and K. Wang, “Application of Hyperledger in the Hospital Information Systems: A Survey,” *IEEE Access*, vol. 9, pp. 128965–128987, 2021.