A Synopsis of Project on

MediTrust – Blockchain based Healthcare Records Management System

Submitted in partial fulfillment of the requirements for the award
of the degree of

Bachelor of Engineering

in

Computer Science Engineering (Data Science)

by

Vanshika Salve(21107010)
Kashish Yadav(21107026)
Khushi Chhoker(21107055)

Under the Guidance of

Mr.Vaibhav Yavalkar
Ms.Aishwarya Londhe

Department of Computer Science Engineering (Data Science)

A.P. Shah Institute of Technology
G.B.Road,Kasarvadavli, Thane(W)-400615
UNIVERSITY OF MUMBAI

Academic Year 2024-2025

Approval Sheet

This Project Synopsis Report entitled ***"MediTrust – Blockchain based Health care Records Management System "*** Submitted by ***"Vanshika Salve"(21107010), "Kashish Yadav"(21107026),"Khushi Chhoker"(21107055),***is approved for the partial fulfillment of the requirenment for the award of the degree of ***Bachelor of Engineering*** in ***CSE Data Science*** from ***University of Mumbai***.

Ms. Aishwarya Londhe
Co-Guide

Mr.Vaibhav Yavalkar
Guide

Ms. Anagha Aher
HOD, CSE Data Science

Place:A.P.Shah Institute of Technology, Thane
Date: 22/10/2024

CERTIFICATE

This is to certify that the project entitled ***" MediTrust – Blockchain based Healthcare Records Management System "*** submitted by ***"Vanshika Salve" (21107010), "Kashish Yadav" (21107026),"Khushi Chhoker" (21107055),*** for the partial fulfillment of the requirement for award of a degree ***Bachelor of Engineering*** in ***CSE Data Science***,to the University of Mumbai,is a bonafide work carried out during academic year 2024-2025.

Ms.Aishwarya Londhe
Co-Guide

Mr.Vaibhav Yavalkar
Guide

Ms. Anagha Aher
HOD, CSE Data Science

Dr. Uttam D.Kolekar
Principal

External Examiner(s)

1.

2.

Internal Examiner(s)

1.

2.

Place:A.P.Shah Institute of Technology, Thane
Date: 22/10/2024

Acknowledgement

We have great pleasure in presenting the synopsis report on **entitled MediTrust – Blockchain based Healthcare Records Management System** We take this opportunity to express our sincere thanks towards our guide **Mr. Vaibhav Yavalkar** & Co-Guide **Ms.Aishwarya Londhe** for providing the technical guidelines and suggestions regarding line of work. We would like to express our gratitude towards his constant encouragement, support and guidance through the development of project.

We thank **Ms.Anagha Aher** Head of Department for his encouragement during the progress meeting and for providing guidelines to write this report.

We express our gratitude towards BE project co-ordinator **Ms.Poonam Pangarkar Ms.Ashwini Rahude**, for being encouraging throughout the course and for their guidance.

We also thank the entire staff of APSIT for their invaluable help rendered during the course of this work. We wish to express our deep gratitude towards all our colleagues of APSIT for their encouragement.

Vanshika Salve
(21107010)

Kashish Yadav
(21107026)

Khushi Chhoker
(21107055)

Declaration

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, We have adequately cited and referenced the original sources. We also declare that We have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Vanshika Salve(21107010)

Kashish Yadav(21107026)

Khushi Chhoker(21107055)

Date: 22/10/2024

Abstract

Healthcare data is crucial and sensitive because it contains information about patients' medical history, treatments along with actions.This information is frequently shared among different stakeholders of the system. As patients' information is vital, therefore, it must be kept accurate, up to date, secret, and available only to those who are authorized to access the specified information. Still, centralized systems are commonly used to maintain healthcare records which increases the security risk. Therefore, this study focuses on protecting the privacy and security of sensitive healthcare documents while sharing them across multiple healthcare participants. In this work, we proposed a privacy-preserving access control framework based on blockchain technology that uses consensus-driven decentralized data management on top of peer-to-peer distributed computing platforms to ensure the privacy, security, accessibility, and integrity of healthcare data. In this project, we propose a blockchain-based healthcare record management system that ensures secure, decentralized storage of patient data while improving accessibility for healthcare providers. By utilizing smart contracts, the system enables automatic verification and seamless sharing of records, maintaining data integrity and confidentiality. The decentralized structure prevents unauthorized access and tampering, enhancing trust in healthcare data management. This solution provides patients with greater control over their medical records and simplifies workflows for healthcare professionals, ensuring efficiency and security in handling sensitive information. Blockchain technology helps to protect transactions from manipulation due to its irreversibility and immutability features. Furthermore, we comprehensively investigate the blockchain-enabled security requirements by including patients, doctors, chemists, and pathology labs as entities of the system that can share information through a proper channel. We have evaluated the proposed framework using Hyperledger Fabric and identified that the developed framework reveals promising benefits in security, regulation compliance, reliability, flexibility, and accuracy.

Keywords: *Blockchain technology, Privacy-preserving, Decentralized storage, Smart contracts, Hyperledger Fabric.*

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Over the decade, the healthcare sector such as medical institutions, insurance organizations, etc., are handling patients' records very carefully. These records are considered an extremely critical asset in terms of privacy and security. This asset includes information, like names, addresses, unique identities (UID), medical history, medical history of family members, medication procedures, prescribed medications, and other related data, known as Electronic Health Records (EHRs). As EHRs contain very sensitive and personal data related to a person and it should be kept secret during the system design from unauthorized access. However, cyber-attackers have performed a number of attacks on medical institutions to steal the health records of millions of patients in the past decades [1]. The Indian government introduces two regulation acts in the Health Insurance Portability and Accountability Act (HIPAA) 1996 [2] and General Data Protection Regulation (GDPR) Act 2018 [3] that covers the numerous guidelines on how to store, process, and secure the medical data in order to prevent scam and theft in the healthcare domain. The target hackers obtain personal data using unlawful ways very easily even after specifying the clear regulations for the healthcare sector by the government. Certainly, the main reason behind this insecurity is the lack of technological understanding within the sector. This leads to many challenges including data security that may result in some common attacks including ransomware and phishing for retrieving personal data. It may also reveal some other characteristics of the system like backup and updates [4].

As per GDPR guidelines, the patient records must be handled by data controllers and should be visible only to the respective departments after generating consent through a proper channel (exceptions may be handled separately for serious health issues or emergency conditions). The information stored in the database should be accurate, trustworthy, and comprehensive. Specifically, in emergency circumstances, the hospital personnel require some necessary and personal health information regarding the patients for better and faster treatment to save their life. The entire system works on the access control mechanisms due to sensitive and confidential information stored in the system and unauthorized access is restricted for anyone. Therefore, the emergency medical team cannot access the health record of the patient and even the patient is also not in the sense to change the access control for his/her EHRs.

Another significant challenge could be that his/her personal and medical records will be at high risk because in the black market the value of a single EHR is approx.25 for credit card details [5]. A number of medical staff have released the EHRs to the black market only for financial gains but this ratio has dropped significantly because of the new litigations formed

by governments all over the globe. Still, attackers can get the records by phishing attacks in which they masquerade as an authority to get the personal data. This attack is extremely successful, especially, in this pandemic situation when everything is going online and everyone is receiving numerous phone calls and emails from different agencies representatives and they ask for some personal details like name, address, unique id, etc. for verification to process further. For instance, the hacker successfully obtained significant information about staff at Magnolia Health Corporation (MHC) using a spoofed email from the CEO. On the other hand, the National Health Service (NHS) was attacked and encrypted with NHS files in 2017; as a result, all 6900 appointments got canceled [6] and there are many such examples reported in the literature for these kinds of thefts.

1.1 Motivation

The motivation behind developing a Healthcare Management System stems from the need to improve the efficiency, accessibility, and accuracy of healthcare services. Traditional systems often involve cumbersome paperwork, manual processes, and disconnected data management, which can lead to delays in patient care, errors, and inefficiencies. By implementing a digital system, healthcare providers can streamline operations, ensure secure and centralized access to patient records, and facilitate better decision-making. This system also aims to enhance patient experience by enabling easier appointment scheduling, reducing waiting times, and improving communication between patients and healthcare professionalsYou can also create section and subsection

1.2 Problem Statement

Accessing health care services across various hospitals or clinics for diagnosis and treatment has become quite widespread, especially for patients with chronic conditions like cancer, due to greater specialisation of health care services and high levels of patient mobility. Physicians can make wiser, safer, and more efficient clinical judgments if they have a thorough understanding of a patient's history. Due to the high sensitivity and privacy of electronic health records (EHR), most EHR data transfer is still done via fax or mail due to a lack of systematic infrastructure support for safe, trustable health data sharing, which can create significant delays in patient care.

1.3 Objectives

The objective of this project is to develop a secure, decentralized system for managing healthcare records using end-to-end encryption, blockchain technology, and advanced cryptographic methods. This ensures data confidentiality, integrity, and accessibility, while empowering patients with control over their own medical information. The project aims to enhance trust in healthcare data management by providing transparent and immutable record-keeping, thus safeguarding sensitive patient information from unauthorized access and tampering.

- Ensure Data Security and Privacy: Implement end-to-end encryption and decentralized storage to protect sensitive patient records from unauthorized access or tampering. By distributing encrypted data across multiple storage points, patient information remains secure from potential breaches.
- Leverage Blockchain for Immutable Record-Keeping: Use blockchain technology and Merkle Trees to create a decentralized, immutable ledger for healthcare records. This ensures transparency and traceability in data modifications, preventing any single entity from controlling the information, thus enhancing trust and accountability.
- Provide Patient Control Over Data: Empower patients with the ability to manage and control access to their medical records by utilizing SHA-256 hashing. This encryption method ensures that only authorized individuals or organizations can view the data, safeguarding patient privacy and ensuring they have control over who can access their personal information.
- Enhance Data Integrity and Transparency: Guarantee that any changes made to healthcare records are logged transparently and are traceable, thanks to the immutable nature of the blockchain, thus preventing any unauthorized or malicious alterations.
- Prevent Centralized Data Vulnerability: By decentralizing storage and management of healthcare records, eliminate the risk associated with centralized control, reducing the potential for data tampering, system failures, or single points of attack.

1.4 Scope

The scope of this blockchain-based healthcare records management system is to improve the security, privacy, and transparency of patient data by using cutting-edge technologies like blockchain, Merkle Trees, and cryptographic hashing. This system not only ensures efficient and tamper-proof management of healthcare records but also facilitates secure data sharing between authorized healthcare providers. It aims to streamline administrative processes, enhance patient care, and integrate advanced technologies such as telemedicine and AI-driven analytics to optimize healthcare delivery and outcomes.

- Enhanced Security and Privacy for Patient Records:** The system ensures that sensitive medical information is securely encrypted using SHA-256 and stored in a decentralized manner, protecting it from unauthorized access or tampering.
- Efficient Data Verification and Storage: By leveraging Merkle Trees, the system allows for efficient storage and quick verification of large volumes of patient data, without the need to revalidate the entire dataset, ensuring data integrity.
- Transparent Access for Authorized Parties: Authorized healthcare providers and entities, such as doctors and insurance companies, can securely and transparently access patient records, ensuring privacy while enabling accurate decision-making.

- Streamlining Administrative Functions: The system helps streamline patient registration, appointment scheduling, and electronic health record (EHR) management, reducing administrative burdens and enhancing the overall patient experience.
- Improved Healthcare Provider Communication and Data Sharing: It facilitates secure communication and data sharing among healthcare professionals, leading to improved collaboration, diagnosis, and treatment outcomes.
- Real-Time Access to Patient Information:The system ensures that medical professionals have real-time access to patient information, which can enhance diagnosis and treatment, especially in critical cases.
- Integration of Advanced Technologies: With the potential for integrating telemedicine, AI-driven analytics, and patient monitoring systems, the system contributes to improved health outcomes, optimized resource allocation, and more informed decision-making.
- Contribution to an Efficient Healthcare Ecosystem: By improving data management and healthcare delivery, the system helps create a more efficient, responsive, and optimized healthcare ecosystem for patients and providers alike.

Chapter 2

Literature Review

The literature review on blockchain-based healthcare record management systems highlights the increasing need for secure, decentralized, and tamper-proof data storage solutions in healthcare. Various studies demonstrate how blockchain technology ensures patient data privacy while enhancing interoperability and transparency between healthcare providers.

2.1 Comparative Analysis of Recent Study

Sr. No	Title	Author(s)	Year	Methodology	Drawback
1	BlockChain for Healthcare Management Systems [1]	Edgar R Dulce Villarreal ,Jose Garcia –Alonso , Enrique Moguel , & Julio Ariel Hurtado Alegria	2023	Conducts a systematic literature review (SLR) on architectural mechanism supporting interoperability & Security in Blockchain based Healthcare Management System	Complexity of Smart Contracts development, security Vulnerabilities, & balancing between interoperability & Security.
2	BlockChain – IOT Healthcare Applications & Trends [2]	Waffa A.N.A A-NBHANY, Ammar Zahary , & Asmaa shargabi	2023	Intersection of IoT, blockchain, and healthcare, analyzing various applications, sensors, hardware, and software used in blockchain-based healthcare systems.	Lacks focus on the software languages, databases, tools, and hardware platforms used in Blockchain-IoT healthcare applications.
3	A Blockchain-Based Electronic Medical Health Records Framework using Smart Contracts [3]	Vardhini B, Shreyas N Dass, Sahana R, Dr. R. Chinnaiyan	2021	The paper proposes using blockchain technology and smart contracts to create a decentralized Electronic Health Record (EHR) system, ensuring secure, immutable, and accessible medical records for stakeholders.	Potential privacy concerns, as it is possible to identify participants in the transactions, and improvements are needed to make medical records more accessible during emergencies.

Sr. No	Title	Author(s)	Year	Methodology	Drawback
4	Development of an Internet-of-Healthcare System Using Blockchain [4]	Suparat Yongjoh, Chakchai So-in, Peerapol Kompunt, Paisarn Muneesawang, Roy I. Morien	2021	The paper presents an Internet-of-Healthcare System (IoHCS) that integrates patient data from hospitals using blockchain technology for secure storage and access, supported by MQTT protocol for real-time data retrieval across multiple systems.	The system's reliance on blockchain increases complexity and can introduce challenges in scalability and integration with various hospital information systems
5	MedAccess: A Scalable Architecture for Blockchain-based Health Record Management [5]	Mohammed Misbhauddin, Abdulaziz AlAbdulatheam, Mohammed Aloufi, Hussien Al-hajji, Ahmad AlGhuwainem	2020	The paper proposes a scalable blockchain architecture using off-chain storage (IPFS), reducing on-chain data storage costs and improving data privacy and accessibility.	Storing large-scale medical records on blockchain remains computationally expensive, and the system requires further cost-reduction strategies for long-term feasibility.
6	BlockHR – A Blockchain-based Healthcare Records Management Framework: Performance Evaluation and Comparison with Client/Server Architecture [6]	Leila Ismail, Huned Materwala, Youssef Sharaf	2020	The study proposes BlockHR, a blockchain-based framework for healthcare record management, and compares its performance with the client-server model, evaluating security, privacy, and execution times for data operations.	BlockHR's write operations are slower than the client-server approach due to the consensus mechanism, though it offers significant improvements in data retrieval speed.

Sr. No	Title	Author(s)	Year	Methodology	Drawback
7	Attribute-based Multi-Signature and Encryption for EHR Management: A Blockchain-based Solution [7]	Hao Guo, Wanxin Li, Ehsan Meamari, Chien-Chung Shen, Mark Nejad	2020	Proposes a hybrid architecture integrating blockchain and edge nodes, using attribute-based multi-signature (ABMS) and attribute-based encryption (ABE) schemes for secure EHR management.	The system's verification phase is computationally intensive, especially as the number of attributes increases, and the implementation relies on external smart sensors for practical encryption.
8	Smart Contract Designs on Blockchain Applications [8]	Alkhansaa Abuhashim, Chiu C. Tan	2020	The paper evaluates the complexity and efficiency of two smart contract designs (Catalog and Sparse) for indexing and querying blockchain ride-sharing data, using Ethereum testnets data for experiments.	Querying Sparse smart contracts is inefficient and time-consuming, especially when scanning long blockchains, making them less suitable for applications needing frequent data retrieval.
9	Blockchain-Based Interoperable Electronic Health Record Sharing Framework [9]	Gracie Carter, Hossain Shahriar, Sweta Sneha	2019	The paper proposes a framework using blockchain and cloud computing (AWS and Ethereum) to enable interoperable EHR sharing with multilayer encryption and smart contracts for secure, automated data exchange.	The solution relies on Ethereum, which faces performance issues like scalability and slower transaction speeds, limiting its efficiency for large-scale healthcare data sharing.

Table 2.1: Comparative Analysis of Recent Studies

Chapter 3

3.1 Proposed System Architecture

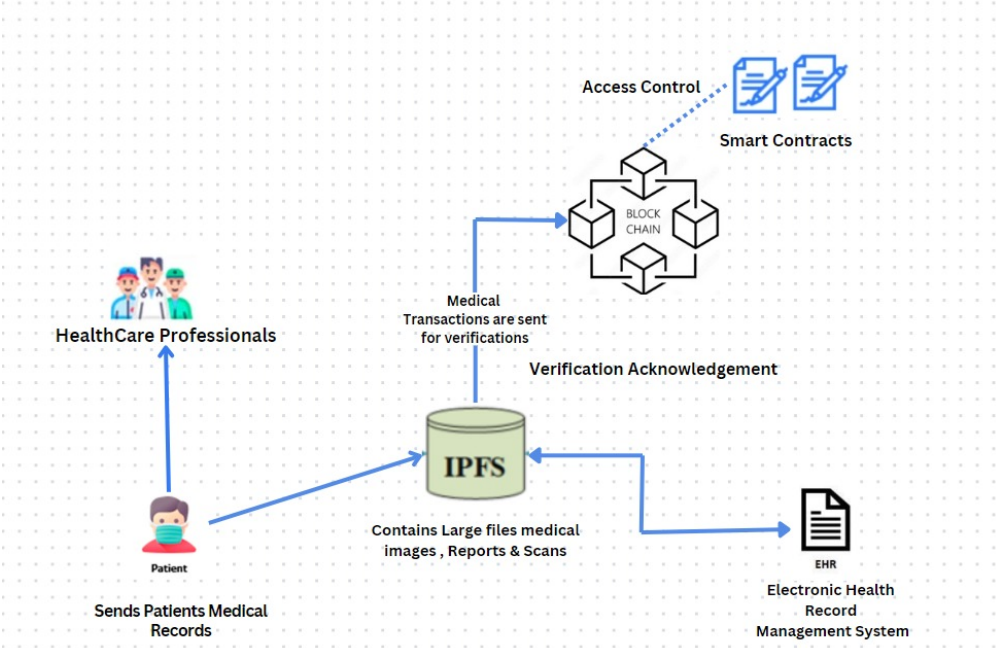

Figure 3.1: Proposed System Architecture of Meditrust

This project design outlines a system for managing patient medical records securely using blockchain technology and decentralized storage. The process starts with patients sending their medical records, including large files such as images, reports, and scans, to an InterPlanetary File System (IPFS), which is a decentralized storage solution designed to hold large medical files. These records are then accessed by healthcare professionals when needed.

The system uses blockchain to handle medical transactions, such as verifying that the records are accurate and belong to the correct patient. Blockchain ensures that every interaction with the records is transparent and secure, and it also employs smart contracts to control access, meaning only authorized individuals can view or update the information.

Once the transactions are verified, the blockchain provides verification acknowledgments to confirm that everything has been processed correctly. The records stored in the IPFS are also connected to an Electronic Health Record (EHR) Management System, which helps

manage and maintain the integrity of patient data. This entire process reduces manual tasks, ensures data privacy, and allows for a streamlined, decentralized approach to handling sensitive medical information.

In addition to enhancing security and privacy, this system also improves efficiency in managing healthcare data. By using decentralized storage like IPFS, it eliminates the need for traditional, centralized databases, reducing the risks of data breaches or loss. The integration of blockchain further ensures that every update or access to the data is immutable, meaning it cannot be altered or deleted, thus creating a trustworthy and transparent environment for handling patient information.

Moreover, the use of smart contracts automates key administrative processes, such as granting access to specific individuals and handling insurance claims. This automation minimizes the need for manual intervention, cutting down on paperwork and reducing errors in record management. Overall, this design provides a scalable, secure, and efficient solution for managing medical records in a way that gives patients more control over their data while simplifying healthcare workflows for professionals.

3.2 Data Flow Diagram(DFD)

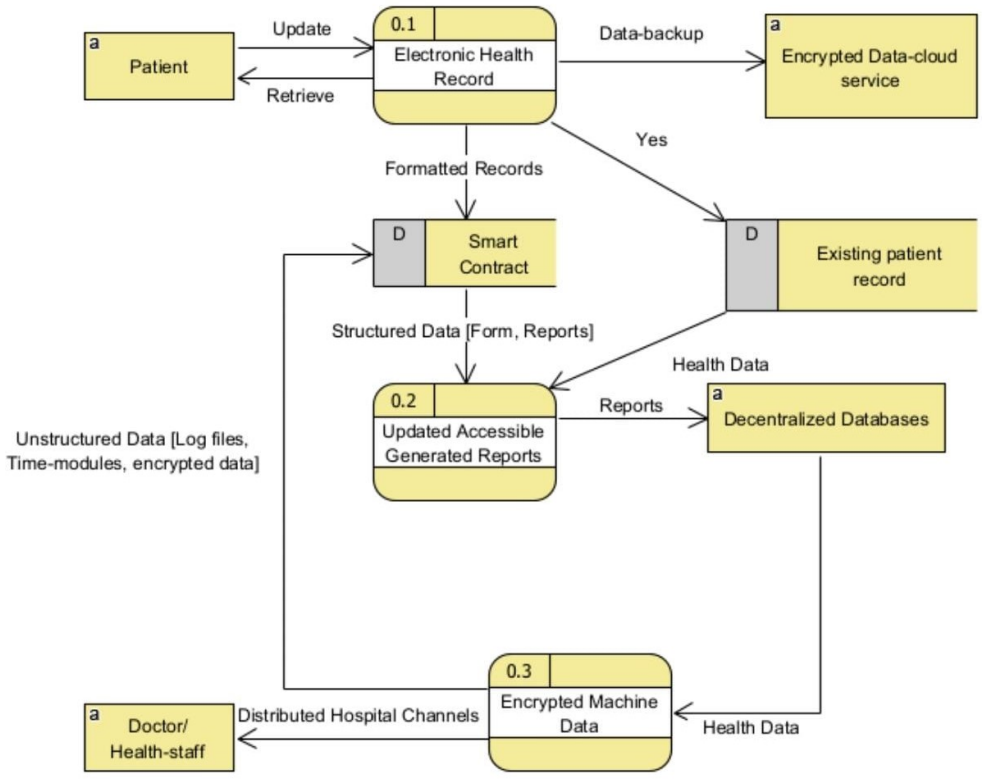

Figure 3.2: Data Flow Diagram of the proposed system

The Data Flow Diagram (DFD) illustrates a blockchain-based healthcare record management system. In this system, patients interact with an electronic health record (EHR), where they can update and retrieve their medical data. The EHR system backs up data to an encrypted cloud service for secure storage. Smart contracts play a pivotal role in verifying

patient records and structuring data such as forms and reports. Once the data is processed, it is made accessible through decentralized databases, ensuring security and accessibility for healthcare providers. Doctors and healthcare staff can access patient records via distributed hospital channels, receiving both structured reports and encrypted machine data, ensuring that sensitive information remains secure. The system also handles unstructured data, such as log files and encrypted data, ensuring comprehensive health data management across different platforms.

3.3 Use Case Diagram

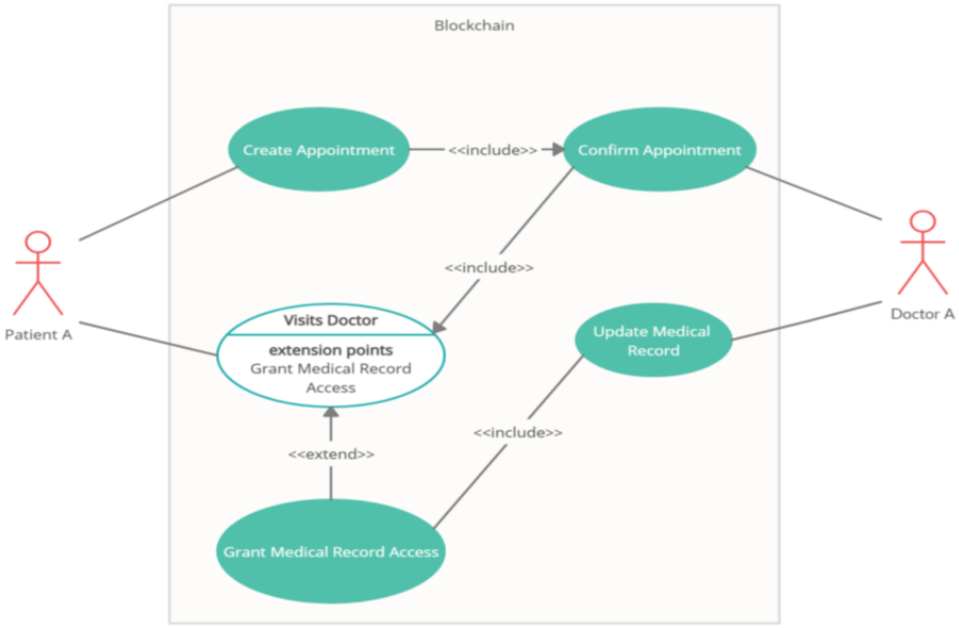

Fig 3.3 UML Use Case Diagram for Basic Scenario of the proposed system

A normal user and a blockchain member are compared in this scenario to see how different access control regulations affect them (patients, doctor, chemist, and path lab). Only approved members will be able to study data on the blockchain, and the rest of the world will be uninformed of any transaction participants. In this case, the usage of a powerful hashing mechanism as well as the notion of a shared ledger are both proven. The participants in the transaction should be provided a copy of the transaction, as illustrated Fig.3.3. The participants who are added as non-admin members on the blockchain are Member A, Patient A, Doctor A, Chemist A, and PathLab A.

The Figure illustrates a permissioned blockchain scenario where Patient A creates an appointment, which is confirmed through the Confirm Appointment use case involving Doctor A. During the visit, the patient may grant the doctor access to their medical records via the Grant Medical Record Access use case, shown as an extension point in the Visits Doctor use case. After the visit, Doctor A updates the patient's medical records using the Update Medical Record use case. The system ensures that all interactions and permissions are securely managed within the blockchain environment.

Chapter 4

Project Implementation

The technology stack required for the implementation of the blockchain-based healthcare records management system is divided into four main components: frontend, backend, database, and algorithms. For the frontend, the system uses HTML, CSS, and JavaScript to create a responsive and interactive user interface. These core web technologies enable the development of web pages where users can interact with the system, such as patients booking appointments or doctors accessing records. Additionally, Web3.js is utilized to connect the frontend to the blockchain, allowing users to interact with the smart contracts and blockchain network from their browser.

In the backend, Node.js and Express.js are used to handle server-side logic and API creation. These technologies allow communication between the frontend and the blockchain network, manage requests, and ensure smooth data flow. Alternatively, Python (Django) can be used as another backend framework to provide structure and manage different aspects of the application, depending on development needs. Furthermore, IPFS (InterPlanetary File System) is integrated to store large medical records off-chain while providing a decentralized, scalable solution for accessing these files securely.

Lastly, the algorithms used include SHA-256 and Merkle Tree. SHA-256 ensures the cryptographic security of the data, generating unique hashes for each medical record that are immutable and tamper-resistant. The Merkle Tree algorithm is used to efficiently verify large sets of data by breaking them into smaller hash components, allowing quick integrity checks across the entire system. These algorithms ensure that healthcare records are stored securely and can be verified for authenticity without compromising patient privacy.

The implementation of our blockchain-based healthcare record management system leverages Merkle trees to ensure data integrity and efficient verification. Each patient's health record is hashed and stored in a Merkle tree structure, where the root hash provides a unique fingerprint of the entire data set. This allows for quick and secure verification of individual records without needing to access the entire dataset, ensuring privacy and reducing processing time. The use of Merkle trees further strengthens the system's ability to detect tampering, providing a robust, scalable solution for managing healthcare records. In our project, we utilized NoSQL databases, specifically MongoDB, to handle the dynamic and unstructured nature of healthcare data.

NoSQL databases are well-suited for managing large volumes of distributed data, providing flexibility in storage and retrieval, which is crucial in a decentralized system. MongoDB's document-based storage model allows us to efficiently manage diverse patient records, reports, and logs without the constraints of traditional relational databases. Its scalability and

high availability features support the real-time access required in a healthcare environment, making it a reliable choice for our blockchain-integrated system.

4.1 Timeline Sem VII

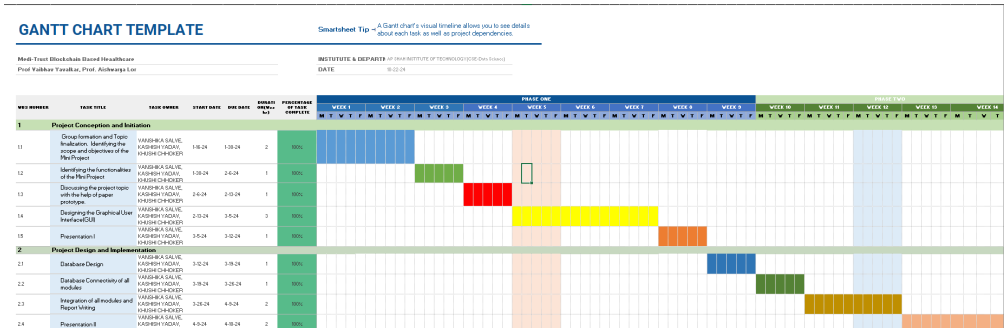

Figure 4.1: Timeline of the Project Milestones

The Gantt chart outlines the scheduling and progress tracking for the "Medi-Trust Blockchain-Based Healthcare" project, divided into two main phases: Project Conception and Initiation and Project Design and Implementation, spanning 14 weeks. The first phase covers tasks such as group formation, defining the project scope, identifying functionalities, and designing the graphical user interface (GUI). Each task is assigned a duration, with the chart indicating 100% completion of all tasks in this phase, as represented by fully shaded blue, green, and red bars. .

The second phase focuses on the implementation of blockchain technology, which includes tasks such as integrating blockchain for data management, ensuring secure connectivity, incorporating smart contracts, and testing the system. These tasks are scheduled to run concurrently between weeks 7 and 13, with progress shown by color-coded bars. The chart illustrates task dependencies and timelines, ensuring efficient coordination among team members and helping the project stay on track for timely completion. The Gantt chart serves as a vital tool for monitoring progress and ensuring the successful delivery of the project.

4.2 System Prototype

The prototype of our Blockchain-Based Healthcare Management System is designed to demonstrate the core functionalities of secure, decentralized health data management. This prototype focuses on enhancing data security, privacy, and transparency, cryptographic hashing, and decentralized storage mechanisms. By integrating these technologies, the system prototype ensures that sensitive patient information is protected from unauthorized access and tampering, while also allowing authorized parties, such as doctors and healthcare providers, to access data transparently. The prototype showcases key features like encrypted patient record storage, decentralized data access control, and immutable audit trails for any data modifications, setting the foundation for a robust healthcare management solution.

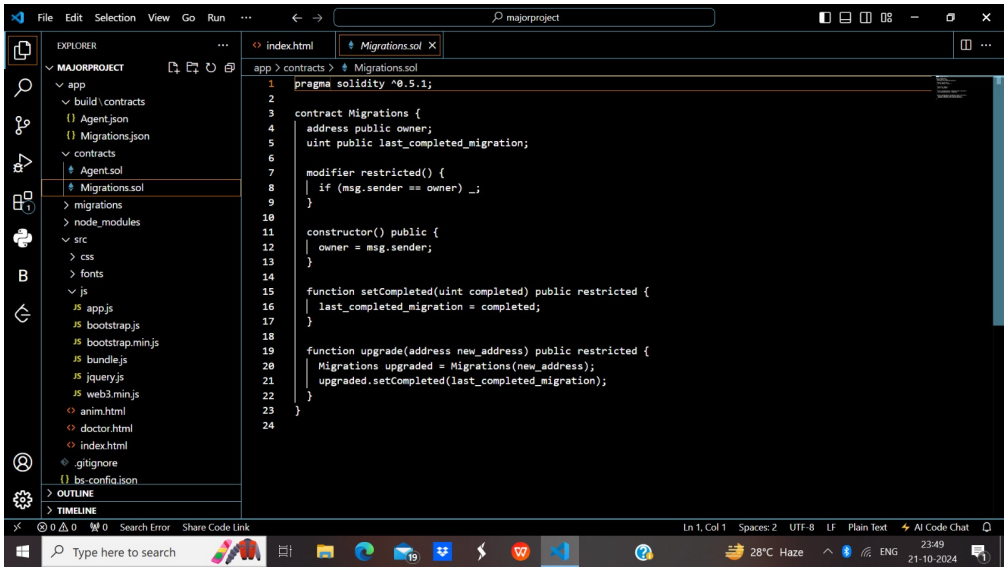

Figure 4.2: Migrations Contract Code in Solidity for Blockchain Deployment

The image displays a Migrations contract written in Solidity, which is primarily used in Ethereum blockchain development to manage and track the deployment of smart contracts. This contract is a key component in the Truffle framework and ensures that contracts are deployed sequentially and correctly.

The contract defines two main state variables: owner, which holds the address of the contract owner (typically the person deploying the contract), A custom modifier called restricted is implemented to ensure that only the owner can invoke certain functions, checking if msg.sender (the address calling the function) matches the owner's address.

The constructor function is executed during the contract deployment, automatically assigning the deployer's address (msg.sender) as the owner. The setCompleted function updates the last completed migration variable to reflect the latest completed migration step. This function is restricted to be called only by the owner, maintaining security and control over the migration process.

Additionally, the contract includes an upgrade function, which allows the migration process to transfer control to a new Migrations contract. This function takes the new contract's address as input and ensures that the migration history is preserved by setting the last In summary, the Migrations contract plays a vital role in managing the deployment process by tracking migration steps, ensuring smooth upgrades .

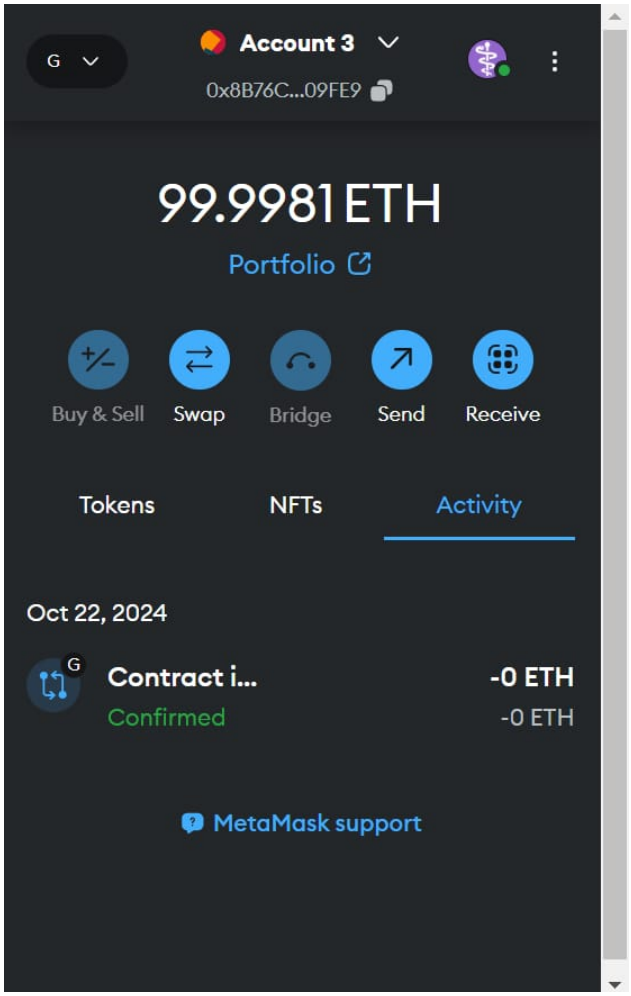

Figure 4.3: MetaMask Account Dashboard with Transaction Activity

The image shows the dashboard of a MetaMask wallet (Account 3) with an Ethereum balance of 99.9981 ETH. The wallet displays common actions such as Buy Sell, Swap, Bridge, Send, and Receive, allowing the user to interact with Ethereum and other blockchain networks. The address of the wallet begins with 0x8B76...09FE9, partially displayed for privacy.

In the Activity section, there is a confirmed transaction involving a contract interaction on October 22, 2024, which is associated with 0 ETH being transferred. This indicates that the transaction likely involved a contract call that didn't transfer any Ether (ETH) but interacted with a smart contract on the blockchain. MetaMask also provides options for viewing tokens and NFTs and has a support link for assistance.

This dashboard highlights MetaMask's role as a user-friendly interface for managing digital assets, performing transactions, and interacting with decentralized applications (dApps) on the Ethereum network.

Chapter 5

Summary

The implementation of a blockchain-based healthcare management system has demonstrated significant improvements in data security, transparency, and access control for sensitive medical records. One of the core components, blockchain technology, ensures that all medical transactions are securely verified and immutably recorded. This system addresses the key concerns of privacy, integrity, and traceability, offering an effective solution to the vulnerabilities in traditional healthcare management. The consensus-driven verification process ensures that medical records are tamper-proof, reducing the risk of data breaches or unauthorized access.

The integration of smart contracts plays a pivotal role in automating access control. By leveraging these self-executing contracts, the system ensures that only authorized healthcare professionals have access to specific medical data, based on predefined permissions. This process eliminates the need for manual checks, increasing the efficiency and accuracy of access control while reducing human errors. The automation also simplifies regulatory compliance, as smart contracts can be programmed to enforce data-sharing policies aligned with standards such as HIPAA and GDPR.

Inter Planetary File System (IPFS) has been utilized to manage the storage of large medical files, such as images, reports, and scans. Instead of storing this data directly on the blockchain, which could lead to performance issues due to its size, IPFS offers a decentralized solution for handling these large files. The use of IPFS ensures that patient medical records are easily accessible by authorized personnel while maintaining the confidentiality and integrity of the data. This decentralized approach also improves data availability and prevents the risks associated with centralized storage, such as single points of failure.

The overall system ensures seamless interaction between healthcare professionals, patients, and the Electronic Health Record (EHR) management system. Patients can securely submit their medical records through the system, which are then verified and shared with healthcare professionals via the blockchain. The blockchain, acting as an intermediary, not only facilitates secure transactions but also provides real-time verification acknowledgments, confirming that the data shared is authentic and valid. This enhances trust among the participants and ensures that the patient's data is handled with utmost care and confidentiality.

Bibliography

[1] Edgar R. Dulce Villarreal, JoseGarcia- Alonso, Enrique Moguel, Julio Ariel Hurtado Alegria, "BlockChain for Healthcare Management Systems," 2023.

[2] Waffa A.N.A A-NBHANY, Ammar Zahary, Asmaa Shargabi, "BlockChain IOT Healthcare Applications Trends," 2023.

[3] Vardhini B., Shreyas N. Dass, SahanaR., R. Chinnaiyan, Blockchain-Based Electronic Medical Health Records Framework using Smart Contracts," 2021.

[4] Suparat Yongjoh, Chakchai So-in, Peerapol Kompunt, Paisarn Muneesawang, Roy I. Morien, "Development of an Internet-of-Healthcare System Using Blockchain," 2021.

[5] Mohammed Misbhauddin, Abdulaziz AlAbdulatheam, Mohammed Aloufi, Hussien Alhajji, Ahmad AlGhuwainem,"MedAccess: A Scalable Architecture for Blockchain-based Health Record Management," 2020.

[6] Leila Ismail, Huned Materwala, Youssef Sharaf, "BlockHR – A Blockchain-based Healthcare Records Management Framework: Performance Evaluation and Comparison with Client/Server Architecture," 2020.

[7] Hao Guo, Wanxin Li, Ehsan Meamari, Chien-Chung Shen, Mark Nejad, "Attribute-based Multi-Signature and Encryption for EHR Management: A Blockchain-based Solution," 2020.

[8] Alkhansaa Abuhashim, Chiu C. Tan, "Smart Contract Designs on Blockchain Applications,"2020.

[9] Gracie Carter, Hossain Shahriar, Sweta Sneha, "Blockchain-Based Interoperable Electronic Health Record Sharing Framework," 2019.

[10] Li Qing, "Research on E-commerce User Information Encryption Technology Based on Merkle Hash Tree," 2019.

[11] Ayesha Shahnaz, Dr. Usman Qamar, Dr. Ayesha Khalid, "Using Blockchain for Electronic Health Records," 2019.