DMPedia Lecture Notes in Computer Science & Engineering
Volume 1, pp. 377-385 2026

International Conference on Multidisciplinary Perspectives in Advanced Computing and Technology (IMPACT 2026)
G. B. Pant University of Agriculture and Technology, Uttarakhand, India. Jan. 10-11, 2026

Blockchain Based Electronic Health Record System

Ansh Pachauri, Aman Kumar Dubey, Anurag Singh, Ankit Kr Singh

Computer Science and Engineering, Galgotias College of Engineering and Technology, Greater Noida, U.P., India

anshpachauri303@gmail.com, aman1dubey122@gmail.com, anurag26official@gmail.com, ankit271975@gmail.com

Abstract:

The rapid digitisation of healthcare has led to widespread adoption of Electronic Health Records (EHRs); however, the majority of currently available systems are based on centralised designs that are vulnerable to security breaches, lack interoperability, and fail to provide adequate patient control. Centralised data repositories are likely to suffer from unauthorised access, data breaches, and single points of failure, while fragmented systems limit the smooth exchange of information between healthcare institutions. The alternatives provided by blockchain technology include a decentralised, tamper-resistant solution that encompasses immutable records, cryptographic security, and auditability. The paper proposes a Blockchain-Based Health Record System that integrates blockchain technology with smart contracts, AES-256 encryption, and the InterPlanetary File System (IPFS) to ensure security, scalability, and patient-centred healthcare data management. In the suggested design, IPFS, which can encrypt and store medical records off-chain, is used to handle access control, consent enforcement, and audit logs, while a blockchain smart contract handles these functions. The suggested system will increase data confidentiality, eliminate single points of failure, and enable data sharing among medical professionals. The system corresponds with the current data protection rules and ethical medical care, as it provides patients with complete ownership and control over their medical records. The paper shows that EHR systems with blockchain have the potential to enhance the security, transparency, and interoperability of digital healthcare ecosystems.

Keywords: Access control, Blockchain, Decentralization, EHR, Encryption, Healthcare Security, IPFS, Smart contracts

1. **Introduction**

Healthcare systems generate a considerable amount of sensitive patient information that must be kept safe and shared effectively to facilitate clinical decision-making and continuity of care. The use of Electronic Health Records (EHRs) has enhanced access and operational efficiency, but most EHR systems are centralised and controlled by institutions. These architectures pose significant risks, including single points of failure, exposure to cyberattacks, insider access, and large-scale data breaches. Poor interoperability is another significant problem of traditional EHR systems. The patient records tend to be passed across different hospitals, laboratories and clinics through incompatible standards, and this creates a lack of completeness in the medical history of the patient and retards the treatment. In any emergency situation, the lack of access to patient data, along with inaccurate details, can have a devastating effect on clinical outcomes. The absence of patient autonomy in the current systems is also of great importance. The patients usually possess limited visibility to the access, sharing, and reuse of their medical data. Consent systems are also usually non-interactive and non-transparent, which erodes trust and contradicts the current privacy laws. The blockchain technology offers a decentralized way of addressing these challenges by allowing the ability to manage data without tampering, cryptographic security and transparent audit trails, without necessarily having a central authority. Blockchain can enable secure, interoperable and patient-centric healthcare data systems when combined with encryption and decentralised storage. The present paper proposes a blockchain-based health record system that will enhance data protection, confidentiality, and interoperability, while enabling patients to retain complete control over their medical records.

2. Literature Review

The recent surge in digital healthcare systems has led to widespread adoption of Electronic Health Records (EHRs) to enhance clinical efficiency, reduce paperwork, and enable faster access to patient information. Nevertheless, the majority of traditional EHRs are built on centralized architectures, whereby the patient data is kept and managed by each hospital or service provider. Several studies have reported that centralised systems are associated with key shortcomings that include a lack of fault tolerance, exposure to cyberattacks, incompatibility, and that patients have insufficient control over their sensitive medical information. Such problems have prompted developers to develop other architectures that are more secure, transparent, and trustworthy. Initial studies of EHR systems focused primarily on improving digitization and accessibility and not with security. N. Zheng[1] also found that the older versions of EHR platforms improved administrative efficiency, yet they were not highly encrypted, had no strong access control, and did not have standardized interoperability mechanisms. It was revealed that centralized databases were susceptible to data breaches, insider abuse as well as sharing of patient records without permission.

Blockchain technology provides a potential solution to these issues because it is decentralized, immutable and transparent. It was not long before researchers realized that these properties are compatible with the needs of healthcare requirements such as data integrity, traceability and resistance to tampering. N. Zheng[1] compared blockchain structures and noted their potential to provide an irrevocable audit trail and secure validation of data across distributed networks. MedRec, proposed by A. Azaria[2] was one of the first blockchain-based health care systems; it manages access permissions but stores actual medical records off-chain. Their plan showed how medical information could be decentralised to patients by adding metadata to the blockchain, and patients receiving and providing access on a case-by-case basis. Although MedRec has greatly enhanced transparency and patient-centric access management, the authors acknowledged scalability constraints and performance costs in implementing the solution on open blockchains. To address the limitation of blockchain storage, a number of researchers suggested hybrid designs that it could be used with off-chain storage systems. X. Yue[3] proposed a healthcare data sharing model, where metadata and access logs are stored on the blockchain, whereas encrypted medical files are kept outside. Their effort indicated that the distinction between data storage and access control enhances the scalability and minimizes the transaction costs. In a similar fashion, B. Shen[4] introduced MedChain, which utilises blockchain as an indexing and authorisation tool and relies on third-party storage for large medical datasets. J. Benet[5] proposed the InterPlanetary File System which has been popular in blockchain-based healthcare research as a decentralized storage platform. IPFS is a location-based addressing system that uses content addresses, which ensures data integrity and tamper resistance capabilities. Several experiments showed that IPFS can be used together with blockchain to provide a decentralized storage of massive medical data (diagnostic images and reports) at a low cost without compromising decentralization. It was stated that IPFS leads to a significant reduction in the storage overhead of a blockchain network and enhances system performance. Access control and consent management in blockchain-based healthcare systems rely heavily on smart contracts. T.-T. Kuo[6] highlighted the fact that smart contracts allow rule-based self-executing authorization processes that do not require the use of intermediaries. Using blockchain logic to encode access policy ensures that permission enforcement is consistent as well as access events are immutably logged. Sternat also emphasised the idea that smart contracts increase trust between stakeholders by providing transparent, verifiable access control without manual policy enforcement. The other requirement for secure healthcare data management is the use of cryptographic techniques. The encryption of sensitive medical records with NIST[7] AES-256 is generally highly recommended as it has high security provisions and it is also efficient. M. J. Dworkin[8] wrote about the appropriateness of AES-256 to large data volumes and its resistance to brute-force attacks. A number of studies used a hybrid cryptography method, where data confidentiality was achieved by using symmetric encryption, but a secure key exchange was implemented by using asymmetric encryption. Nevertheless, few studies in the existing literature discuss the major management strategies, which is a major challenge. To conclude, the available literature shows that blockchain, together with smart contracts, encryption, and decentralized storage, can greatly improve the safety and transparency of the healthcare data management systems. Nevertheless, there are still gaps in scalability, usability, efficient off-chain storage integration, and all-inclusive patient-centric access control. This paper builds upon prior studies by proposing with a suggestion of a hybrid blockchain-based health record system that combines AES-256 encryption, IPFS-based decentralized storage, and smart contract-based access control to overcome these limitations and provide scalability, security, and patient data sovereignty. designations.

3. Methodology

The system presented in this paper proposes a Blockchain-Based Health Record System which is expected to guarantee the safe, decentralized, and patient-centered management of electronic health records. The implementation is an web-based application, which is connected to a blockchain platform (e.g., Ethereum or Hyperledger Fabric) to provide immutability and transparency, and have reliable access control. Before storing the medical records, the AES-256 medical records including prescriptions, laboratory reports, diagnostic images, and treatment histories using AES-256 encryption. The encrypted files are recorded on InterPlanetary File System that provides decentralized and scalable data storage. In every file, a unique content identifier is created that is placed on the blockchain using smart contracts alongside access metadata. Smart contracts systematically control authorization where patients get to choose access to healthcare providers or withdraw the access. Access events are permanently registered on the blockchain which is accountable and auditable. The decentralized system enhances the interoperability of healthcare facilities without reducing the privacy of data, security, and patient ownership.

2. System Architecture

The proposed Blockchain-Based Health Record System has a hybrid and decentralized system architecture that provides security, scalability, and patient-centric data management. The architecture is divided into four major layers, namely, the user interface layer, the application layer, the blockchain layer, and the storage layer, blockchain layer. Patients and healthcare providers have their own dashboards in a web-based application, which are provided through the user interface layer. The application layer is implemented using Node.js which processes authentication, file encryption and communication with blockchain and storage services. The medical records are not stored in the blockchain, instead, encrypted metadata and content identifiers are logged. The storage layer is based on the InterPlanetary File System (IPFS) to store encrypted medical files in a decentralized format. The AES-256 encryption ensures data confidentiality prior to storage. This multi-layered architecture will allow secure sharing of data as well as fine-grained access control and enable healthcare institutions to interact with one another as well as meet the standards of healthcare data protection.

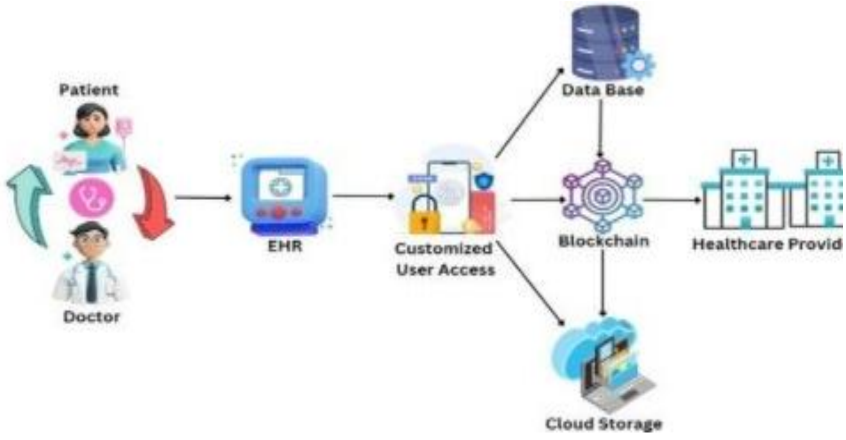


Fig. 1. System Architecture

Source: Blockchain Technology in Healthcare: A Systematic Review and Future Research Directions [9]

3. Use Case Diagram

The use-case of this application consists of three important entities which are an Admin, a patient, and a doctor which would be used to fulfill efficient and safe healthcare administration:

1. Patients: The smart contracts would allow patients to safely access their medical test reports and manage the sharing of their data. They create their online identity in the form of accounts and passwords, which enables them to see specially tailored treatment plans.

2. Doctors: The doctors participate in adding and updating of patient medical records as well as validating them. They also openly prescribe drugs using the blockchain. They are also able to demand a patient record through contract addresses to enable a smooth retrieval of the information to make informed medical decisions.

3. Admin: Admin are important in managing the functionality of systems. They control the user accounts, such as doctor and patient accounts, and the general integrity of the decentralized healthcare ecosystem.

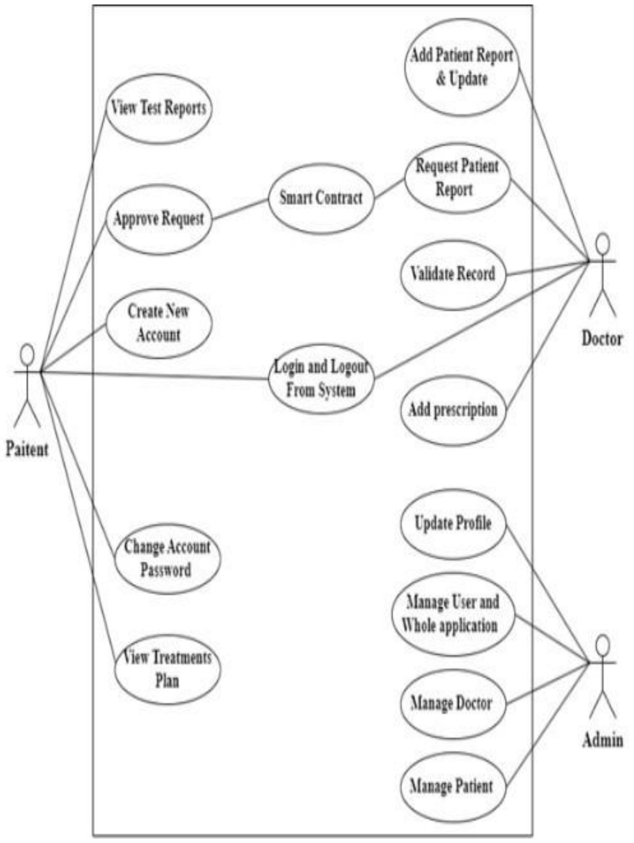


Fig. 2. Use Case Digram

4. Tools and Protocols

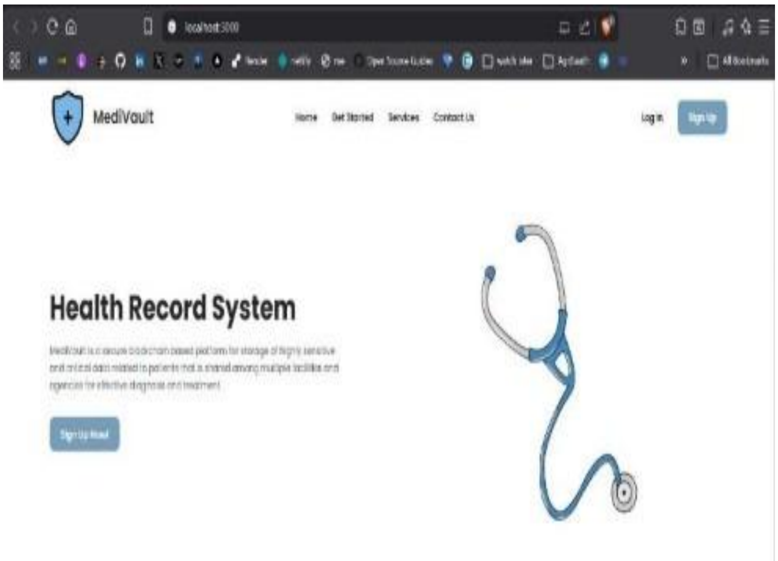
The Blockchain-Based Health RecordSystem implementation is based on the use of both the latest development tools and the security protocols to guarantee reliability, security, and interoperability. The main blockchain platforms applied to implement the smart contracts and decentralized access control are Ethereum and Hyperledger Fabric. The code used to implement smart contracts is Solidity with Ethereum and chaincode with Hyperledger Fabric.The development of the backend services is carried out with the help of Node.js and Express.js are used to performuser authentication, encryption tasks, blockchain transactions, and file handling. A web-based user interface is implemented using React.js, which offers patient and healthcare provider specific dashboards. InterPlanetary File System is adopted as a decentralized storage architecture of encrypted medical records that allows storage of content-addressable data at a large scale. To gain confidentiality of medical data, it is encrypted using AES-256 before storage. Web3.js and MetaMask allow one to use secure blockchain communication and signature on transactions. The components of the system are all connected b through HTTPS and the application of the RESTful API that guarantees safe exchange of data and interoperability within the system..

5. Result

The proposed Blockchain-Based Health Record System was evaluated in terms of functionality, security, and performance. The system based on a hybrid blockchain and decentralized storage architecture provided solid evidence of security in electronic health records storage and retrieval. All medical records were encrypted with AES-256 encryption, and hence during storage and retrieval, ensured data confidentiality before being saved into the InterPlanetary File System. The implementation of smart contract-based access control mechanisms went as intended whereby patients were able to issue and revoke access permissions dynamically. All the transactions and access requests were permanently recorded on the blockchain, which formed the audit trail that was clear and verifiable. Off-chain storage reduced blockchain storage overhead by a significant margin through content identifiers (CIDs) to ensure the integrity of data. There were strong interoperability of the frontend, backend, blockchain network and decentralized storage services. Although unauthorized attempts to access information were denied and logged, authorized healthcare providers could efficiently retrieve and decrypt medical records. These results verify that the suggested strategy is effective in enhancing patient control, security, and transparency when managing electronic health records.

1. Home Page

The homepage of the system is also available via the creation of the user accounts and can be considered the main entry point into the application. It is through this home page that users access the system. It has a signup form and a login form to patients and specific addresses of doctors and admins.



Health Record System

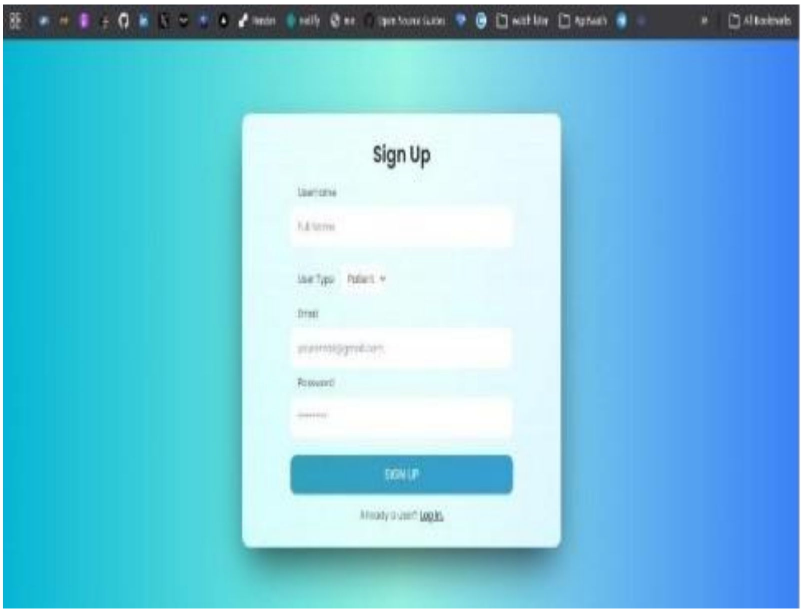
MediVault is a secure blockchain based platform for storage of highly sensitive and critical data related to patients that is shared among multiple facilities and agencies for effective diagnosis and treatment.

Fig. 3. Home Page

The different categories of users (doctors, patients and admins) should have their separate accounts to access the pages. Any attempt to use wrong or duplicate information when creating an account of the administrator will lead to access denied.

2. Registration Page

New users can create an account in the system by entering the necessary credentials on the sign-up page. In addition to entering a username and choosing a user type (patient, doctor, or administrator), users must also supply a working password and email address. The system safely add the user into system and it assigns the user the appropriate access premissions as per the type of role.



Sign Up

Username

Full Name

User Type Patient

Email

youremail@gmail.com

Password

••••••••

Fig. 4. Registration Page

6. Conclusion

In this paper, a safe and decentralized health record system based on blockchain was introduced to overcome the main weaknesses of the conventional Electronic Health Record (EHR) systems. The proposed system provides confidentiality, integrity, transparency, and patient-centricity of healthcare data by combining blockchain technology and smart contracts, AES-256 encryption, and decentralized storage, based on IPFS.

The hybrid architecture eliminates points of failure and enables safe interoperability between healthcare institutions. Smart contracts automate access control and consent management, providing an immutable audit trail that promotes trust and regulatory compliance. Off-chain encrypted storage is scalable and enables effective management of large medical datasets without violating privacy.

The next step in work is to optimize the work of the systems and achieve high performance by using sophisticated consensus mechanisms and trying to integrate with other emerging technologies, including artificial intelligence and Internet of Medical Things (IoMT) devices. Further studies can explore large-scale real-world implementations, cross-border medical information flow and secure analytics of encrypted medical records. The suggested framework provides a clear foundation for safe, open, and suitable digital healthcare systems.

References

[1]. N. Zhang, “Blockchain-Based Secure HER Systems,” IEEE Access, 2018.

[2]. A. Azaria, “MedRec: Using Blockchain for Medical Data Access and Permission Management,” IEEE Int. Conf. Open Big Data (OBD), Vienna, Austria, Aug. 2016.

[3]. X. Yue, “Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control,” J. Med. Syst., vol. 40, no. 10, pp. 1–8, Oct. 2016.

[4]. B. Shen, “MedChain: Efficient Healthcare Data Sharing via Blockchain,” Appl. Sci., vol. 9, no. 6, pp. 1–18, Mar. 2019.

[5]. J. Benet, “IPFS – Content Addressed, Versioned P2P File System,” 2017.

[6]. T.-T. Kuo, “Blockchain distributed ledger technologies for biomedical and health care applications,” 2017.

[7]. NIST, “Advanced Encryption Standard (AES),” FIPS 197, 2001.

[8]. M. J. Dworkin, “Recommendation for Block Cipher Modes of Operation: Methods and Techniques,” 2001.

[9]. Mohanty B, Das SM, Mishra US, Shaikh ZH, Kumar A. Effect of patients' attitude on their satisfaction and switching intention in the generic medicine industry: An empirical analysis in India. Asia Pacific Journal of Health Management. DOI: https://doi.org/10.24083/apjhm. v17i2.1821.