TCET

DEPARTMENT OF ARTIFICIAL INTELLIGENCE & DATA SCIENCE

Choice Based Credit Grading Scheme with Holistic and Multidisciplinary Education
Under Autonomy - CBCGS-HME 2023
University of Mumbai

UNIFIED HEALTHCARE DATA MANAGEMENT: A BLOCKCHAIN BASED PATIENT-CENTRIC SYSTEM

BACHELOR OF TECHNOLOGY (Third Year)

Artificial Intelligence and Data Science

By

Yash Kamath

Mridula Kandalgaonkar

Under the guidance of

Mrs. Himani Tiwari
Assistant Professor,
AI&DS Department

Artificial Intelligence & Data Science
Thakur College of Engineering & Technology
Thakur Village, Kandivali (East), Mumbai-400101

(Academic Year 2024-25)

ABSTRACT

In today’s digital era, the healthcare sector increasingly relies on Electronic Health Records (EHRs) to streamline patient care and information exchange. However, centralized EHR systems face critical challenges such as data breaches, lack of interoperability, and limited patient control over personal health data. These vulnerabilities often lead to unauthorized access, fragmented information, and compromised patient safety. This study proposes a decentralized, blockchain-based framework that empowers patients by giving them full control over their medical records while enhancing data security and transparency.

The proposed model leverages a hybrid storage mechanism—storing large medical files off-chain using InterPlanetary File System (IPFS) and maintaining essential metadata on-chain. This approach ensures scalability, data integrity, and tamper-proof logging of every interaction. Smart contracts are employed to enforce access permissions, enabling patients to control who can view or share their records and for how long. Additionally, Decentralized Identity (DID) systems are used to authenticate users, further enhancing security and eliminating dependency on centralized identity providers.

Built using Hyperledger Fabric, the framework allows only authorized participants to access the system, ensuring compliance with data privacy regulations such as HIPAA. By offering a unified, patient-centric platform, this system addresses existing flaws in healthcare data management, fosters trust among stakeholders, and paves the way for a more secure, interoperable, and efficient healthcare ecosystem.

Keywords—*Blockchain in Healthcare, Patient-Centric Systems, Electronic Health Records (EHR), Decentralized Identity (DID), Smart Contracts, Hyperledger Fabric, Interoperability, Data Privacy, IPFS, Secure Data Management*

1. Introduction

In recent years, the healthcare sector has become increasingly vulnerable to data breaches, with 2015 alone witnessing over 112 million health records illegally disclosed. Major incidents, such as the breaches at Anthem, Premera, and Excellus Blue Cross, have exposed millions of sensitive patient records. This alarming trend is largely driven by rapid digitalization and the widespread adoption of Electronic Health Records (EHR), which, while improving efficiency, have also made healthcare data a prime target for cyberattacks.

Data breaches in healthcare can be classified into two categories: internal and external. Internal breaches involve misuse of access privileges, accidental data exposure, or negligence, whereas external breaches result from hacking, phishing, ransomware, and other malicious attacks. The impact of these breaches can be severe, leading not only to financial loss but also to compromised patient safety, incorrect treatments, and loss of trust.

While EHR systems have revolutionized healthcare by facilitating better data sharing and care coordination through Health Information Exchanges (HIE), their centralized nature makes them susceptible to unauthorized access and data loss. To address these challenges, blockchain technology offers a decentralized and secure alternative. This report explores how blockchain can provide a patient-centric system that ensures data integrity, privacy, and accessibility, transforming the future of healthcare data management.

2. Motivation

The increasing digitalization of the healthcare industry has transformed the way patient information is stored and accessed. Electronic Health Records (EHRs) have become the standard for maintaining medical data, aiming to streamline patient care and improve coordination between healthcare providers. However, this shift towards centralized data systems has brought about significant concerns regarding data privacy, security, and accessibility. High-profile data breaches and unauthorized access to sensitive patient records highlight the fragility of existing systems and the urgent need for more robust security measures.

Blockchain technology presents a transformative solution to these challenges. Its decentralized nature ensures that no single entity has complete control over patient data, reducing the risk of breaches. Blockchain also provides immutability, meaning once data is entered, it cannot be altered or tampered with—ensuring integrity and trust. Through features like decentralized identity (DID) and smart contracts, patients can gain full control over who accesses their data, how it is used, and for how long. This not only enhances security but also empowers patients in the data-sharing process, fostering greater transparency and accountability in healthcare systems.

3. Objectives

The primary goal of this research is to design and develop a blockchain-based framework for unified healthcare data management that is both secure and patient-centric. This involves creating a platform where patients can store, manage, and share their health records securely across different healthcare systems. By implementing a hybrid storage system—where large files like X-rays are stored off- chain and only metadata is kept on-chain—the model ensures scalability without compromising on performance or security.

Another key objective is to leverage decentralized identity (DID) and smart contracts to automate access control and data-sharing permissions. Patients will have the ability to define who can access specific parts of their health data, for what purpose, and for what duration. Additionally, the framework aims to facilitate interoperability among various healthcare platforms, allowing for seamless collaboration between hospitals, clinics, and laboratories. The system is designed to adhere to privacy regulations such as HIPAA, thereby promoting trust among all stakeholders while enhancing data privacy and operational efficiency.

4. Problem Statement

The current healthcare system faces challenges like fragmented data and lack of interoperability, making it difficult for providers to access complete patient histories. This leads to delays, repeated tests, and potential misdiagnoses. Patients also have limited control over their data, and centralized EHR systems are prone to breaches. This research proposes a blockchain-based, patient-centric platform that unifies medical records and enhances data security. By leveraging decentralization, smart contracts, and decentralized identity (DID), the system empowers patients to manage access to their data while ensuring transparency, accountability, and tamper-proof records for better and more informed healthcare delivery.

5. Literature Survey

Sreenivasan and Chacko (2021) in their research [1] explored the critical challenges in Electronic Health Record (EHR) systems, particularly focusing on interoperability issues that arise from diverse standards and fragmented infrastructures. They highlighted the necessity of consolidating health data from multiple sources, such as hospitals, pharmacies, and mobile health devices, into a unified patient-centric system like Personal Health Records (PHRs), which offers greater accessibility and enables seamless data exchange across healthcare platforms. However, they note the ongoing challenges, such as naming conflicts and access control discrepancies, that hinder effective interoperability. This work lays a foundational understanding of EHR challenges, but it does not fully address the potential of emerging technologies like blockchain to enhance data privacy and scalability, suggesting a path for further research in improving the security and flexibility of healthcare data management.

Blockchain technology was reviewed to improve clinical data security and management by AbelSalam [2]. Their research widened the perspective of blockchain, involving better openness and data immutability, more access control over the data thus improving data security. The research discusses a decentralized system of blockchain to avoid any unauthorized changes while keeping in mind the need to enable seamless data sharing among patients and healthcare providers. However, the paper also highlights some drawbacks such as the difficulty of integrating blockchain into current systems due to obligations of standard structures and scalability problems because of the computational complexity of consensus.

MedRec [3], a blockchain computing-based system, was developed to solve problems related to scattered medical records and interoperability. Their approach gave patients the privilege of having more control and transparency over their medical records. However, using Ethereum presents challenges like transaction costs and scalability. A permissioned blockchain like Hyperledger could address these issues by offering faster processing, reduced costs, and enhanced privacy. Despite these limitations, MedRec showcases a promising approach to transforming EHR management.

6. Proposed System

Our proposed system envisions a future where patients are truly in control of their own medical data. Today, patient records are scattered across hospitals, clinics, and labs—often stored in incompatible formats and managed by third parties. This makes it difficult for patients to access their complete medical history or share it securely with healthcare providers when needed. Our system aims to solve this by creating a unified, secure platform where all medical records can be stored in one place, managed directly by the patient. Whether it's a blood report, an X-ray, or a prescription, patients can upload their documents, control who can view them, and track every instance of data access—all from a single interface.

The system goes beyond just storage. It introduces a consent-based sharing model where patients decide what information is shared, with whom, and for how long. Healthcare providers such as doctors and labs can request access, but they can only view data if the patient allows it. This puts patients at the center of the healthcare process, making them active participants rather than passive recipients. The system also ensures transparency by logging every access event so patients can see who accessed their data and why. In doing so, it empowers individuals, strengthens doctor-patient trust, and contributes to a more connected and ethical healthcare ecosystem.

7. Architecture

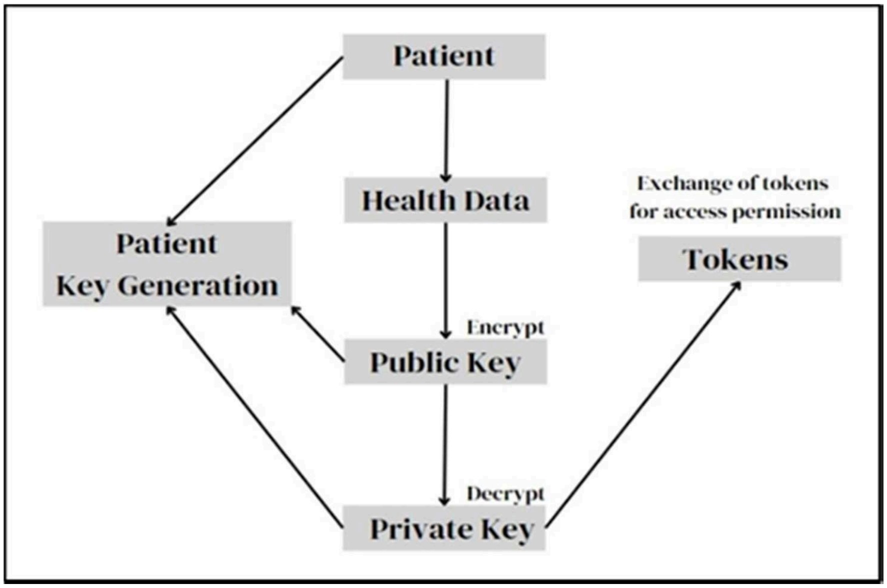


Fig.1. Framework for Secure Patient's Data Management System

1. **Blockchain Framework Selection** – For our proposed system, we decided to choose Hyperledger Fabric, a permissioned blockchain which acts as the backbone for secure, immutable, and transparent data tracking. Unlike public (permissionless) blockchains like Ethereum, Hyperledger Fabric is designed specifically for applications where keeping data private is very important. In the context of healthcare, this will ensure that only authorized entities will enter the blockchain. It uses a special method called Practical Byzantine Fault Tolerance (PBFT) to handle transactions quickly and efficiently, making it suitable for handling many users and frequent data updates.

2. **Storage Mechanism** - Healthcare sector is known for its wide range of formats for data records that comes along with the disadvantage of scalability. Even Blockchain struggles to handle such large and diverse formats of data in real-time. To resolve this, our system implements a hybrid storage mechanism which combines two approaches:

   2.1. **On chain Storage**: Stores small but critical metadata, including access logs, data- sharing permissions, and cryptographic hashes of medical files. This ensures that data stored on the blockchain cannot be changed or deleted and can be easily traced creating a reliable audit trail.

   2.2. **Off chain Storage**: Stores large medical files such as X-rays, CT scans, and blood reports in an encrypted format on decentralized storage systems like IPFS (Inter Planetary File System). The blockchain maintains a cryptographic hash (a unique digital fingerprint) of each off-chain file to ensure data integrity and verify that the file has not been tampered with. This hybrid approach lets us leverage the security and transparency of blockchain along with efficient storage of large and diverse file formats.

3. **Decentralized Identity (DID)** -To empower patients with full control over their health data, each user—patients, healthcare providers, and lab technicians—is assigned a unique DID during registration. DID-based authentication eliminates dependence on centralized identity systems, significantly reducing the risk of data breaches. Users can verify their identities directly, ensuring secure access to their information. Patients will retain cryptographic keys,
   which gives them the ability to control access to their data. This prevents unauthorized entities from viewing or altering their medical records, safeguarding privacy. The use of DIDs will enable seamless interaction between different healthcare platforms, creating a unified ecosystem where patient data can be securely shared across multiple systems without compromising security.

4. **Smart Contract**- Smart contracts play the role of automating the enforcement of business logic, ensuring that all interactions with patient data follow predefined rules. Smart contracts embed data-sharing protocols and access permissions directly into the system, guaranteeing that only authorized users can view and use sensitive medical information based on the conditions set by the patient. They help enforce rules around data access and updates, ensuring the system adheres to privacy regulations like HIPAA. They ensure that data sharing and changes are conducted only with the patient’s consent and are in full compliance with legal standards. These contracts eliminate the need for third parties, making the system more efficient and reducing the risk of human error while ensuring secure and reliable data management.

8. Methodology

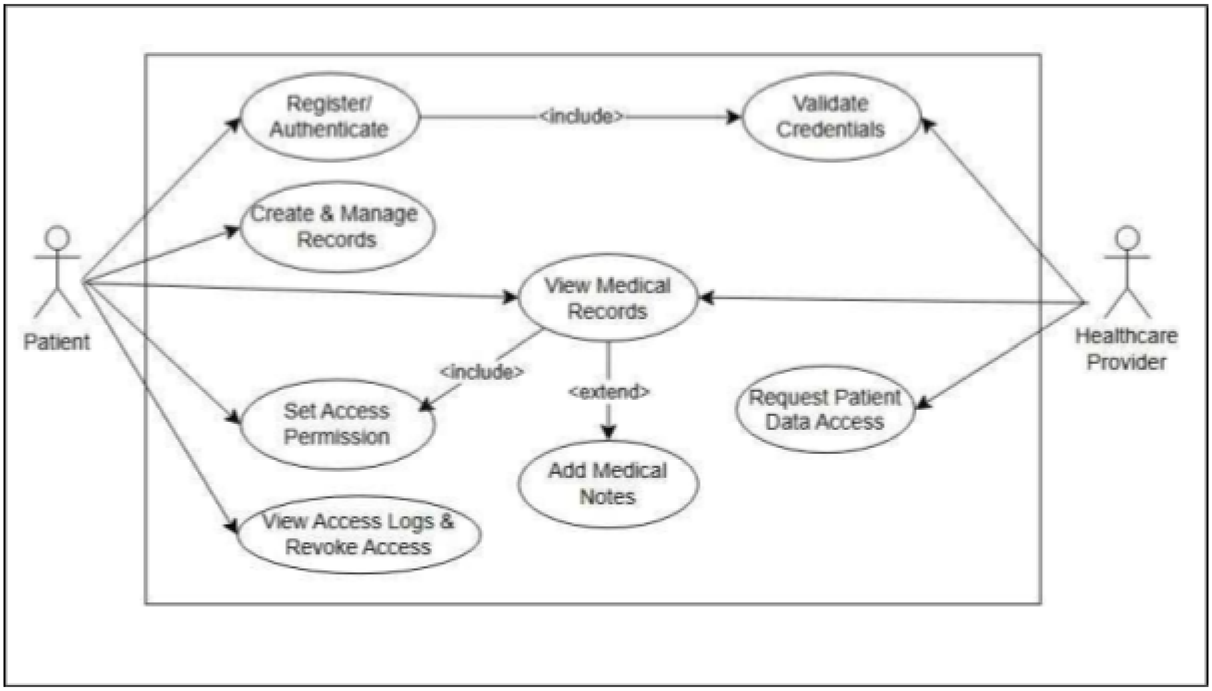


Fig 2. Use Case Diagram

1. **User Registration and Functionality** - As we are using a permissioned blockchain for our system, every user, may it be a patient, doctor or lab technician must be authorized before being able to enter and access our blockchain. The user registration and authentication process are crucial for ensuring that only valid users have access to the system. The registration involves both the patients and healthcare providers being verified by the Health Administration. Upon successful registration, a unique identity (via Decentralized Identity - DID) is assigned to each user.

2. **Patient Registration:** A patient registers by providing basic information like name, date of birth, and government id. This data is verified and validated by the Health Administrator by cross checking with the government databases. After registration, the patient receives a unique DID, which is linked to their personal healthcare data.

3. **Healthcare Provider Registration:** Healthcare providers (doctors, labs, clinics) are registered similarly, but their credentials are verified based on their professional qualifications. Only verified healthcare providers can interact with patient data. Upon successful registration, users (patients or healthcare providers) are given a private key for accessing the system securely. The registration and authentication ensure that only authorized users can interact with the system.

4. **Data Storage and Management in Hybrid System -**The storage of patient data in the system is designed to ensure ease of use, privacy and security. We will see how each of the users (patient, doctors / lab technicians) will interact with the data. Patients can upload and manage their health records, such as medical prescriptions, diagnostic reports, X-rays, and immunization histories, through the system's user-friendly interface. When a patient uploads a file to the system, the file is first encrypted locally and then are stored off chain in the Inter Planetary File System (IPFS). This approach prevents the blockchain from being overloaded with large data files. A hash of the file (a unique cryptographic representation of the file) is generated by IPFS and stored on-chain. This guarantees data integrity and ensures any unauthorized changes to the file are detectable.

Metadata related to the file—such as the upload timestamp, file type and hash of the file (a unique cryptographic representation of the file) generated by IPFS is recorded on the blockchain for an immutable and tamper-proof record.

As for the case of healthcare providers, the system implements an advanced access control mechanism using smart contracts and permissioned blockchain to ensure that patients maintain full ownership of their health data. Patients can decide who can access their data (e.g., doctors, labs, family members) and how much of their data can be shared. This is done through a user-friendly interface that allows patients to specify access rights. These access rights can be granular, enabling the patient to allow only certain parts of their health records to be shared (e.g., test results, medical history). Patients can also set a time frame for how long the data is accessible. After this period, the access is revoked automatically by the system, ensuring that no one can access the data beyond the predefined period. At any time, patients can revoke access to their data. This can be done with a simple click through the interface, ensuring that they maintain full control over who sees their information.

5. **Access Tracking-**Each time someone accesses a patient's data; the system logs the event immutably on the blockchain. These records include details such as the identity of the person accessing the data, the timestamp, and the type of data accessed. An audit trail is generated for every data-sharing event, allowing patients to review who accessed their information, when, and for what purpose. This transparency fosters trust in the system, enabling patients to monitor all interactions with their data while ensuring accountability from healthcare providers.

6. **Smart Contract Driven Permission-**Smart contracts are the backbone of our data-sharing mechanism. They automate the process of granting and revoking access permissions to ensure that no manual intervention is required for these processes. When a healthcare provider seeks access to a patient’s records, a smart contract is activated. The patient receives a notification and has the ability to either approve or reject the request. Upon approval, the smart contract ensures that the healthcare provider’s access is granted as per the patient's preferences. If a patient decides to revoke access, a smart contract is triggered again to terminate access. The smart contract will automatically update the blockchain and ensure that no unauthorized user can access the data after the revocation. By automating the access control process, smart contracts eliminate the need for intermediaries and ensure that the patient’s preferences are always adhered to, providing an efficient and secure way of managing data access

Type	**Name**	**Description**
Blockchain Framework	Hyperledger Fabric	A permissioned blockchain where only authorized users can interact with the system.
Storage Solution	IPFS (InterPlanetary File System)	A decentralized storage system for off- chain storage of large files like X-rays and medical reports.
Encryption Library	AES (Advanced Encryption Standard)	Used to encrypt patient files (e.g. reports, X-rays) before storing them in IPFS.
Authentication	Decentralized Identity (DID)	Provides secure identity management and ensures data ownership by the patient.
Smart Contract Platform	Chaincode (Hyperledger)	Smart contracts form the backbone of our data-sharing mechanism by automating the process of granting and revoking access
Cryptography Library	OpenSSL/ Hyperledger Crypto Library	Ensures data encryption, secure key generation, and certificate management.
Frontend	HTML, CSS, React.JS	For building user interfaces with interactive features for patients and healthcare providers.
Programming Languages	Solidity	To code the entire Smart Contract
	JavaScript	To code the backed logic of the blockchain web application.

9. Results and Discussion

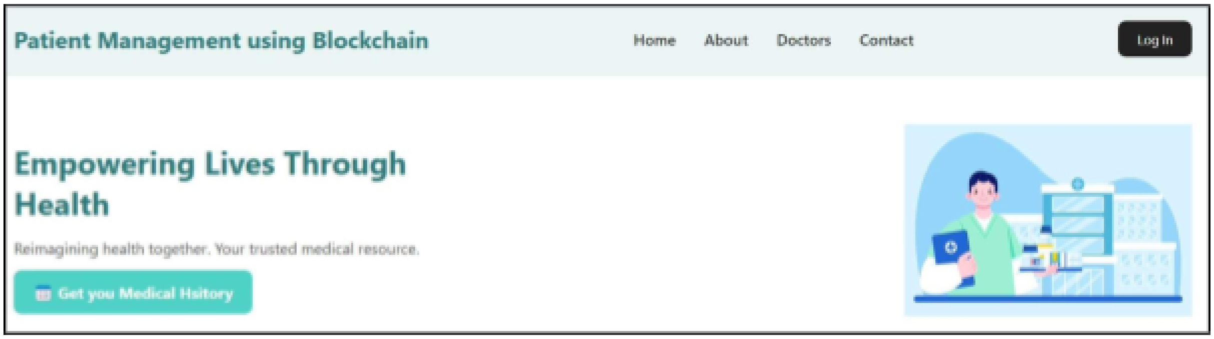
The implementation of our proposed blockchain-based healthcare data management system successfully demonstrates enhanced security, transparency, and patient-centric control. Patients were able to securely upload and manage their health records using a simple interface. The use of decentralized identity (DID) and smart contracts ensured that only authorized parties could access sensitive data, strictly under patient consent.

Performance testing showed that the hybrid storage model (on-chain metadata and off-chain encrypted files) provided a scalable solution without compromising efficiency. Smart contracts automated access control and maintained a tamper-proof log of all interactions, improving trust and reducing manual administrative efforts.

Feedback from simulated test users highlighted improved data accessibility, control, and confidence in the system’s security. Overall, the system proved to be a viable model for transforming traditional healthcare data management into a more secure, transparent, and patient-empowered process.

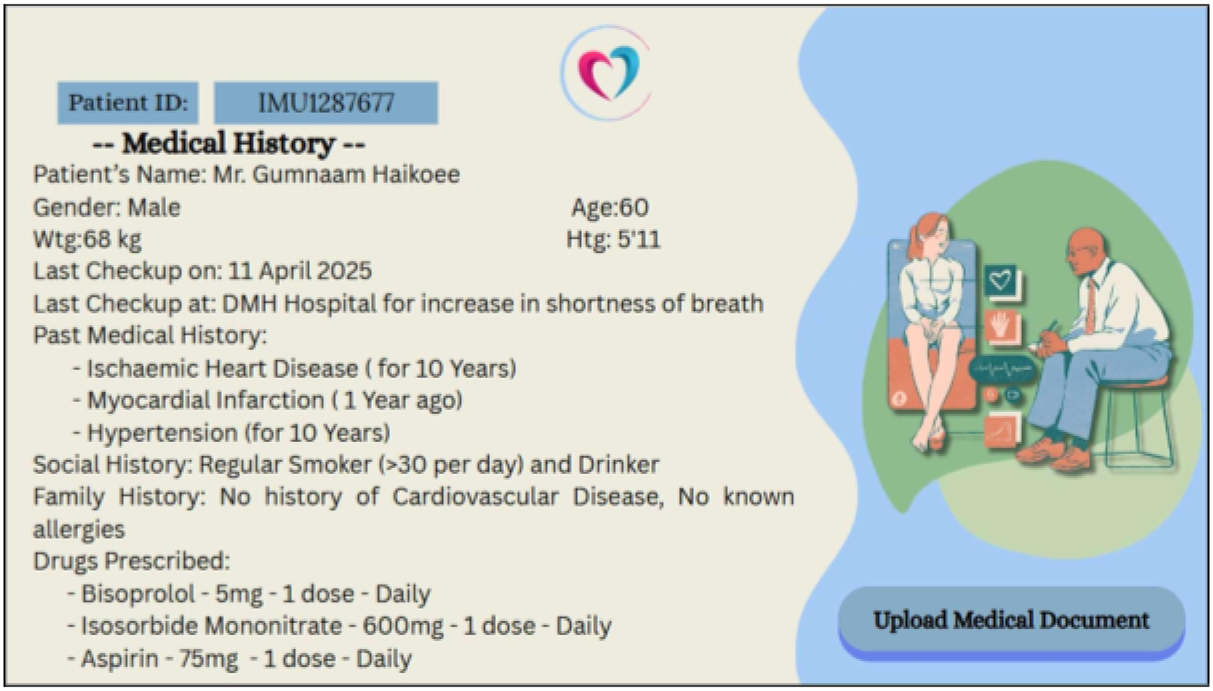
Moreover, the system's architecture demonstrated strong interoperability by allowing different healthcare providers to access standardized data formats via blockchain, reducing fragmentation. The integration of Hyperledger Fabric and IPFS proved effective in balancing security and performance. Latency during data retrieval remained minimal, even when accessing large off-chain medical files. This confirms that the system is not only secure but also practical for real-world healthcare environments where quick access to patient data can be critical for diagnosis and treatment.

Prototype



Empowering Lives Through Health

Reimagining health together. Your trusted medical resource.



Patient ID: IMU1287677

-- Medical History --

Patient's Name: Mr. Gumnaam Haikoee

Gender: Male Age:60

Wtg:68 kg Htg: 5'11

Last Checkup on: 11 April 2025

Last Checkup at: DMH Hospital for increase in shortness of breath

Past Medical History:

- Ischaemic Heart Disease (for 10 Years)
- Myocardial Infarction (1 Year ago)
- Hypertension (for 10 Years)

Social History: Regular Smoker (>30 per day) and Drinker

Family History: No history of Cardiovascular Disease, No known allergies

Drugs Prescribed:

- Bisoprolol - 5mg - 1 dose - Daily
- Isosorbide Mononitrate - 600mg - 1 dose - Daily
- Aspirin - 75mg - 1 dose - Daily

10. Conclusion & Future Scope

This research accounts for the paradigm shift blockchain technology can bring into secure patient data management in the healthcare sector. The key features of blockchain-impermanence, decentralization, and cryptographic security-offer a valid solution to most of the modern-day data management challenges confronting healthcare systems. By bringing integrity and privacy to sensitive patient information, blockchain provides a substantial alternative to centralized systems, which are at risk of unauthorized changes and breaches.

Utilization of blockchain technology in healthcare can address some of the most crucial issues with preserving patient privacy, increasing data confidentiality, and complying with privacy laws like HIPAA. Furthermore, blockchain enables the sharing of information among healthcare providers while controlling who has access to particular sections of data-an ever-important factor contributing towards worldwide interoperability among common services, thereby creating a more symbiotic X. atmosphere between such entities as hospitals, clinicians, patients, and insurance firms.

Also, as discussed, the development of blockchain can further benefit precision medicine by enabling a more accurate and timely analysis of patient data. Blockchain, through the transparent and immutable record of patient histories, makes a reliable base for enhanced decision-making and personalized care. However, blockchain technology has its fair number of hurdles to scalability, cost, and regulatory compliance. More research is needed to enhance blockchain adoption in the healthcare sector. Despite these challenges, this study demonstrates the great promise that blockchain holds in effecting an informed shift in the data management of health, enhanced patient outcomes, a strengthened security posture, and overall healthier health system operations. With continuing inquiry and application in blockchain, we behold tomorrow's landscape of secure, transparent, interoperable healthcare data management being born.

Although our proposed system describes how we can implement a blockchain-based Patient Data Management System (PDMS) from ground up, connecting it with pre existing healthcare software rises a challenge. Future efforts can focus on designing standardized APIs or middleware bridges that will enable seamless compatibility between diverse existing healthcare platforms. By addressing these challenges, we can facilitate wider adoption of the proposed system.

11. References

[1] M. Sreenivasan and A. M. Chacko, "Interoperability issues in EHR systems: Research directions," in *Data Analytics in Biomedical Engineering and Healthcare*, K. C. Lee, S. S. Roy, P. Samui, and V. Kumar, Eds. Academic Press, 2021, pp. 13–28. [Online]. Available: https://doi.org/10.1016/B978-0-12-819314-3.00002-1

[2] F. M. AbdelSalam, "Blockchain revolutionizing healthcare industry: A systematic review of blockchain technology benefits and threats," *Perspectives in Health Information Management*, vol. 20, no. 3, p. 1b, Sep. 2023. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC10701638/

[3] A. L. Ekblaw, A. S. Azaria, J. Halamka, and M. L. D. Lippman, "A case study for blockchain in healthcare," *Office of the National Coordinator for Health Information Technology (ONC)*, 2016. [Online]. Available: https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf