# Healthcare Record Management system Using Blockchain Technology

Khushi Lawankar, Prof .S.N.Sawalkar

*Abstract:* **This project introduces an innovative online healthcare document management system designed to streamline insurance claims processing by leveraging blockchain technology. By storing medical transactions on a blockchain, the system ensures enhanced transparency, security, and immutability, effectively mitigating risks associated with data tampering and unauthorized access.A key feature of the system is its integration with wearable health tracking devices, facilitating the collection of accurate and real-time health data. This data can be securely linked to patients' health records, enabling authorized healthcare providers to access pertinent medical information remotely. Such integration not only enhances patient care but also reduces the necessity for in-person consultations, thereby increasing efficiency in healthcare delivery.**

**The application of blockchain in this context offers significant advantages, including decentralized data storage, enhanced patient privacy through encryption and access controls, and the use of smart contracts to automate and validate insurance claims processes. These features collectively contribute to a more secure, transparent, and patient-centric healthcare ecosystem. this project exemplifies the transformative potential of combining blockchain technology with healthcare data management. By addressing critical issues of data security and interoperability, the system paves the way for more efficient and trustworthy healthcare services, with the added benefit of facilitating seamless insurance claim processes.**

**In the current medical insurance claims process, there are problems of low efficiency and complex services. When a patient applies for medical insurance claims, he/she must go to the hospital to apply for a diagnosis certificate and receipt and then send the relevant application documents to the insurance company. The patient will not receive compensation until the company completes the verification with the patient's hospital. However, we can improve the current dilemma through blockchain technology. Blockchain technology can effectively open up the information channels of the insurance industry and medical institutions, promote industry integration, and enhance the ability of insurance companies to obtain information.**

## 1. INTRODUCTION

The healthcare sector is undergoing a significant transformation, driven by the need for secure, efficient, and patient-centric data management systems. Traditional Electronic Health Record (EHR) systems often face challenges related to data breaches, unauthorized access, and interoperability issues. These challenges not only compromise patient privacy but also hinder the seamless exchange of medical information across different healthcare providers. To address these concerns, the integration of blockchain technology into healthcare data management has emerged as a promising solution. Blockchain technology offers a decentralized and immutable ledger system that enhances the security and transparency of medical transactions. By storing medical records on a blockchain, patients gain greater control over their data, ensuring that only authorized individuals can access sensitive information. This approach not only safeguards patient privacy but also facilitates the accurate and timely sharing of information among healthcare providers, leading to improved patient outcomes.

In the context of insurance claims, the application of blockchain technology can significantly streamline the process. By maintaining an encrypted and tamper-proof record of medical transactions, insurers can verify claims more efficiently, reducing the potential for fraud and administrative overhead. Smart contracts, a feature of blockchain technology, can automate the verification and approval processes, ensuring compliance with regulatory standards and expediting claim settlements. To further enhance the security of medical data, the implementation of hybrid encryption algorithms is proposed. Hybrid encryption combines the strengths of symmetric and asymmetric encryption methods, offering robust protection against unauthorized access. This dual-layered approach ensures that even if one encryption layer is compromised, the data remains secure, thereby providing a higher level of security for sensitive health information.

Moreover, the integration of wearable health tracking devices with blockchain-based systems can

revolutionize patient monitoring and care. These devices can collect real-time health data, which, when securely stored on a blockchain, can be accessed by authorized healthcare providers. This continuous flow of information enables proactive healthcare interventions, reduces the need for frequent in-person visits, and enhances the overall efficiency of healthcare delivery.the development of a blockchain-based healthcare document management system for insurance claims represents a significant advancement in healthcare technology. By ensuring the security, integrity, and interoperability of medical data, such a system not only enhances patient trust but also streamlines administrative processes, reduces costs, and improves the quality of care. As the healthcare industry continues to evolve, embracing innovative technologies like blockchain and hybrid encryption will be crucial in addressing existing challenges and meeting the growing demands for secure and efficient healthcare solutions.It is totally different in case of a diagnostic center or in case of a general practitioner. Anyway, in both cases ultimately (name, value) pairs describe the results of an encounter and different structuring procedures integrate the data into EHR records. The (name, value) pairs are implicitly always extended by several essentials attributes, where the time of the event represents a crucial role. In order to integrate these isolated data silos a series of interfaces.

## 2. LITERATURE SURVEY

1. Security and Privacy Enhancements

Author Shi et al. conducted a systematic review focusing on the application of blockchain in EHR systems, emphasizing security and privacy aspects. The study identified that blockchain's decentralized and immutable nature can effectively prevent unauthorized access and tampering of medical records. However, the authors also noted challenges such as scalability issues and the need for standardized protocols to ensure widespread adoption.

2. Interoperability and Data Sharing

A study published in *Sustainability* (2023) proposed a blockchain-based framework aimed at improving interoperability among disparate EHR systems. By aligning with international standards like HIPAA and HL7, the framework facilitates secure and seamless data exchange across healthcare providers, enhancing patient care coordination and reducing administrative burdens.

3. Access Control Mechanisms

Author Viswanathan and Lakshmi (2016) introduced a fine-grained access control system utilizing attribute-based encryption within a blockchain framework. Implemented on the Hyperledger Fabric platform, this approach ensures that only authorized individuals with specific attributes can access sensitive health data, thereby reinforcing patient privacy and data security.

4. Scalability and System Integration

Research by a team in Korea explored the use of consortium blockchain, specifically Hyperledger Fabric, to integrate existing EHRs without the need for a centralized supervisory system. The study demonstrated that such an approach could enhance scalability and availability, allowing for efficient access to patient records across multiple healthcare institutions while maintaining data integrity

5. Personal Health Records (PHRs) and Patient Empowerment

A systematic review highlighted the application of blockchain in managing Personal Health Records (PHRs), emphasizing patient empowerment through data ownership and control. The decentralized nature of blockchain enables patients to manage access to their health information, fostering trust and engagement in their healthcare journey. EMRChain and PHD-Chain. EMRChain manages Electronic Medical Records (EMRs) by combining off-chain storage and on-chain verification techniques. On the other hand, PHD-Chain is specifically designed for housing personal healthcare data generated by patients themselves. Their proposed consensus algorithm is built upon Proof of Work and features a modified transaction processing method. This approach has shown a commendable throughput of 46 transactions per second, surpassing the capabilities of both Ethereum and Bitcoin. However, it's important to note that the platform's scalability and performance during high-stress and crisis situations still require further testing and evaluation [12]. blockchain technology holds significant promise for transforming Electronic Health Record (EHR) management systems. It offers decentralized, secure, and transparent solutions for EHR sharing patient control, data integrity, and interoperability. Various blockchain models like Ethereum,

Hyperledger, Corda, and Tendermint have been proposed, providing advantages like improved privacy, data security, patient empowerment, and access control [13] [14]. However, addressing scalability, performance, and emergency access backup systems remains crucial for practical blockchain-based health record management.

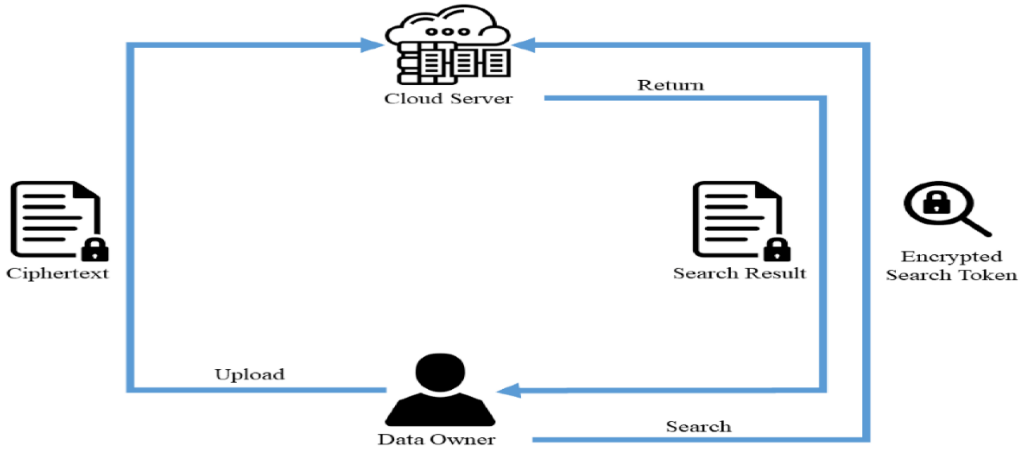
EMRChain and PHD-Chain blockchain technology holds significant promise for transforming Electronic Health Record (EHR) management systems. It offers decentralized, secure, and transparent solutions for EHR sharing patient control, data integrity, and interoperability. Various blockchain models like Ethereum, Hyperledger, Corda, and Tendermint have been proposed, providing advantages like improved privacy, data security, patient empowerment, and access control [13] [14]. However, addressing scalability, performance, and emergency access backup systems remains crucial for practical blockchain-based health record management.

EMRChain and PHD-Chain. EMRChain manages Electronic Medical Records (EMRs) by combining off-chain storage and on-chain verification techniques. On the other hand, PHD-Chain is specifically designed for housing personal healthcare data generated by patients themselves. Their proposed consensus algorithm is built upon Proof of Work and features a modified transaction processing method. This approach has shown a commendable throughput of 46 transactions per second, surpassing the capabilities of both Ethereum and Bitcoin. However, it's important to note that the platform's scalability and performance during high-stress and crisis situations still require further testing and evaluation [12].

## 3. METHEDOLOGY

Record (EHR) 4. METHODOLOGY

We proposed blockchain technology to keep healthcare records transparently and securely on blockchain servers in encrypted format. It is essential to implement robust security measures to protect the devices and the data they collect. In traditional encryption, once the data is encrypted into ciphertext, it will limit the functionality and practicality of the data usage as the user cannot efficiently search or access the data. Hence, searchable encryption (SE) has been the interest to many researchers lately. SE allows users to perform a keyword search on the encrypted data by using a search token without exposing the content and search information. In a searchable encryption scheme: Blockchain application research in the healthcare industry has been increasingly popular because blockchain storage can provide a durable medium for the EHR. This is because the data storage on the blockchain network is immutable, and any data modification can be easily detected by the new block created upon modification. Hence, data stored on the blockchain will subsequently become tamper-proof and support non-repudiation. In general, this section describes two different approaches of the blockchain implementation for data outsourcing.Storing the entire EHR on the blockchain network,Storing the EHR metadata on the blockchain network and outsourcing the EHR to third party cloud storage.




- The data owner extracts useful information from the data before encrypting the data with the secret key.
- Constructs the index lookup table and encrypts it using the secret key.
- Upload the encrypted index and data/ciphertext to the cloud storage.
- The data owner can submit an encrypted query with a search token to search on the cloud server.

- The cloud server will perform the search process without learning the keyword and the data being searched.
- Encrypted data that satisfies the search function will be retrieved and returned back to the data owner.

Global communication becomes more natural for everyone, and patients have greater freedom when there is no longer a requirement for a central server or for authorities to stand between patients and their data. Blockchain technology generally gives people more power. It becomes possible for hospitals and patients to communicate effectively and decentralize relevant data and information. The system that gathers, transfers, and saves data is also made incredibly easy to maintain and open for inspection by anybody by utilizing a blockchain.

Choosing the new AES algorithm

Fifteen competing symmetric algorithm designs were subjected to preliminary analysis by the world cryptographic community, including the National Security Agency (NSA).

- speed and reliability in the encryption and decryption processes;
- key and algorithm setup time; and
- resistance to various attacks -- both in hardware- and software-centric systems.

Triple DES Algorithm Description

Triple DES (3DES) is a symmetric key encryption algorithm that enhances the security of the original Data Encryption Standard (DES) by applying the encryption process three times. This algorithm is widely used for securing sensitive information in financial and other secure communications systems.

Triple DES Modes of Operation

The core of 3DES involves encrypting, decrypting, and then encrypting the data again. The process uses the DES algorithm in the following steps:

1. Encryption with Key 1 (K1): The plaintext is encrypted using DES and the first key.
- Decryption with Key 2 (K2): The output from the first step is decrypted using DES and the second key. Decrypting here is deliberate, to add complexity and avoid weaknesses

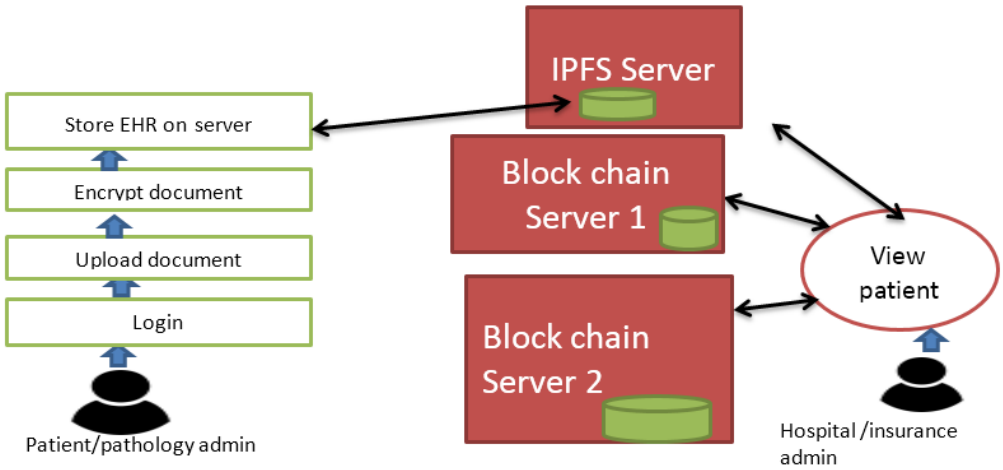
## 4. SYSTEM DESIGN

The system design of the Blockchain-Based Healthcare Record Management System integrates advanced technologies to ensure secure, efficient, and transparent handling of Electronic Health Records (EHRs). The architecture is structured into multiple layers, each serving a distinct function:

1. User Interface Layer: This layer provides a web-based portal for various stakeholders, including patients, doctors, insurance companies, medical stores, and pathology labs. Users can interact with the system to perform actions such as viewing, uploading, or requesting access to EHRs.

2. Application Layer: Serving as the intermediary between the user interface and the underlying technologies, this layer handles business logic, user authentication, and access control. It ensures that only authorized users can perform specific actions, maintaining the integrity and confidentiality.

3. Encryption and Hashing Module: Before any EHR data is stored or transmitted, it undergoes encryption using the Advanced Encryption Standard (AES) to protect sensitive information. Additionally, the Secure Hash Algorithm (SHA-256) is applied to generate a unique hash of the data, ensuring its integrity and enabling tamper detection.




Data Flow Diagram

## 5. RESULT

The developed system consists of five main modules: Admin, Pathology Lab, Medical Store, Patient, Hospital, and Insurance Company. Below is a description of the roles and responsibilities of each module:

1. Admin Module:
2. Patient Module:
3. Insurance Company Module:
4. Medical Store Module:
5. Hospital Module:

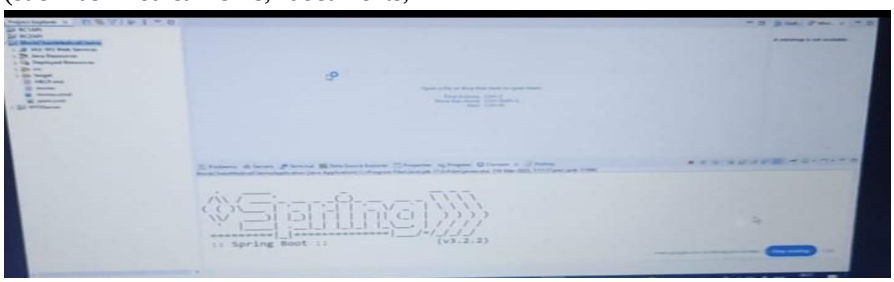
Data Storage and Security

All data in the system is securely stored using blockchain and IPFS (InterPlanetary File System).

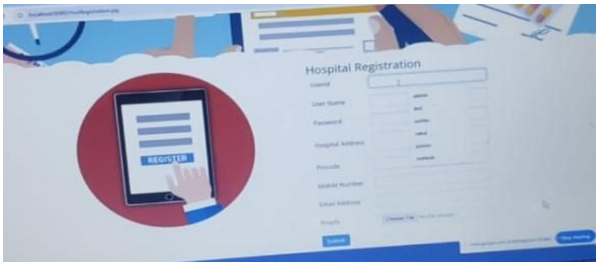
1. IPFS Storage:
   - The system uses IPFS to store large data files (such as medical bills, documents, etc.). IPFS divides these files into smaller blocks, improving efficiency and scalability.
2. Blockchain for Security:
   - Each document uploaded by users is secured on a blockchain server. This ensures that the data is immutable and tamper-proof..

Technology Stack

- Java IDE: The system is developed using Java as the primary development language to implement the backend functionality.
- SQL Workbench: SQL Workbench is used to manage and interact with the database, ensuring the structured storage of data such as patient details, claims, and other medical records.
- AIVEN Cloud Platform: The system integrates with AIVEN Cloud, a cloud platform used to store and manage the SQL data securely




Here's a clearer version of how the application runs.




The application has specific registration pages for patients, hospitals, and insurance companies. Below is an overview of how each registration process works:


After successful registration, users are directed to the login page Upon clicking 'Submit,' users will be redirected to their respective portals — Patient, Hospital, Medical, or Insurance — within the application."


After logging in, the patient is directed to the Patient Portal, where they can upload documents, grant access permissions, and submit insurance claims.

Here SQL Workbench: SQL Workbench is used to manage and interact with the database, ensuring the structured storage of data such as patient details, claims, and other medical records.

## 6. CONCLUSION

In conclusion, the proposed blockchain-based healthcare record management system represents a transformative step towards a more secure, efficient, and patient-centric healthcare environment. By addressing critical issues related to data security, interoperability, and administrative efficiency, this system lays the groundwork for future innovations in healthcare technology and sets a precedent for the adoption of blockchain solutions in the medical field.The implementation of a blockchain-based healthcare record management system marks a significant advancement in the secure handling of electronic health records (EHRs). By leveraging blockchain technology, the system ensures that medical transactions are stored in a decentralized, tamper-proof, and transparent manner. This approach addresses the increasing concerns over health data breaches by providing a robust framework that enhances data security and patient privacy.

The integration of Advanced Encryption Standard (AES) for data encryption and Secure Hash Algorithm (SHA) for hashing ensures that patient information remains confidential and unaltered. These cryptographic techniques safeguard the integrity of medical records, making unauthorized access or modifications virtually impossible. Furthermore, the use of smart contracts within the blockchain facilitates automated, transparent, and secure processing of insurance claims, reducing administrative burdens and minimizing the potential for fraud. In addition to serving patients and healthcare providers, the system extends its functionality to include modules for insurance companies, medical stores, and pathology labs. This comprehensive approach ensures that all stakeholders in the healthcare ecosystem can securely access and manage relevant information, fostering a more integrated and efficient healthcare delivery system.

## 7. FUTURE SCOPE

In this project we proposed blockchain based secure EHR sharing and insurance processing system.. One of the main challenges facing blockchain in healthcare is scalability. Current blockchain systems like Bitcoin and Ethereum struggle with transaction throughput, which can become problematic when handling the massive amounts of healthcare data generated daily. There is further scope of improvising this idea by implementing Artificial Intelligence (AI), Internet of things (IoT) and much more available technology to develop a more comprehensive health care model in future

Integration with Artificial Intelligence (AI) and Machine Learning (ML)

The integration of blockchain with AI and ML can significantly enhance healthcare applications:

- Predictive Analytics and Decision Support: AI models that analyze healthcare data stored on a blockchain could provide real-time insights into patient health, predicting medical conditions or suggesting treatments based on historical data.
- Personalized Healthcare: Blockchain can ensure that patient data is securely shared across healthcare providers, while AI can analyze this data to create personalized treatment plans, identify rare diseases, and recommend the most effective therapies based on individual medical histories.

- Automated Diagnosis: Blockchain-based systems could store diagnostic results securely, while AI models process and cross-reference this data for more accurate and timely diagnoses.

Enhanced Patient-Centric Care: Blockchain enables patients to have greater control over their health data, allowing them to grant or revoke access to their records as needed. This empowerment fosters a more patient-centric approach to healthcare delivery.

Improved Data Security and Privacy: The decentralized and immutable nature of blockchain ensures that health records are secure from unauthorized access and tampering. This is particularly crucial as healthcare data breaches continue to rise.

- Interoperability Across Systems: Blockchain can facilitate seamless data exchange between different healthcare providers and systems, overcoming current interoperability challenges. This ensures that patient data is consistently available, regardless of where care is provided.

Research and Data Analytics

- Blockchain can allow anonymized data sharing for research without compromising individual privacy.

## ACKNOWLEDGEMENT

First and foremost,I would like to express my sincere gratitude to my Prof.S.N.Sawalkar who has in the literal sense, guide and supervised me.I am indebted with a deep sense of gratitude for the constant inspiration and valuable guidance throughout th work.

## REFERENCES

[1] Herper, M. The C Exposes Our Health Care System's Weaknesses. We Can Be Stronger. STAT. 2020 March 2.

[2] Hölbl M, Kompara M, Kamišalić A, Zlatolas LN., A Systematic Review of the Use of Blockchain in Healthcare. Symmetry. 2018 Oct; 10(10):470.

[3] Lee AR, Kim MG, Kim IK. SHAREChain: Healthcare Data Sharing Framework using Blockchain-registry and FHIR. In: 2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM); 2019 Nov 18–21; San Diego, CA, USA. IEEE; 2020.

[4] Guo R, Shi H, Zheng D, Jing C, Zhuang C, Wang Z. Flexible and Efficient Blockchain-Based ABE Scheme With Multi-Authority for Medical on Demand in Telemedicine System. IEEE Access. 2019 Jun; 7:88012–25.

[5] Andola N, Prakash S, Venkatesan S, Verma S. SHEMB:A Secure Approach for Healthcare Management System Using Blockchain. In: 2019 IEEE Conference on Information and Communication Technology; 2019 Dec 6–8; Allahabad, India. IEEE; 2020.

[6] Saha, A.; Amin, R.; Kunal, S.; Vollala, S.; Dwivedi, S.K. Review on "Blockchain technology based medical healthcare system with privacy issues". Secur. Priv. 2019, 2, e83. [CrossRef]

[7] Abu-elezz, I.; Hassan, A.; Nazeemudeen, A.; Househ, M.; Abd-alrazaq, A. The benefits and threats of blockchain technology in healthcare: A scoping review. Int. J. Med. Inform. 2020, 124, 102396.

[8] Hasselgren, A.; Kralevska, K.; Gligoroski, D.; Pedersen, S.A.; Faxvaag, A. Blockchain in healthcare and health sciences—A scoping review. Int. J. Med. Inform. 2020, 134, 102222.

[9] Dubovitskaya, A.; Novotny, P.; Xu, Z.; Wang, F. Applications of Blockchain Technology for Data-Sharing in Oncology: Results from a Systematic Literature Review. Oncology 2020 , 98, 223–231.

[10] Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. Healthcare 2019, 7, 56.