BLOCKCHAIN SOLUTION FOR PATIENT RECORD SECURITY

Kunal Meher[1]*, Beatrice S.[2], Sushama Khanvilkar[2], Chhaya Dhavale[2], Jaychand Upadhyay[2], Vijay Jumb[2], Kirti Motwani[2], Nilambari Narkar[2]
[1]*Atlas Skill Tech University, Mumbai, India*
[2]*Xavier Institute of Engineering, Mumbai, India*

KEYWORDS
HER
Blockchain
cybersecurity
Information protection

ABSTRACT:
The presented Electronic Health Record (EHR) system aims to leverage blockchain technology to achieve enhanced security in transmission of data, improving data integrity, providing controlled access, interoperability, maximize productivity and empowering patients by empowering them to manage their health data. Blockchain system is recognized as a promising approach to these problems, providing a safe and decentralized platform for managing patient records. Our solution, which is built on blockchain technology, addresses critical issues in healthcare data management, such as unauthorized access, data tampering, and the absence of a unified and interoperable platform. By utilizing a distributed ledger, our system guarantees that patient data stays private while being easily available to authorized stakeholders. Smart contracts are utilized to govern access permissions and streamline the process of data sharing among healthcare providers, thereby facilitating a safe and efficient sharing of medical information. The presented EHR system utilize blockchain system to establish a protected, decentralized, and unchangeable record of patients' medical histories. The system revolutionize the way health records are stored, accessed, and managed. By integrating Ethereum, Smart Contracts, and the Interplanetary File System (IPFS), the system ensures safe, transparent, and efficient handling of medical data. The integration of blockchain system into EHR systems has demonstrated considerable potential in mitigating some of the foremost obstacles within the domain. Due to its intrinsic decentralization, immutability, and openness, blockchain is the ideal tool for improving security, preserving data integrity, and building stakeholder trust in EHR systems.

1. Introduction

Electronic Health Records (EHRs) are digitized comprehensive medical histories that include patients' treatment plans, diagnoses, medications, lab reports, scans, and can be extended to contain demographic, genetic, and psychological information of a population. This information is spread across different healthcare providers, including physicians, specialists, and pharmacies (6). Compared to traditional paper-based records, EHRs provide many benefits, such as better accessibility, better care coordination, and lower administrative expenses. Before the advent of electronic documentation, medical documentations were paper-based, usually kept in folders, binders, and filing cabinets, with handwritten forms and progress notes. Technological advancements have led to digitized medical records, which are more accessible and cost-effective. Government regulations, like the Health Information Technology for Economic and Clinical Health (HITECH) Act in the United States, have spurred adoption, improving patient care through real-time access and more coordinated healthcare. Digitization also reduces expenses related to paper-based medical records, including printing, storage, and retrieval. (6).

Analyzing information from EHRs ensures more accurate diagnoses. Healthcare providers can recognize trends, monitor patient outcomes, and pinpoint areas for enhancement. However, the present state of EHRs faces challenges in aspects such as interoperability, patient access, and cybersecurity (6). Interoperability issues arise because different healthcare systems use varied EHR systems that not always communicate well with each other, leading to fragmented patient information. Furthermore, upholding patient privacy and ensuring access to their own health information continues to be a major challenge, and growing instances of data breaches and cyberattacks that target private health data have raised worries about cybersecurity.

Blockchain system can improve the security and privacy of EHRs by providing a decentralized, tamper-proof ledger for all transactions and data access. Each block in the chain forms a chronological and unchangeable record by including a cryptographic hash of the previous block. The potential applications of blockchain extend across various sectors, including healthcare. EHR systems that utilize blockchain ensure consensus, decentralization, immutability, and data transparency. The cryptographic elements of public/private key access, proof of work, and distributed data enhance to a higher level of integrity for healthcare data (2)(9). Furthermore, blockchain-based EHR systems can address interoperability challenges by offering a standardized framework for data exchange among different healthcare providers. This can guarantee that, no matter where it is kept, patient data is constantly available and current. Furthermore, by enabling fine-grained access controls that guarantee only authorized personnel may access particular health information, blockchain improves patient control over their data.

This paper describes a blockchain-based decentralized web application that uses Access Control and the Interplanetary File System (IPFS) for storing and securing patients' health records. Our approach aims to revolutionize EHR systems by providing patients who have control over their own health records and eliminating the need for third-party involvement. By leveraging blockchain technology, we present a system that enhances the security, privacy, and interoperability of EHRs, finally resulting in better healthcare outcomes.

Standards and Existing Systems

This section discusses existing EHR standards and systems that utilize blockchain technology, analyzing their approaches, methodologies, algorithms, and the limitations observed during practical applications.

Regulatory Compliance and Standards

The incorporation of blockchain system into EHR systems presents numerous opportunities. However, for widespread adoption, it is crucial to implement standards and regulations to protect patient privacy and security worldwide. This section explores the importance of ensuring safer Patient Health Information (PHI) and system interoperability.

HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. law intended to secure the privacy and security of medical records. When applied to EHR using blockchain technology, we can investigate how blockchain can support HIPAA compliance by creating a decentralized, tamper-proof log of all transactions and data access. The immutable nature of blockchain guarantees that once information is recorded, it cannot be changed or erased, thus preserving the integrity of patient records and audit trails. Furthermore, blockchain's cryptographic methods enhance the secure transmission and storage of data, further bolstering HIPAA compliance. (4) (5).

GDPR Compliance

The General Data Protection Regulation (GDPR) is an EU regulation aimed at safeguarding data protection and privacy. It establishes stringent requirements for the processing and transfer of personal data, including healthcare information. Blockchain technology can support GDPR compliance by offering transparent and auditable data management practices. With its distributed ledger, patients can gain more control over their data, allowing them to provide and withdraw access permissions. Smart contracts can streamline consent management, ensuring data is accessed and processed only with explicit patient consent. However, issues like data minimization and the "right to be forgotten" may need further investigation to ensure blockchain-based EHR systems fully comply with GDPR standards (4).

IHE Standards

Integrating the Healthcare Enterprise (IHE) started by healthcare professionals and industry to enhance the way computer systems in healthcare exchange records. Blockchain technology can help with interoperability by providing a decentralized platform for data sharing among disparate healthcare systems. This can ensure seamless integration and communication between healthcare providers, enhancing care coordination and patient outcomes (1).

FHIR Standards

Fast Healthcare Interoperability Resources (FHIR) is a standard for sharing healthcare records electronically. In the context of blockchain, FHIR can be used to structure EHR data, making it easier for health apps to integrate into health records. Blockchain's distributed ledger can enhance FHIR standards by offering a safe and transparent platform for storage and sharing structured healthcare data.

Table 1. Existing Blockchain-Based EHR Systems

System	Description	Strengths	Weaknesses
MedRec	Utilizes innovative blockchain smart contracts to establish a decentralized content management system for healthcare records across multiple providers. (3).	Provides a complete, immutable record of authentication permissions, facilitating ease of data access and auditing.	Limited scalability and high computational costs associated with maintaining blockchain transactions.

OmniPHR	Offers a distributed model to integrate Personal Health Records (PHRs) for use by patients and healthcare providers. It employsa routing overlay and the Chord algorithm for data distribution, and uses a publish-subscribe system for node communication (10).	Decentralizes data storage and maintains an equitable distribution of data blocks throughout the network.	Complexity in managing and maintaining the distributed network and ensuring consistent data availability.
MeDShare	Uses smart contracts along with an access control mechanism to efficiently monitor record activity and revoke access from unauthorized entities upon detecting permission violations. (11).	Minimizes risk to data privacy by enabling secure data exchange between cloud service providers and research or medical institutes.	Potential issues with ensuring real-time data availability and managing access control effectively across different entities.

2. Methods

The management and security of patient health records represent one of the biggest challenges in the healthcare sector. While traditional EHR systems offer a centralized platform for storing patient data, they often face concerns related to data safety, integrity, interoperability, and confidentiality. Concerns such as unauthorized access to confidential health records, data breaches, and difficulties in sharing data seamlessly among different healthcare providers are significant challenges. This project aims to design and implement an EHR system utilizing blockchain technology to tackle these issues. With its decentralized and secure architecture, blockchain can regulate access to information, ensure the security and integrity of patient information, and facilitate easy information sharing among authorized parties.

Mathematical Expression

Consider a set of patients $P = \{p_1, p_2, ..., p_n\}$, each with their Electronic Health Records $EHR = \{ehr_1, ehr_2, ..., ehr_n\}$. Also, consider a set of healthcare providers $H = \{h_1, h_2, ..., h_m\}$ with a corresponding set of permissions $Permissions = \{p_1, p_2, ..., p_m\}$. The objective is to design a blockchain-based EHR system that ensures:

Patient Control (PC): The system must guarantee that patients have control over their health data, enabling them to provide and withdraw access permissions to healthcare providers.

$PC(ehr_i) = 1$; if patient p_j grants access to provider h_k for ehr_i
$= 0$; otherwise

Data Privacy (DP): The system should ensure the confidentiality of patient data through cryptographic methods, preventing unauthorized access.

$DP(ehr_i) = 1$; if only authorized entities can access ehr_i
$= 0$; otherwise

Interoperability (I): The presneted EHR system must support seamless data exchange among healthcare providers, promoting interoperability.

$I(h_j,h_k) = 1$; if interoperable data exchange is facilitated between h_j and h_k
$= 0$; otherwise

Solving these challenges will lead to an EHR system that ensures patient-centric control, robust data privacy, and effective interoperability, thereby addressing the current shortcomings in healthcare data management.

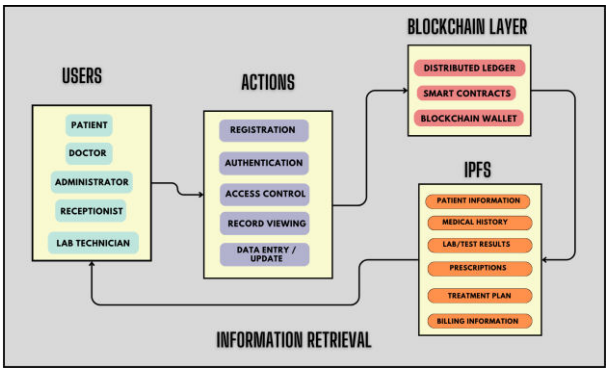

Figure 1. EHR Block diagram

The above block diagram consists of various blocks such as users, blockchain layer, database layer and the different services that can be performed such as Registration, Authentication, Access Control, Record Viewing and Data Entry and Update. Users consist of patients, healthcare providers, administrator, regulatory authority and legal representatives. While the blockchain layer consists of distributed ledger, smart contracts and blockchain wallet. The various types of data in the database includes patient information, medical history, lab/test results, prescriptions, treatment plan and billing information. All of this information retrieval can be done by the users on the basis of their specific permissions.

System Architecture:

- Patient Interface:
  - Allows patients to access their medical records securely.
  - Provides functionality for granting and revoking access to healthcare providers.
- Doctor Interface:
  - Enables healthcare providers to view and update patient records upon receiving proper authorization.
  - Facilitates the recording of diagnoses, treatments, and other medical interventions.
- Administration Interface:
  - Used by system administrators to oversee the network, manage Smart Contracts, and handle system updates.
- Security Layer:
  - Implements encryption, authentication, and authorization mechanisms to protect sensitive data.
  - Utilizes Ethereum's public-private key infrastructure for secure access.
- Data Layer:
  - Contains the IPFS for storing medical documents, images, and other large files.
  - Links to the blockchain via unique identifiers stored in Smart Contracts.

Workflow:

- Record Creation:
  - A new medical record is created on the blockchain with a unique identifier.
  - Relevant documents are uploaded to IPFS, and the hash is stored in the blockchain.

  Access Control:
  - Patients grant access to healthcare providers through Smart Contracts.
  - Access can be time-bound or transaction-specific, based on patient consent.

  Updates and Audits:
  - Healthcare providers update records after treatment, with all changes tracked and auditable.
  - Smart Contracts ensure only authorized updates are made.

  Data Retrieval:
  - Authorized parties retrieve data using the unique identifiers, ensuring data is up-to-date and has not been tampered with.

Our fundamental framework encompasses three pivotal components: Ethereum, Smart Contracts, and the Interplanetary File System (IPFS), each playing a unique and crucial role in the development of our system.

Potential Impact:

- Enhanced Security: Implementing blockchain and IPFS will greatly minimize the possibility of data breaches and unauthorized access to confidential health records.

- Patient Empowerment: Patients will gain greater authority over their medical data, which involves the capacity to provide and withdraw access to healthcare providers.
- Operational Efficiency: The system will optimize health record management, lowering administrative costs and eliminating redundant processes.
- Improved Healthcare Outcomes: With improved data management and accessibility, healthcare providers can make more informed decisions, resulting in better patient care and outcomes.

By streamlining the management of health records and reducing administrative overhead, blockchain can lead to cost savings for healthcare providers and patients alike. Blockchain's ledger can serve as a transparent and tamper-proof audit trail, aiding in regulatory compliance and facilitating audits.

Key Components:

- EthereumBlockchain:
  - Serves as the backbone of the system, providing a decentralized framework for transaction processing and Smart Contract execution.
  - Ensures data integrity and security through cryptographic techniques.

  Smart Contracts:
  - Automate the verification and execution of transactions, ensuring compliance with predefined rules and protocols.
  - Manage access control, consent management, and data sharing agreements.

  Interplanetary File System (IPFS):
  - Stores large data files off-chain to prevent bloating the blockchain.
  - Provides a peer-to-peer network for storing and accessing files, ensuring high availability and redundancy.

  QR Code:
  - Our application offers customers a streamlined experience by utilizing QR code capabilities that are fully linked with MetaMask.
  - Our system can automatically get the related address by scanning the account's QR code, saving you the trouble of copying and pasting by hand.
  - Our QR code feature makes using MetaMask incredibly efficient and allows users to concentrate on their work without unnecessary interruptions.

  Book a Demo:
  - The user can book a demonstration of the installation set up to better understand the working of the platform.

3. Results

The incorporation of blockchain technology into EHR systems offers numerous practical applications for hospitals and clinics. Below are examples showcasing the advantages and potential real-world impact of these systems:

Enhanced Data Security and Privacy

Example: Secure Patient Data Management

A hospital implements a blockchain-based EHR system to manage patient records. Each patient's data is encrypted and stored on the blockchain, ensuring that only authorized personnel can access it. The decentralized nature of the blockchain prevents unauthorized access and data breaches, significantly enhancing the security and privacy of patient information.

Advantages:

- Improved protection against cyberattacks and unauthorized access.
- Ensured data integrity and immutability, preventing tampering or loss of data.
- Enhanced patient trust in the healthcare system.

Interoperability and Data Sharing

Example: Seamless Data Exchange Among Providers

A clinic uses a blockchain-based EHR system that enables smooth data exchange with other healthcare providers, including specialists, laboratories, and pharmacies. This interoperability ensures that patient information is readily available across different platforms, facilitating coordinated and efficient patient care.

Advantages:

- Real-time access to comprehensive patient histories by all involved healthcare providers.
- Reduction in redundant tests and procedures, leading to cost savings.

- Enhanced continuity of care and better-informed treatment decisions.

Patient-Centric Healthcare

Example: Patient-Controlled Health Records

A hospital implements a blockchain-based EHR system that allows patients to manage their own health records. Patients can provide or withdraw access to their data, enabling them to take a more active role in their healthcare decisions. This system also enables patients to easily transfer their health records when switching providers.

Advantages:

- Increased patient engagement and empowerment.
- Streamlined process for patients to share their health information with new healthcare providers.
- Improved accuracy and completeness of health records, as patients can verify that their data is current.

Efficient and Transparent Audit Trails

Example: Auditable Access Logs

A clinic employs a blockchain-based EHR system that ensures a clear and immutable log of entire data access and modifications. This record of transactions allows for efficient monitoring and auditing of data usage, ensuring accountability and compliance with regulatory requirements.

Advantages:

- Improved compliance with regulations such as GDPR and HIPAA.
- Increased accountability and transparency in data management.
- Facilitation of audits and investigations, reducing the time and resources required for compliance checks.

By implementing these blockchain-based EHR systems, hospitals and clinics can significantly enhance data security, interoperability, patient engagement, and regulatory compliance, leading to improved healthcare outcomes and operational efficiencies.

4. Conclusion

To conclude, Blockchain technology can be integrated with EHR systems to increase patient privacy, expedite data management procedures, and promote interoperability amongst various healthcare providers. Giving people authority over their health data can also empower them and advance patient-centric healthcare. Despite the significant potential, it is vital to remember that EHR Blockchain systems still have a wide area of future scope.

References

1. SoerenBittins, Gerhard Kober, Andrea Margheri, Massimiliano Masi, Abdallah Miladi and VladimiroSassone. Healthcare Data Management by Using Blockchain Technology. Springer Singapore: 2021, pp. 1–27. https://doi.org/10.1007/978-981-15-9547-9_1.
2. Deloitte. Blockchain: Opportunities for Health Care. (Cited at 2024 Apr 28). Available from: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunities-for-health-care.pdf.
3. Ariel Ekblaw and Asaf Azaria. MedRec: Medical Data Management on the Blockchain. Available from: https://viral.media.mit.edu/pub/medrec.
4. N. Ettaloui, S. Arezki, and T. Gadi. An Overview of Blockchain-Based Electronic Health Records and Compliance with GDPR and HIPAA. Data and Metadata, vol. 2, p. 166, 2023. https://doi.org/10.56294/dm2023166
5. Vaishali Gaikwad (Mohite) et al. Fraud detection using machine learning and blockchain. Int. J. Recent Innov. Trends Comput. Commun. 11.6s, 2023, pp. 584–590. https://doi.org/10.17762/ijritcc.v11i6s.6970
6. National Institutes of Health. Opportunities and Challenges with Electronic Health Records. (Cited at 2024 Apr 28). Available from: https://www.nih.gov/sites/default/files/research-training/initiatives/pmi/opportunities-challenges-electronic-health-records.pdf
7. Sabita Khatri et al. A Systematic Analysis on BlockchainIntegrationWith Healthcare Domain: Scope and Challenges. IEEE Access 9, 2021, pp. 84666–84687. https://doi.org/10.1109/ACCESS.2021.3087608
8. Abdullah Al Mamun, Sami Azam, and Clementine Gritti. Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction. IEEE Access 10, 2022, pp. 5768–5789. https://doi.org/10.1109/ACCESS.2022.3141079.
9. KunalMeher et al. Peer-to-Peer Conferencing using Blockchain, WebRTC and SI. Int. J. Recent Innov. Trends Comput. Commun. 11.8s, 2023, pp. 651–656. https://doi.org/10.17762/ijritcc.v11i8s.7252

10. Alex Roehrs, Cristiano André da Costa, and Rodrigo da Rosa Righi. OmniPHR: A distributed architecture model to integrate personal health records. Journal of Biomedical Informatics 71, 2017, pp. 70–81. ISSN: 1532-0464. https://doi.org/10.1016/j.jbi.2017.05.012.
11. Qi Xia et al. MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. IEEE Access 5, 2017, pp. 14757–14767. https://api.semanticscholar.org/CorpusID:9991173.
12. Mohammad Zarour et al. Evaluating the Impact of Blockchain Models for Secure and Trustworthy Electronic Healthcare Records. IEEE Access 8, 2020, pp. 157959–157973. https://doi.org/10.1109/ACCESS.2020.3019829.