

Health Data Exchange governed by Ledger Systems with Secure Distributed Storage Mechanisms

G. Sandhya Rani¹, Vasakula Rakshith², Thurpati Saikumar², Banothu Akhil², K Parusharamudu²

¹Assistant Professor, ²UG Student, ^{1,2}Department of Computer Science and Engineering

^{1,2}Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India.

ABSTRACT

The rapid advancement of digital technologies in healthcare has increased the need for secure, transparent, and efficient management of medical data. However, most existing systems rely on centralized architectures, where sensitive patient information is controlled by a single authority. This creates vulnerabilities such as data breaches, unauthorized access, and single points of failure, which can compromise data integrity and patient privacy. The core problem addressed in this research is the lack of a decentralized and tamper-resistant mechanism for managing Electronic Health Records (EHR). Current solutions often suffer from limited transparency, inefficient data sharing between patients and doctors, risks of data manipulation, dependency on intermediaries, and scalability issues due to large medical files like reports and prescriptions. To address these challenges, this research proposes a blockchain-based healthcare management system integrated with the Inter-Planetary File System (IPFS). Blockchain technology, implemented using Ethereum and Web3, ensures secure, immutable, and transparent transaction handling through smart contracts. IPFS is used for decentralized storage of medical files, with only cryptographic hashes stored on the blockchain to reduce storage overhead while maintaining data integrity. The system enables patients to book appointments, upload medical reports, and securely share them with doctors. Doctors can access records, provide diagnoses, and generate prescriptions, which are also stored via IPFS and linked to the blockchain. This ensures that data cannot be altered without detection, enhancing trust. The proposed system improves data security, privacy, reliability, and scalability in healthcare data management.

Key words: Blockchain, Electronic Health Records (EHR), InterPlanetary File System (IPFS), Ethereum, Web3, Smart Contracts, Decentralized Systems, Healthcare Data Security, Data Privacy, Medical Data Management,

1. INTRODUCTION

The rapid adoption of digital health technologies and e-health platforms has significantly transformed modern healthcare by enabling services such as remote patient monitoring, telemedicine, and efficient management of Electronic Health Records (EHR). However, this growing dependence on digital infrastructure has introduced critical security and privacy challenges, including unauthorized data access, data breaches, and identity theft [1]. Conventional authentication mechanisms, such as password-based systems and two-factor authentication (2FA), are insufficient to address these issues due to their vulnerability to cyberattacks, lack of scalability, and limited capability to establish strong trust among users [2]. As a result, there is a pressing need for a more secure, scalable, and robust authentication and access control framework in healthcare systems. Figure 1 illustrates a blockchain-based authentication and access control model designed for e-health users.

Blockchain technology provides a decentralized, immutable, and cryptographically secure environment that can effectively address these challenges by ensuring data integrity and secure access management without relying on a central authority. Through distributed ledger mechanisms and consensus protocols, blockchain enables reliable authentication and controlled data sharing. Prior studies have demonstrated that blockchain-based authentication frameworks leveraging Practical Byzantine Fault Tolerance

(PBFT) improve privacy-preserving authentication, although they may still face computational and storage constraints [3]. Similarly, privacy-focused access control models incorporate techniques such as Geometric Data Perturbation (GDP) and K-means clustering to strengthen security, but scalability remains a concern, particularly in Internet of Medical Things (IoMT) environments. Advanced encryption methods like Searchable Attribute-Based Encryption (SABE) provide fine-grained access control and ensure confidentiality of medical data, yet they often introduce high computational overhead and latency during decryption [4].

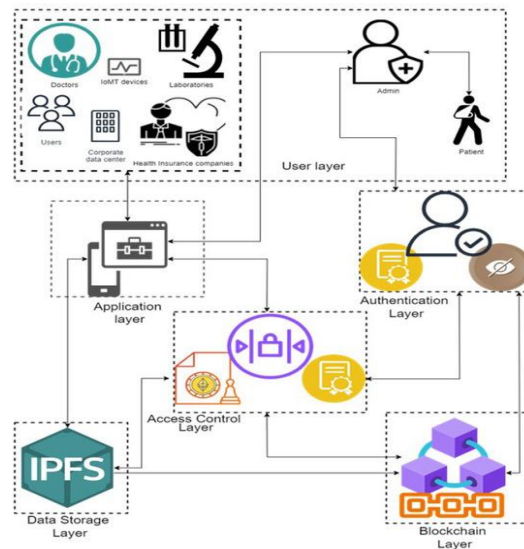


Figure 1: blockchain-based authentication and access control model for e-health users.

Additionally, privacy-preserving frameworks utilizing zero-knowledge proofs (ZKP) and blockchain-based privacy coins support compliance with General Data Protection Regulation (GDPR) standards, but they are associated with increased transaction costs and performance limitations. Despite its advantages, blockchain integration in e-health systems is still challenged by issues such as processing latency, high computational requirements, storage limitations, and synchronization delays between on-chain and off-chain data, which can impact real-time data accessibility [5].

2. LITERATURE SURVEY

Alabdulatif, A., et al. [6] presented a blockchain-based paradigm for privacy-preserving authentication and access control specifically designed for e-health systems. The architecture utilises the Ethereum blockchain, smart contracts, blind signatures, Proof of Authority (PoA) consensus, and one-way hash functions to improve data integrity, security, and privacy in a decentralised framework. The proposed methodology addresses computational efficiency and scalability issues via the implementation of lightweight cryptographic techniques, achieving an average authentication delay of 0.059 milliseconds, which represents a 4000-fold improvement compared to current approaches, demonstrating significant performance optimization. Tahir, N.U.A., et al. [7] investigated the potential of blockchain technology to transform Electronic Health Record (EHR) administration, integrity, and security. EHRs store vital health information such as medical history, diagnosis, prescriptions, and imaging findings, which may be shared with healthcare professionals to improve patient care. The existing EHR systems have a centralized framework, leading to single points of failure, data management limitations, and security vulnerabilities, which blockchain aims to overcome through decentralization and immutability.

Hussien, H.M., et al. [8] developed this study bridges the gap between PHRs and blockchain technology by offloading the vast medical data into the InterPlanetary File System (IPFS) storage and establishing

an enforced cryptographic authorisation and access control scheme for outsourced encrypted medical data. The access control scheme is constructed on the basis of the lightweight cryptographic concept named smart contract-based attribute-based searchable encryption (SC-ABSE), enabling efficient, secure, and scalable data sharing while preserving confidentiality. Ryu, J., et al. [9] proposed a new authentication protocol to prevent and address security issues within hospital systems. The proposed protocol encrypts medical records on a private blockchain, allowing them to be securely shared among institutions, hospitals, and insurance companies. This ensures data availability and recovery even if a ransomware attack paralyzes the server, thereby enhancing resilience and fault tolerance in healthcare systems.

Hashim, F., et al. [10] proposed a transaction-based smart contract triggering system for inter-blockchain communication, enabling EHR sharing among independent blockchains. They use local and global smart contracts that execute automatically upon transaction creation. Local smart contracts manage intra-blockchain data exchange, whereas global smart contracts enable interoperability across different blockchain networks, improving scalability and cross-domain data accessibility. Shojaei, et al. [11] developed this systematic literature review identifying various technologies and methods employed to enhance the security and privacy of medical data within HISs. Technologies such as IoT, blockchain, mobile health applications, cloud computing, and hybrid approaches are analyzed, highlighting their roles in strengthening healthcare data protection and enabling secure digital transformation.

Mani, et al. [12] presented an innovative patient-centric healthcare data management (PCHDM) system comprising on-chain and off-chain components. On-chain storage maintains hashes of health records in Hyperledger Fabric, while off-chain solutions encrypt and store actual data in IPFS. This hybrid architecture ensures scalability, confidentiality, and efficient storage management while addressing blockchain storage limitations. Mandarino, V., et al. [13] evaluated key challenges associated with large-scale data management, particularly cost and performance issues in blockchain systems. A hybrid decentralized application (dApp) architecture was proposed, where medical records are stored locally on user devices, while blockchain maintains indexing and metadata, balancing efficiency, privacy, and decentralization.

Sonkamble, R.G., et al. [14] suggested a decentralized patient-centered healthcare data management (PCHDM) with a blockchain-based EHR framework to address issues of confidentiality, access control, and privacy of record. This patient-centric architecture keeps the patient at the center of control for secured storage of EHR data. It is effective in the storage environment with the interplanetary file system (IPFS) and blockchain technology. In order to control unauthorized users, the proposed secure password authentication-based key exchange (SPAKE) implements smart contract-based access control to EHR transactions and access policies. Reegu, F.A., et al. [15] defined the interoperability issues in the existing blockchain-based EHR frameworks, reviews various national and international standards of EHR, and further defines the interoperability requirements based on these standards. The proposed framework can offer safer methods to interchange health information for the healthcare sector and can provide the properties of immutability, security, and user control on stored records without the need for centralized storage.

3. PROPOSED SYSTEM

A blockchain-based protocol for secure healthcare record management, designed to address limitations of traditional systems such as unauthorized access, data tampering, and inefficient record management. The system integrates blockchain, smart contracts, and IPFS storage to create a decentralized, secure, and transparent environment. Patients, doctors, and administrators interact with the system through a user-friendly interface, enabling actions such as uploading medical reports, generating prescriptions,

and booking appointments while maintaining strict access control. The architecture is divided into three main layers: the user interface layer, the blockchain and smart contract layer, and the IPFS storage layer as shown in Figure 2. Users authenticate themselves using their credentials, after which smart contracts validate requests and enforce access permissions. Medical records are stored on IPFS, and the corresponding hash is recorded on the blockchain, ensuring data immutability and verifiability. This combination of technologies prevents unauthorized modifications and provides an audit trail for all healthcare transactions. The system follows a sequential operational workflow that guarantees security, efficiency, and traceability. Each step, from user authentication to record retrieval, is designed to ensure that sensitive patient data is protected while remaining accessible to authorized personnel. By combining decentralized storage with cryptographic security, SEC-HEALTH provides a robust and scalable solution for modern healthcare data management.

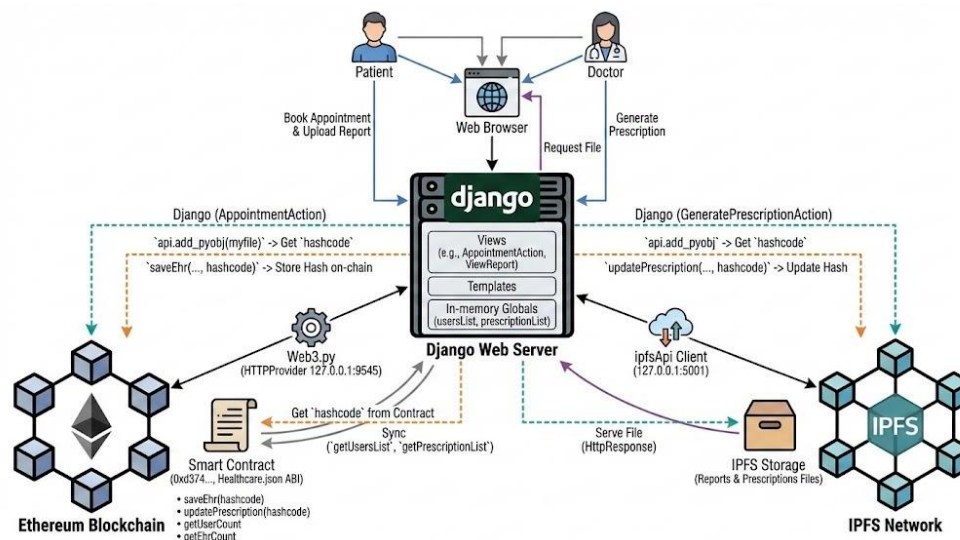


Figure 2: Operational Workflow of health System.

- Patients, doctors, or administrators log in through the web interface.
- Users submit requests such as appointment bookings, report uploads, or prescription updates.
- The smart contract verifies the request, enforces access control, and records the transaction.
- Large files (medical reports, prescriptions) are uploaded to IPFS and a unique content-addressed hash is generated.
- The hash and transaction details are stored on the blockchain for immutability and traceability.
- Authorized users retrieve records by accessing IPFS using the blockchain-stored hash.
- All transactions are logged for monitoring, auditing, and verification.

4. RESULTS ANALYSIS

The results section presents the key findings of the study in a clear and structured manner. It highlights the main outcomes derived from data analysis, often using tables, graphs, or summaries for better understanding. This section focuses only on what was observed, without interpretation or discussion. Important patterns, trends, and relationships in the data are described concisely. The aim is to provide factual evidence that directly relates to the research objectives. It serves as the foundation for further discussion and conclusions.

Figure 3 depicts the confirmation of an appointment booking between a patient and a doctor. It illustrates how the system records the booking details along with blockchain transaction information for verification. The figure represents the successful execution of appointment scheduling through secure

processing. It highlights how transaction receipts ensure transparency and traceability of operations. The inclusion of appointment ID and doctor details confirms that the booking has been completed. This screen reflects the system's ability to maintain reliable and tamper-proof records.

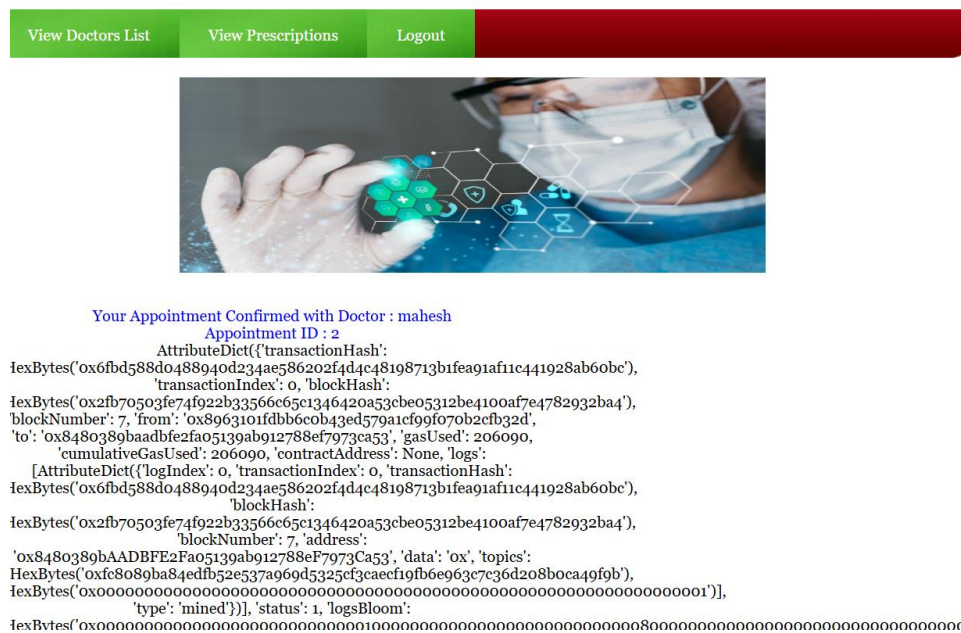


Figure 3: Appointment Confirmation with Doctor.



Figure 4: View Appointments.

Figure 4 illustrates the appointment management interface where doctors can view all scheduled appointments associated with their profile. It depicts how detailed information such as patient name, doctor name, disease description, report details, and booking date are organized in a structured format. The figure represents the integration of medical data stored through decentralized mechanisms, where report references are linked using secure hash values. It highlights how doctors can access reports and initiate prescription generation directly from the appointment record. The presence of actionable options indicates the system's capability to support real-time clinical decision-making. This screen reflects the seamless interaction between data retrieval, verification, and medical workflow execution.

Figure 5 depicts the confirmation screen displayed after successfully updating a prescription within the system. It illustrates the completion of the prescription generation process performed by the doctor. The

figure represents how the system acknowledges successful execution of the operation and ensures that the updated data is securely recorded. It highlights the backend integration where prescription details are stored in decentralized storage and linked through blockchain transactions. This screen confirms that the operation has been validated and processed without errors. It also reflects the reliability and responsiveness of the system in handling critical healthcare updates.



Figure 5: Prescription Update Confirmation.

5. CONCLUSION

The Blockchain and IPFS-based Healthcare Record Management System provides a secure, reliable, and decentralized solution for managing medical data. By integrating IPFS for distributed storage and blockchain for immutable record keeping, the system ensures that sensitive healthcare information remains protected from unauthorized access and tampering. The use of cryptographic hashing guarantees data integrity, while smart contracts automate key operations such as authentication, record updates, and access control. The integration of Django with Web3 and IPFS enables smooth coordination between application logic and decentralized components. The system effectively overcomes limitations of centralized architectures by eliminating single points of failure and improving transparency. It also supports efficient data sharing among patients and doctors through role-based access control mechanisms. The architecture demonstrates improved scalability, reliability, and fault tolerance in handling healthcare data.

REFERENCES

- [1] Sharma, A.; Kaur, S.; Singh, M. A secure blockchain framework for the internet of medical things. *Trans. Emerg. Telecommun. Technol.* 2024, 35, e4917.
- [2] Preetha, A.D.; Kumar, T.P. Securing IoT-based healthcare systems from counterfeit medicine penetration using Blockchain. *Appl. Nanosci.* 2023, 13, 1263–1275.
- [3] Yakubu, B.M.; Ali, S.M.; Khan, M.I.; Bhattarakosol, P. PatCen: A blockchain-based patient-centric mechanism for the granular access control of infectious disease-related test records. *PLoS ONE* 2024, 19, e0310407.
- [4] Altaf, A.; Iqbal, F.; Latif, R.; Yakubu, B.M.; Latif, S.; Samiullah, H. A survey of blockchain technology: Architecture, applied domains, platforms, and security threats. *Soc. Sci. Comput. Rev.* 2023, 41, 1941–1962.
- [5] Javed, L.; Yakubu, B.M.; Waleed, M.; Khaliq, Z.; Suleiman, A.B.; Mato, N.G. Bhc-iot: A survey on healthcare iot security issues and blockchain-based solution. *Int. J. Electr. Comput. Eng. Res.* 2022, 2, 1–9.
- [6] Alabdulatif, A. Blockchain-Based Privacy-Preserving Authentication and Access Control Model for E-Health Users. *Information* 2025, 16, 219. <https://doi.org/10.3390/info16030219>.

- [7] Purmani, S. S. R. (2025). Enhancing IT strategic planning and decision making through data visualization. *International Journal of Enhanced Research in Management & Computer Applications*, 14(4), 75–81.
- [8] Kalae, U. K. (2021). Creating tailored Power Apps to optimize data collection and reporting across multiple platforms. *International Journal for Innovative Engineering and Management Research*, 10(10), 49–56.
- [9] Hashim, F.; Shuaib, K.; Sallabi, F. Connected Blockchain Federations for Sharing Electronic Health Records. *Cryptography* 2022, 6, 47. <https://doi.org/10.3390/cryptography6030047>.
- [10] Shojaei, P.; Vlahu-Gjorgievska, E.; Chow, Y.-W. Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review. *Computers* 2024, 13, 41. <https://doi.org/10.3390/computers13020041>.
- [11] Poojari, R. (2024). Empirical Analysis of Context Window Enhancement Methods in Retrieval-Augmented Generation Models. *Journal of Computational Analysis and Applications*, 33(2).
- [12] Mandarino, V.; Pappalardo, G.; Tramontana, E. A Blockchain-Based Electronic Health Record (EHR) System for Edge Computing Enhancing Security and Cost Efficiency. *Computers* 2024, 13, 132. <https://doi.org/10.3390/computers13060132>.
- [13] Sonkamble, R.G.; Bongale, A.M.; Phansalkar, S.; Sharma, A.; Rajput, S. Secure Data Transmission of Electronic Health Records Using Blockchain Technology. *Electronics* 2023, 12, 1015. <https://doi.org/10.3390/electronics12041015>.
- [14] Reegu, F.A.; Abas, H.; Gulzar, Y.; Xin, Q.; Alwan, A.A.; Jabbari, A.; Sonkamble, R.G.; Dziyauddin, R.A. Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System. *Sustainability* 2023, 15, 6337. <https://doi.org/10.3390/su15086337>.