A PROJECT REPORT ON

Healthcare Records Management System Using Blockchain

SUBMITTED TO THE SAVITRIBAI PHULE UNIVERSITY, PUNE
IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE

OF

BACHELOR OF ENGINEERING (Computer Engineering)

SUBMITTED BY

Atharva Walke	Exam No: B190054217
Nikhil Awatade	Exam No: B190054220
Tejas Bendkule	Exam No: B190054227
Atharva Deshmukh	Exam No: B190054261

DEPARTMENT OF COMPUTER ENGINEERING
Pune Institute of Computer Technology
Dhankawadi, Pune - 411043

SAVITRIBAI PHULE PUNE UNIVERSITY

2023-2024

CERTIFICATE

This is to certify that the project report entitled
Healthcare Records Management System Using Blockchain

Submitted by

Atharva Walke	Exam No: B190054217
Nikhil Awatade	Exam No: B190054220
Tejas Bendkule	Exam No: B190054227
Atharva Deshmukh	Exam No: B190054261

is a bonafide student of this institute and the work has been carried out by him/her under the supervision of **Prof. R.R.Jadhav** and it is approved for the partial fulfillment of the requirement of Savitribai Phule Pune University, for the award of the degree of **Bachelor of Engineering** (Computer Engineering).

Prof. R.R.Jadhav
Internal Guide
Dept. of Computer Engg.

Dr. G.V. Kale
Head
Dept. of Computer Engg.

Dr. S.T. Gandhe
Principal
Pune Institute of Computer Technology

Place:Pune
Date:

ACKNOWLEDGEMENT

It gives us great pleasure in presenting the project report on ***'Healthcare Records Management System Using Blockchain****.*

We would like to take this opportunity to thank ***Prof. R.R.Jadhav*** *giving me all the help and guidance we needed. We are really grateful to them for their kind support. Their valuable suggestions were very helpful.*

We are also grateful to ***Dr. G.V. Kale****, Head of Computer Engineering Department, PICT for his indispensable support, suggestions.*

In the end our special thanks all faculty members for their whole hearted cooperation for completion of this report. We also thank our laboratory assistants for their valuable help in laboratory.

Atharva Walke
Nikhil Awatade
Tejas Bendkule
Atharva Deshmukh
(B.E. Computer Engg.)

ABSTRACT

In an evolving healthcare landscape, ensuring patient focus is paramount to the quality and efficiency of services. This project proposes the use of blockchain technology to transform healthcare systems, with greater emphasis on patient-centered improvements. Using blockchain's inherent characteristics of transparency, immutability and decentralization, the proposed system aims to address various challenges inherent in traditional healthcare systems, such as data security, collaboration and patient privacy

The ultimate goal of this project is to create a patient-centric healthcare system that empowers individuals to have greater control over their medical information, and patients through the use of blockchain technology that facilitates seamless communication with healthcare providers den Health care organizations will have a unified and secure platform to access, manage and share their health records, eliminating the need for unnecessary paperwork and streamlining the entire care process.

Additionally, the proposed system would enable the secure sharing of medical information between authorized persons, ensuring that healthcare professionals can access complete and accurate information to make informed decisions about patients look at it. By establishing a network of trust, the project aims to foster collaboration and collaboration among various stakeholders in the healthcare delivery system, ultimately improving patient outcomes and improving healthcare delivery face.

Combining blockchain technology, patient-centric design principles, smart contracts and innovation, this project seeks to transform healthcare by putting patients at the center of care delivery through empowerment individuals to manage their health information. It's also about creating a patient-centered healthcare system.

Index

List of Figures

CHAPTER 1

INTRODUCTION

1.1 Overview

The Healthcare Records management system involve detailing how patient records are stored, accessed, and updated on the blockchain network, ensuring data integrity, privacy, and interoperability among different healthcare stakeholders.

The architecture of this system comprises multiple components, including a distributed ledger for storing encrypted patient records, smart contracts for executing predefined rules, and user interfaces for interaction. Patient records are encrypted and stored on the blockchain network, ensuring confidentiality and integrity. Each record is associated with a unique identifier, allowing authorized parties to access relevant information while maintaining privacy.

Smart contracts govern access control mechanisms, allowing patients to grant permissions for healthcare providers to view or update their records. Access rights are managed transparently on the blockchain, minimizing the risk of unauthorized access.

The blockchain ledger serves as a tamper-proof audit trail, enabling regulatory compliance and accountability. All transactions are timestamped and cryptographically secured, providing a transparent and immutable record of data access and modifications

1.2 Motivation

The motivation for developing a real-time healthcare records management system is from the recognition of significant challenges within traditional healthcare record management systems. These challenges include data breaches, lack of interoperability between healthcare providers, compromised patient privacy, and inefficiencies in data exchange processes.

Our thoughts are driven by the understanding that effective management of healthcare records is fundamental to ensuring patient safety, improving clinical outcomes, and enhancing overall quality of care. We aim to address these challenges and improve the healthcare ecosystem by leveraging blockchain technology, which offers unique capabilities such as decentralization, immutability, transparency, and cryptographic security.

1.3 Problem Definition and Objectives

Problem Definition: Traditional healthcare record management systems face several challenges, including data breaches, lack of interoperability, compromised patient privacy, and inefficiencies in data exchange processes. These challenges hinder effective patient care and compromise the integrity and security of healthcare data. Therefore, there is a need for innovative solutions to address these issues and enhance healthcare record management.

Objectives:

1. Enhance Data Security: Implement a blockchain-based system to enhance the security of healthcare records by leveraging cryptographic techniques and decentralized storage.
2. Improve Interoperability: Facilitate seamless data exchange between different healthcare providers and systems by adopting standardized protocols and interoperable data formats.
3. Smart Contracts: Implement smart contracts to automate and enforce predefined rules and conditions for data access, sharing, and updating, thereby streamlining administrative processes and ensuring compliance.
4. Decentralized Identifiers (DIDs): Employ DIDs to uniquely identify patients and healthcare providers within the blockchain network, enabling secure and interoperable data exchange while preserving privacy.
5. Regulatory Compliance: Ensure compliance with relevant healthcare regulations and data protection laws, such as HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation), and others, to safeguard patient rights and privacy.

1.4 Project Scope & Limitations

The The project focuses on transitioning from centralized methods of storing medical data to a decentralized system using blockchain technology. Specifically, it entails the development of a blockchain-based platform for healthcare record management. This transition aims to enhance the security of patient health records by leveraging cryptographic techniques to encrypt data and store it across multiple nodes in the blockchain network. Moreover, standardized protocols and data formats will be implemented to improve interoperability between different healthcare organizations and systems. Smart contracts will facilitate seamless data exchange and ensure consistency in data representation. Patients will gain greater control over their health data through public-private key cryptography, allowing them to access and manage their records securely. Integration of smart contracts into the blockchain network will automate and enforce agreements between various parties involved in healthcare record management, such as consent management for data sharing and access control policies enforcement.

However, several challenges must be addressed during implementation. Technological hurdles, including scalability, network congestion, and transaction costs, need to be mitigated through careful selection of blockchain platforms and optimization of network architecture. Regulatory compliance with healthcare regulations and data protection laws, such as HIPAA and GDPR, is crucial and will be integrated into the platform to ensure secure handling of patient data. The complexity of integrating blockchain with existing healthcare IT infrastructure and systems must be navigated, with compatibility issues and interoperability concerns addressed through thorough testing and stakeholder collaboration. User adoption may vary, influenced by factors such as user training and perceived benefits. Therefore, education and training programs will be implemented to ensure user comfort with the new system. Lastly, data migration from existing healthcare records to the blockchain-based system requires meticulous planning and execution to preserve data integrity and minimize disruptions to healthcare operations

1.5 Methodologies of Problem solving

Requirement Analysis: Conduct a comprehensive analysis of the requirements and challenges associated with traditional healthcare record management systems. Identify the specific needs of patients, healthcare providers, and other stakeholders to inform the design and implementation of the blockchain-based solution.

Technology Evaluation: Evaluate different blockchain platforms and technologies to determine the most suitable option for the project's requirements. Consider factors such as scalability, security, interoperability, and ease of integration with existing healthcare IT infrastructure.

System Design: Design the architecture of the blockchain-based healthcare record management system. Define the data models, smart contracts, and user interfaces required to ensure data security, interoperability, and user accessibility. Consider the integration of additional features such as encryption, and audit trails.

Prototype Development: Develop a prototype or proof-of-concept implementation of the blockchain-based healthcare record management system. This involves implementing core functionalities such as patient registration, record creation, data encryption, and smart contract integration. Iterate on the prototype based on feedback and testing results.

Integration with Existing Systems: Integrate the blockchain-based system with existing healthcare IT infrastructure and systems. Ensure compatibility and interoperability between the blockchain network and other systems used by healthcare organizations, such as electronic health record (EHR) systems and medical devices.

Testing and Quality Assurance: Conduct rigorous testing of the blockchain-based system to ensure functionality, security, and performance. Perform testing scenarios to validate data integrity, access controls, interoperability, and system scalability. Implement quality assurance measures to identify and address any issues or vulnerabilities.

User Training and Adoption: Provide training and support to users, including patients and healthcare staff, on how to use the blockchain-based system effectively. Promote awareness and adoption of the system through educational initiatives, demonstrations, and incentives. Gather feedback from users to continuously improve the system's usability and functionality.

Deployment and Maintenance: Deploy the blockchain-based healthcare record management system in production environments. Implement mechanisms for continuous monitoring, maintenance, and updates to ensure system stability, security, and performance. Address any issues or challenges that arise during deployment and provide ongoing support to users

CHAPTER 2

LITERATURE SURVEY

2.1 Centralized Systems

Centralized EHR systems store medical records in a central database managed by healthcare organizations. Access to the database is controlled through role-based authentication, where users are granted specific permissions based on their roles within the organization. These systems employ encryption techniques to protect sensitive patient data from unauthorized access. Regular audits and access logs are maintained to monitor user activity and ensure compliance with security policies. While centralized EHR systems provide a convenient way to store and access medical records, they are vulnerable to data breaches and single points of failure.

2.2 Decentralized Electronic Health Record (EHR) Systems

Decentralized EHR systems leverage blockchain technology to distribute medical records across a network of nodes. Each node in the network maintains a copy of the entire blockchain, ensuring redundancy and data integrity. Patient records are encrypted and stored in blocks on the blockchain, making them tamper-proof and secure. Access to patient records is controlled through smart contracts, which enforce access permissions based on predefined rules. Decentralized EHR systems offer enhanced security and privacy compared to centralized systems, as patient data is not stored in a single location and cannot be easily tampered with.

2.3 Personal Health Record (PHR) Systems

Personal health record (PHR) systems empower individuals to store and manage their own medical records securely. These systems allow patients to create and maintain their health records electronically, providing them with full control over their data. PHR systems often employ encryption and authentication mechanisms to ensure the security and privacy of patient information. Patients can choose to share their records with healthcare providers as needed, enabling seamless communication and collaboration. PHR systems promote patient engagement and empowerment by giving individuals direct access to their health information.

2.4 Cloud-Based Electronic Health Record (EHR) Systems

Cloud-based EHR systems store medical records on remote servers maintained by third-party cloud service providers. These systems offer scalability, flexibility, and cost-effectiveness compared to traditional on-premises solutions. Cloud-based EHR systems implement robust security measures such as data encryption, access controls, and regular security audits to protect patient data from unauthorized access and breaches. However, concerns about data privacy, compliance, and vendor lock-in are important considerations when adopting cloud-based EHR systems.

2.5 Hybrid Electronic Health Record (EHR) Systems

Hybrid EHR systems combine elements of both centralized and decentralized storage architectures. These systems store sensitive patient data in a centralized database while using blockchain technology to secure and authenticate access to the data. Hybrid EHR systems offer the benefits of both centralized and decentralized approaches, including scalability, data integrity, and interoperability. However, implementing and managing hybrid systems can be complex and require careful consideration of security, privacy, and regulatory requirements.

CHAPTER 3

SOFTWARE REQUIREMENTS SPECIFICATION

3.1 Assumptions and Dependencies

Understood. The dependency of your project is solely on having a smartphone and a stable internet connection. These two factors are crucial for the functioning and accessibility of the real-time Records management system. Here's how each dependency contributes to the project:

3.1.1 Electronics Devices

Standard desktop computers or laptops for accessing the HRMS web application are required. Any electronic device which supports a browser works. But it is best recommended to use Chrome as it has compatibility with MetaMask. Just install the MetaMask extension in your browser and connect it to your wallet. This is required for making transaction while booking an appointment. Moderate hardware specifications (e.g., multi-core processors, 8 GB RAM) to ensure smooth performance of the web application.

3.1.2 Stable Internet Connection

A stable internet connection is essential for seamless communication between the attendees' smartphones and the attendance system's server. It enables real-time synchronization of attendance data, ensuring that attendance records are immediately updated and accessible to administrators and educators. A stable internet connection also facilitates the transmission of attendance data securely and reliably, preventing any delays or disruptions in the process.

By having a smartphone and a stable internet connection as the sole dependencies, the real-time attendance system becomes more accessible and convenient for users. It eliminates the need for additional hardware or infrastructure, making the system cost-effective and adaptable to various environments. However, it is important to ensure that attendees have access to smartphones and reliable internet connectivity to fully utilize the benefits of the system.

3.2 Functional Requirements

3.2.1 Immutable Record Storage

The system should ensure that once healthcare records are added to the blockchain, they cannot be altered or deleted. This immutability is a fundamental characteristic of blockchain technology and ensures the integrity and trustworthiness of the records..

3.2.2 Permissioned Access Control

Implement a permissioned blockchain network where only authorized entities, such as healthcare providers, patients, and relevant stakeholders, can access specific healthcare records. Access control mechanisms should be enforced through cryptographic keys and smart contracts.

3.2.3 Interoperability and Data Standardization

Ensure compatibility and seamless exchange of healthcare records between different healthcare providers and systems. Adherence to industry standards such as HL7 (Health Level Seven) for data exchange and FHIR (Fast Healthcare Interoperability Resources) for data representation is crucial.

3.2.4 Integration with Existing Systems

Ensure seamless integration with existing electronic health record (EHR) systems, healthcare databases, and other healthcare IT infrastructure. APIs (Application Programming Interfaces) and middleware should be provided to facilitate data exchange and interoperability between the blockchain-based system and legacy systems.

3.3 External Interface Requirements

3.3.1 User Interfaces

Patient Interface: Patients should have a user-friendly interface to access their medical records securely. This interface should allow them to view, update, and share their health information with authorized parties.

Healthcare Provider Interface: Healthcare professionals need an intuitive interface to access patient records, update information, and track patient history. This interface should integrate seamlessly with existing Electronic Health Record (EHR) systems.

Administrator Interface: System administrators require a comprehensive interface to manage user access, configure system settings, monitor.

3.3.2 Integration with Healthcare Systems

Electronic Health Record (EHR) Systems: The blockchain-based healthcare records management system must integrate with existing EHR systems used by healthcare providers. This integration ensures interoperability and allows for the seamless exchange of patient data between different healthcare entities.

Health Information Exchange (HIE) Networks: Integration with HIE networks facilitates the secure exchange of patient information between different healthcare organizations while ensuring compliance with privacy regulations.

Pharmacy Systems: Integration with pharmacy systems enables the transmission of electronic prescriptions and medication-related information between healthcare providers and pharmacies.

3.3.3 Blockchain Network Interfaces

Consensus Mechanism: The system should support a consensus mechanism that ensures the integrity and immutability of data stored on the blockchain. Common consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT).

Smart Contract Integration: Smart contracts can be used to automate certain processes within the healthcare records management system, such as permission management, data sharing agreements, and payment processing.

3.4 Nonfunctional Requirements

3.4.1 Performance Requirements

1. Throughput: The system should handle a high volume of transactions efficiently, ensuring timely recording and retrieval of healthcare records.
2. Response Time: Transactions such as adding or retrieving records should have minimal latency to provide a seamless user experience.
3. Scalability: The system should be scalable to accommodate an increasing number of users and records without compromising

performance.

4. Consistency: Consistency in transaction processing is crucial to ensure that all nodes in the blockchain network reach consensus effectively without delays.

5. Fault Tolerance: The system should remain operational even in the event of network disruptions or node failures, maintaining data integrity and availability.

3.4.2 Safety Requirements

1. Data Integrity: Blockchain's immutability should ensure that healthcare records cannot be altered or tampered with once they are recorded, ensuring the accuracy and reliability of patient data.

2. Regulatory Compliance: The system should comply with relevant healthcare regulations (such as HIPAA in the United States) to ensure the privacy and security of patient information.

3. Auditability: All transactions and changes to healthcare records should be auditable, allowing for traceability and accountability.

4. Disaster Recovery: Implement mechanisms for data backup and recovery to ensure that healthcare records remain accessible even in the event of a disaster or system failure.

3.4.3 Security Requirements

1. Encryption: Utilize strong encryption techniques to secure data both in transit and at rest, protecting patient confidentiality and preventing unauthorized access.

2. Access Control: Implement role-based access control mechanisms to restrict access to healthcare records based on users' roles and privileges, ensuring that only authorized personnel can view or modify sensitive information.

3. Identity Management: Utilize digital signatures and cryptographic techniques to authenticate users and ensure that only authorized individuals can interact with the system.

4. Blockchain Security: Ensure the security of the blockchain network through consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS), preventing unauthorized changes to the distributed ledger.

3.5 System Requirements

1. Blockchain Framework: Determine which blockchain framework suits the requirements best. Options include Ethereum, Hyperledger Fabric, R3 Corda, etc.

2. Consensus Mechanism: Choose the appropriate consensus mechanism for the blockchain network, such as Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), etc.

3. Smart Contract Development: Define the smart contracts necessary for managing healthcare records, including access control, data integrity verification, and data sharing agreements.

4. Server Infrastructure: Depending on the scale of the system, servers should have adequate processing power, memory, and storage to handle the blockchain network and associated databases.

5. Redundancy: Implement redundant hardware configurations to ensure high availability and fault tolerance.

6. Security Measures: Employ hardware security modules (HSMs) to safeguard cryptographic keys and ensure the integrity of the blockchain network.

3.6 Analysis Models: SDLC Model to be applied

For a healthcare records management system utilizing blockchain technology, a suitable Software Development Life Cycle (SDLC) model would need to encompass the unique requirements and challenges of blockchain integration, as well as the sensitive nature of healthcare data. Let's explore an analysis using a modified version of the Waterfall model, adapted to fit the intricacies of blockchain development in healthcare:

1. Requirements Gathering and Analysis: Identify stakeholders including healthcare providers, patients, regulatory bodies, and IT professionals. Define the functional and non-functional requirements for the healthcare records management system, considering data security, privacy, interoperability, and regulatory compliance.

2. System Design: Design the architecture of the blockchain-based healthcare records management system, considering factors such as data encryption, decentralization, consensus mechanisms, and smart contracts.

3. Implementation: Develop the smart contracts and deploy them onto the blockchain network, ensuring that they enforce the necessary rules for data access, sharing, and validation. Implement the front-end interfaces for healthcare professionals, administrators, and patients, enabling secure access to the blockchain-based system.

4. Testing: Conduct comprehensive testing to validate the functionality, security, and performance of the blockchain-based healthcare records management system. Perform penetration testing and vulnerability assessments to identify and mitigate potential security risks.

5. Deployment: Deploy the blockchain-based healthcare records management system in a controlled environment, ensuring minimal disruption to existing healthcare operations. Provide training and support to healthcare professionals and system administrators to facilitate the adoption of the new system.

6. Maintenance and Support: Establish procedures for ongoing maintenance, including regular backups, system updates, and security audits. Provide continuous support to address user inquiries, troubleshoot technical issues, and implement enhancements based on user feedback and evolving regulatory requirements.

CHAPTER 4

SYSTEM DESIGN

4.1 System Architecture

4.1.1 Mathematical Model

The Electronic Health Record (EHR) Management System utilises a sophisticated mathematical model to maintain the confidentiality, integrity, and efficiency of healthcare record management using blockchain technology. At their heart, cryptographic methods like SHA-256 and Elliptic Curve Cryptography (ECC) protect the confidentiality and integrity of patient health information, ensuring that sensitive data is tamper-proof throughout its lifecycle. This security foundation is supplemented by a consensus mechanism, driven by algorithms such as Proof of Work (PoW) or Proof of Stake (PoS), that validates and adds new blocks of data to the blockchain ledger, ensuring the immutability and trustworthiness of the health record database.

Smart contracts developed in Solidity automate access control and data sharing policies by carrying out preset actions based on established conditions, ensuring safe and transparent governance of health record access and sharing. Advanced data structures, such as Merkle trees, are used to efficiently organise and store health records within the blockchain ledger, allowing for quick and safe access while ensuring data integrity. Furthermore, performance analytic tools that employ queueing theory and stochastic processes forecast system performance under different loads and conditions, resulting in optimal resource utilisation and user experience. In summary, this mathematical model supports the Electronic Health Record Management System's ability to transform healthcare record management, benefiting patients, healthcare providers, and the industry as a whole.

4.2 Architecture diagram

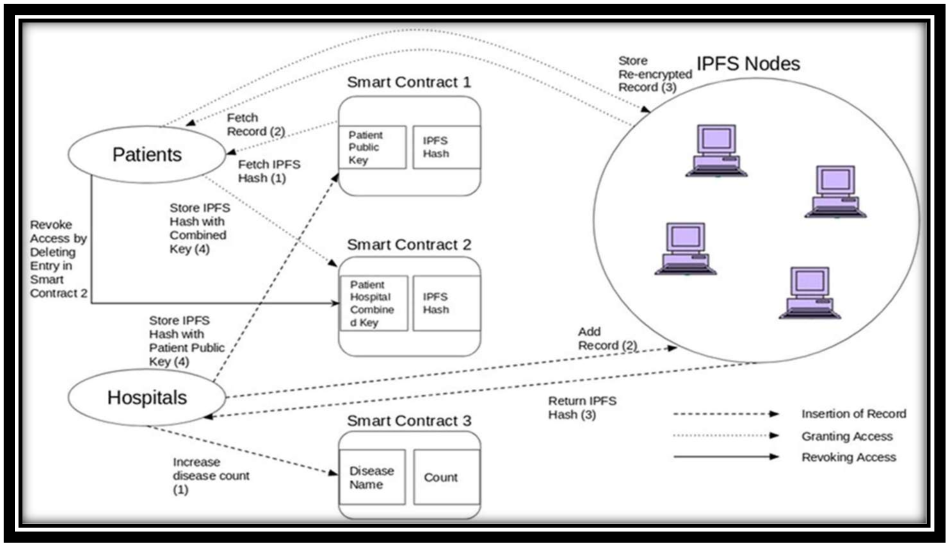


Figure 4.1: Architecture diagram

4.3 Activity Diagram

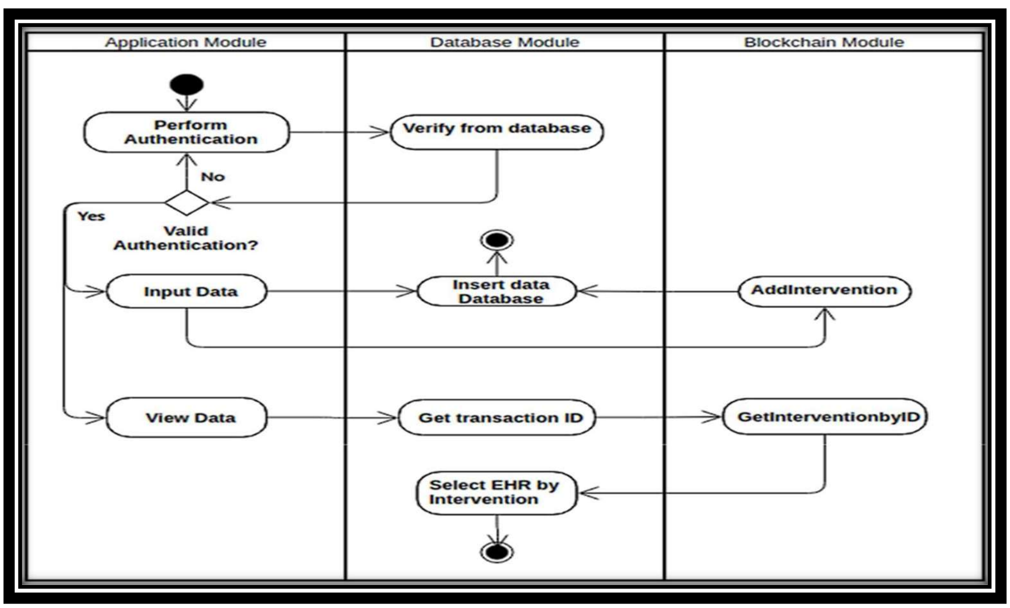


Figure 4.2: Activity diagram

4.4 Use Case Diagram

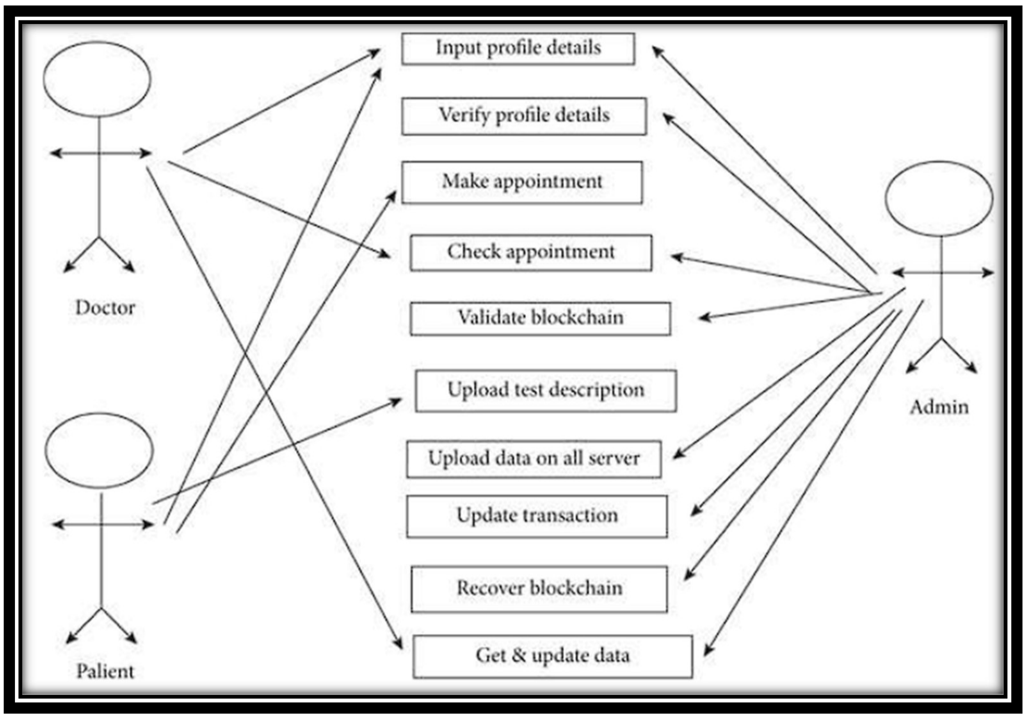


Figure 4.3: Use Case Diagram

4.5 Class Diagram

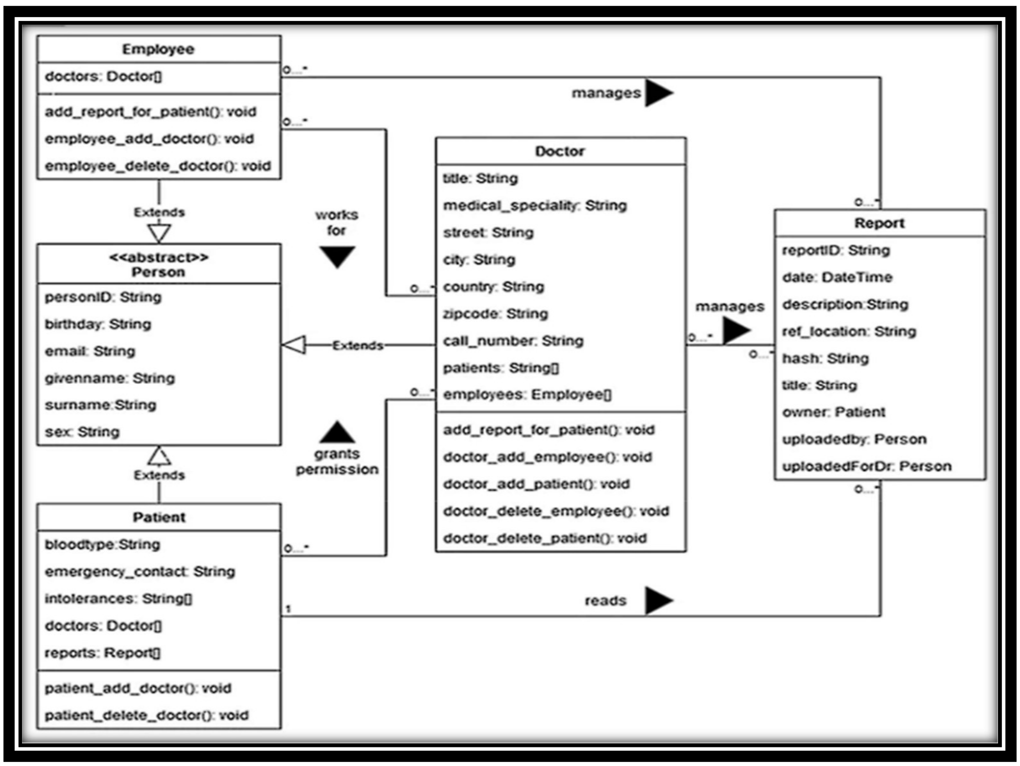


Figure 4.4: Class diagram

4.6 Component Diagram

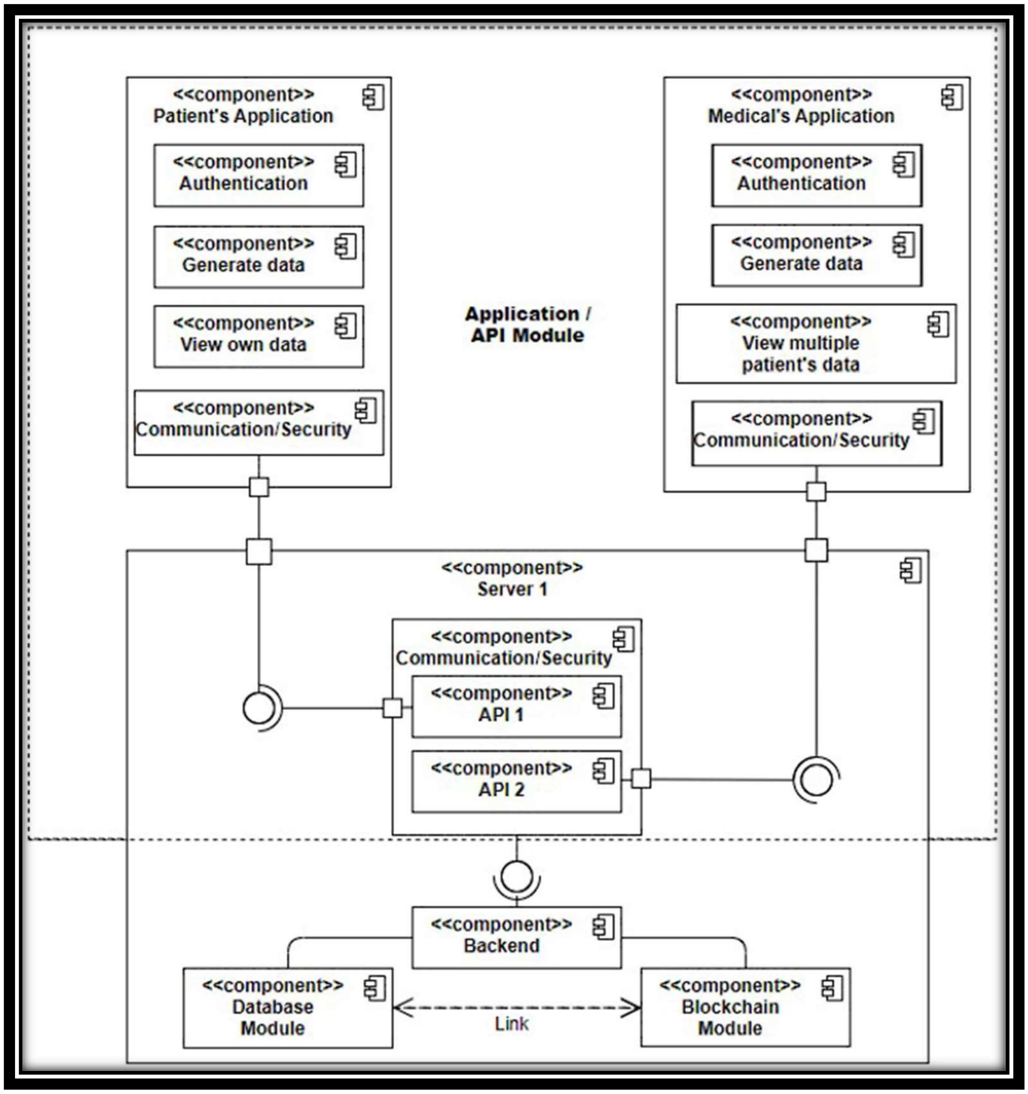


Figure 4.5: Component Diagram

CHAPTER 5

PROJECT PLAN

5.1 Project Estimate

5.1.1 Reconciled Estimates

Reconciled Estimates conciled estimates for the attendance management software project:

Development Time: Based on the complexity of integrating blockchain technology into the healthcare records management system and the expertise required in blockchain development, the development time for this project is estimated to be around 12 months.

Development Cost: Considering the specialized skills needed for blockchain development, as well as infrastructure costs and other expenses, the development cost is estimated to be around 150,000/.

Hardware Cost: The hardware required for implementing blockchain technology, such as servers for hosting blockchain nodes and secure storage devices, can vary depending on specific requirements. However, the estimated cost for the required hardware is around 30,000/-.

Software Cost: The cost of software licenses for blockchain platforms, development tools, and any necessary security software is estimated to be around 25,000/-

Testing and QA Cost: Given the critical importance of ensuring the security and integrity of healthcare records, a significant portion of the project budget will be allocated to testing and quality assurance. Based on the scope of the project, the testing and QA cost is estimated to be around 15,000/-.

Maintenance Cost: After the system is implemented, ongoing maintenance and support will be essential to ensure its continuous operation and security. The maintenance cost is estimated to be around 10,000/- per year. Overall, the reconciled estimates for the Blockchain Health Record Management System project are as follows:

Total Project Cost: 250,000/-
Development Time: 12 months
Hardware Cost: 30,000/-
Software Cost: 25,000/-
Testing and QA Cost: 15,000/-
Implementation Cost: 20,000/-
Maintenance Cost: 10,000/- per year

This project plan provides a comprehensive framework for managing the development and implementation of a Blockchain Health Record Management System, ensuring that all aspects of the project are carefully considered and addressed to achieve successful outcomes.

5.2 Risk Management

5.2.1 Risk Identification

The first step in risk management is to identify potential risks that may impact the project. The project team has identified the following potential risks:

Technical risks related to the implementation of health care records management technologies, such as compatibility issues, implementation chal- lenges, and potential security vulnerabilities. Security risks related to data breaches or unauthorized access, such as theft or loss of data, hacking at- tempts, and user errors. Resource risks related to the availability of skilled development and testing personnel, such as staff turnover, skill gaps, and budget constraints. Schedule risks related to delays in development or de- ployment due to unforeseen circumstances, such as unexpected technical is- sues, resource constraints, or changes in project scope.

5.2.2 Risk Analysis

Once potential risks have been identified, the project team will conduct a risk analysis to assess the likelihood and potential impact of each risk. This will involve assigning a risk score to each potential risk based on factors such as its likelihood, severity, and impact on the project timeline, budget, and functionality.

The project team will prioritize the risks based on their potential impact on the project and develop contingency plans to address the highest priority risks. The team will also conduct ongoing risk assessments throughout the project lifecycle to ensure that new risks are identified and addressed in a timely manner.

5.3 Project Schedule

5.3.1 Task Network

1. Gather project requirements
2. Design system architecture (Dependent on task 1)
3. Develop user interfaces (Dependent on task 2)
4. Implement smart contracts (Dependent on task 2)
5. Integrate IPFS for storing the data (Dependent on tasks 3 and 4)
6. Test and debug the system (Dependent on task 5)
7. Create user documentation (Dependent on task 6)
8. Deploy the system on the server (Dependent on task 7)
9. Conduct user acceptance testing (Dependent on task 8)
10. Address feedback and make necessary improvements (Dependent on task 9)
11. Finalize documentation (Dependent on task 10)
12. Project closure and handover

5.3.2 Timeline Chart

Sr No	Task	Labour Days/ Week
1	Topic selection	2 weeks
2	Feasibility study	1 week
3	Project Design	2 weeks
4	Plan System architecture	2 weeks
5	Detailed design specifications	2 weeks
6	Detailed study on research papers and referred work	2.5 weeks
7	Data collection and data preprocessing	3 weeks
8	Environmental setup	2 week
9	Implementation of smart contracts.	2 weeks
10	Develop UI modules and APIs	4 weeks
11	Integration of IPFS database	10 days
12	Perform testing and evaluation	2 weeks

CHAPTER 6

PROJECT IMPLEMENTATION

6.1 Overview of Project Modules

- Doctor Module – This module manages the frontend related to doctor panel.
- Patient Module – This module manages the frontend related to patient panel.
- Blockchain Module – This module handles the interaction between the doctor or patient with the underlying blockchain network.
- IPFS Module - This module handles the file upload and download functions.

6.2 Tools and Technologies Used

- Front-end: React.js, Metamask
- Blockchain: Ethereum
- Smart Contracts: Solidity
- Web3.js library for interacting with the blockchain
- IPFS (InterPlanetary File System) for secure document storage

6.3 Solidity and Smart Contract

Solidity is a programming language specifically designed for writing smart contracts on blockchain platforms, with Ethereum being the most prominent one. Smart contracts are self-executing contracts with the terms of the agreement directly written into code. Solidity was created to facilitate the development of such contracts, enabling developers to define rules and behaviors for decentralized applications (dApps) and automate transactions without the need for intermediaries.

A smart contract is a self-executing contract with the terms of the agreement directly written into code. These contracts run on a blockchain and automatically execute actions when predefined conditions are met.

Functions Defined in Smart Contract:

1. BookAppointment
2. GetAllAppointmetns
3. UploadDocument
4. GetAllDocuments
5. RegisterAsDoctor
6. RegisterAsPatient
7. GetAllDoctors
8. CheckIfDoctor
9. CheckIfPatient

6.4 Truffle suite

Truffle Suite is a development framework for Ethereum blockchain development. It provides a suite of tools that streamline the process of developing, testing, and deploying smart contracts and decentralized applications (dApps) on the Ethereum network. Truffle Suite consists of several components:

1. Truffle: Truffle is the core component of the suite. It is a development environment, testing framework, and asset pipeline for Ethereum. Truffle simplifies the process of writing, compiling, deploying, and managing smart contracts.
2. Ganache: Ganache is a personal Ethereum blockchain for development and testing purposes. It allows developers to create a local blockchain environment that mimics the behavior of the Ethereum mainnet or testnets. Ganache provides features such as instant mining, configurable gas settings, pre-funded accounts, and built-in contract debugging. It's an invaluable tool for testing smart contracts in a controlled environment without incurring real transaction costs.

6.5 IPFS Integration

IPFS stands for InterPlanetary File System. It’s a decentralized protocol and network designed to create a more resilient and distributed method of storing and sharing hypermedia in a peer-to-peer fashion.

When a patient uploads a document, this document gets stored on an IPFS system, which returns us a unique CID that is used to access this file. This CID is stored securely in the blockchain protected via encryption.

CHAPTER 7

SOFTWARE TESTING

7.1 Type of Testing

- Functional Testing: This type of testing ensures that the system functions as per the requirements and specifications provided. In attendance management system, functional testing can include testing of features such as attendance marking, reports generation, alerts and notifications, etc.
- Usability Testing: Usability testing helps to evaluate the ease of use of the system by the end users. In attendance management system, usability testing can include testing of the user interface, ease of navigation, user-friendliness of the system, etc.
- Performance Testing: Performance testing ensures that the system can handle expected load and work as expected under different scenarios. In attendance management system, performance testing can include testing of the system's response time, speed, reliability, scalability, etc.
- Security Testing: Security testing helps to evaluate the system's ability to prevent unauthorized access, maintain confidentiality, and prevent data breaches. In attendance management system, security testing can include testing of authentication and authorization, encryption of data, data storage security, etc.
- Integration Testing: Integration testing ensures that the different modules of the system work together seamlessly. In attendance management system, integration testing can include testing of integration of facial recognition, Bluetooth, QR code scanning, etc.
- Regression Testing: Regression testing ensures that the changes made to the system do not affect the existing functionality. In attendance management system, regression testing can include testing of attendance marking, report generation, etc. after adding new features or making changes.
- Acceptance Testing: Acceptance testing ensures that the system meets the user's requirements and expectations. In attendance management system, acceptance testing can include testing of the system's compliance with the institute's attendance policies and procedures

Test Case ID	Description	Input	Expected Output	Actual Output	Status
TC #001	Test doctor registration	Enter valid details	Takes the user to their dashboard	Takes the user to their dashboard	Pass
TC #002	Test patient registration	Enter valid details	Takes the user to their dashboard	Takes the user to their dashboard	Pass
TC #003	Verify patients can book and appointment with doctor	Select the doctor Enter time and date	Appointment booked message is displayed	Appointment booked message is displayed	Pass
TC #004	Verify document upload feature	Click upload document Enter name Select document	Document gets uploaded	Document gets uploaded	Pass
TC #005	Verify doctor can see appointments	Login to doctor Go to 'My Appointments' tab	All appointments are listed	All appointment are listed	Pass
TC #006	Verify doctor can see all documents of patients	Click on 'View Details' for any patient.	All documents are listed and can be viewed	All documents are listed and can be viewed	Pass

CHAPTER 8

RESULTS

8.1 Outcomes

The detailed explanation of key outcomes for the healthcare records management system project utilizing blockchain technology encompasses various aspects ranging from technical achievements to the impact on stakeholders and compliance with regulatory standards. Here's a breakdown of the key outcomes:

1. Enhanced Data Security: Implementation of blockchain technology ensures data immutability, tamper-resistance, and encryption, significantly enhancing the security of healthcare records. Patient data stored on the blockchain is protected from unauthorized access, mitigating the risks of data breaches and identity theft

2. Improved Data Integrity and Traceability: Blockchain's distributed ledger ensures the integrity of healthcare data by providing a transparent and auditable record of all transactions. Every interaction with patient records, including access, modification, and sharing, is recorded on the blockchain, enabling traceability and accountability.

3. Streamlined Interoperability:Integration with existing healthcare IT systems and adherence to industry standards such as HL7 and FHIR facilitate seamless interoperability between disparate healthcare systems.Blockchain-based data exchange protocols enable secure and standardized communication, promoting interoperability across healthcare providers and organizations.

4. Empowered Patients: Patients gain greater control over their healthcare data, with the ability to securely access and share their records with healthcare providers as needed. Smart contracts enable patients to specify access permissions and consent requirements, empowering them to manage their data privacy preferences.

5. Regulatory Compliance: The healthcare records management system adheres to regulatory standards such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation), ensuring compliance with data privacy and security regulations. Smart contracts enforce regulatory requirements for data access, consent management, and data sharing, reducing the risk of non-compliance and associated penalties.

8.2 Screen Shots

Figure 8.1: Doctor Login

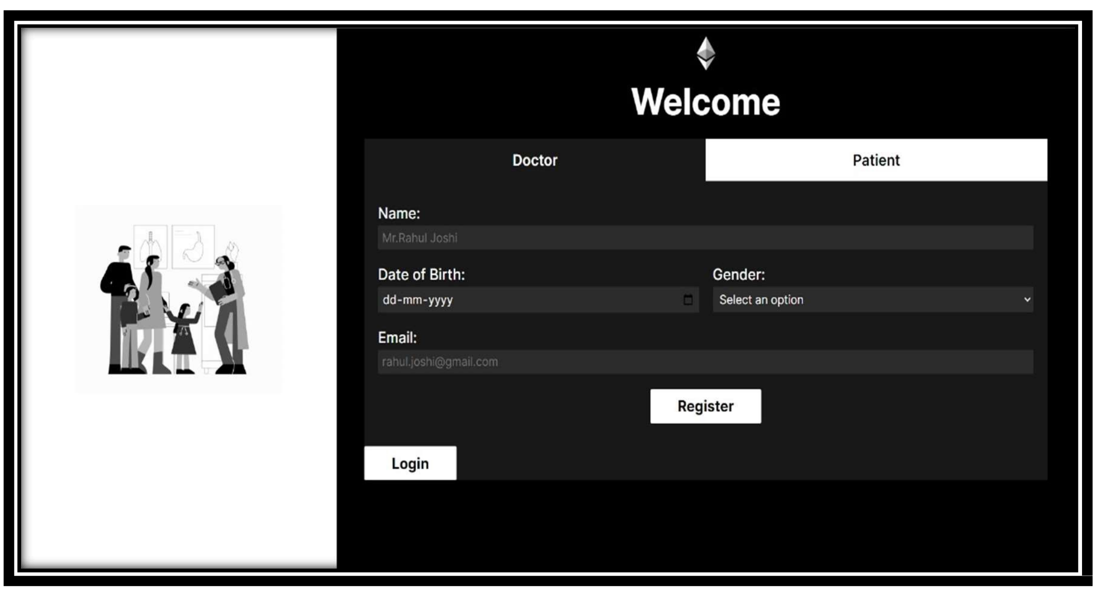


Figure 8.2: Patient Login

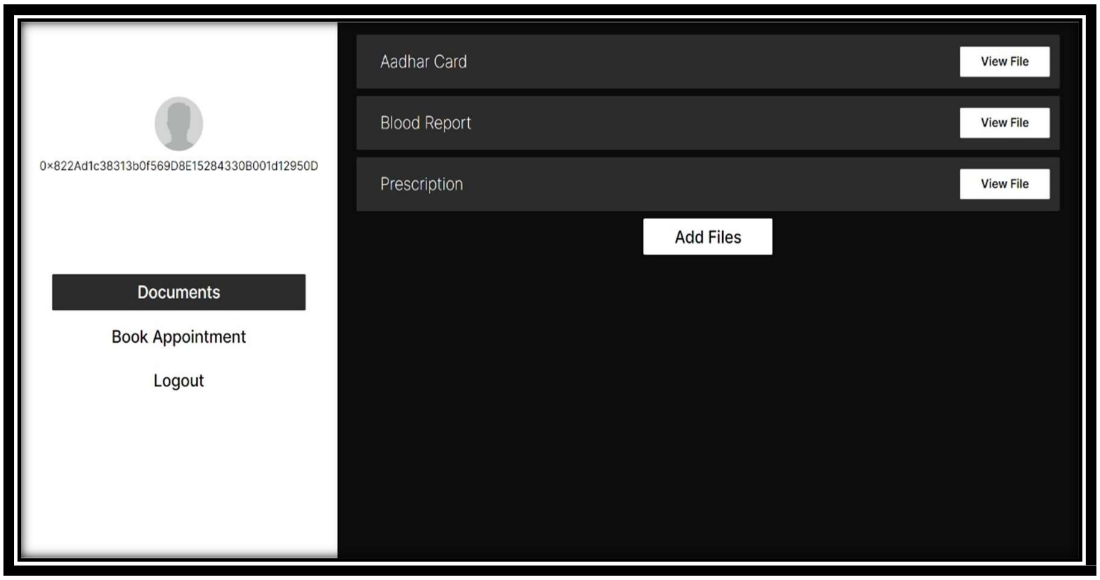


Figure 8.3: Patient Document Dashboard

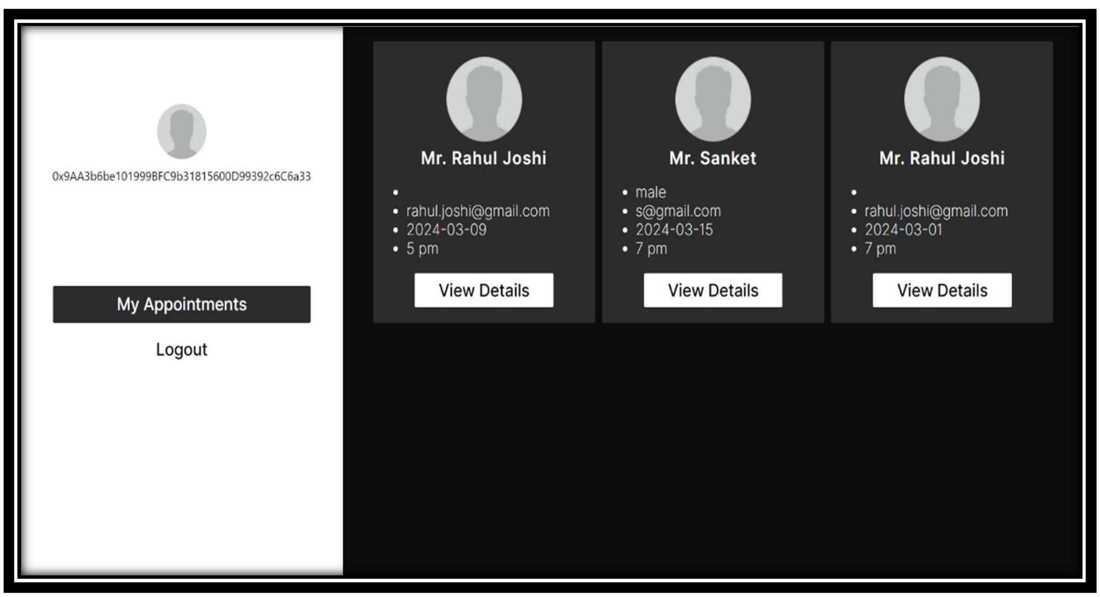


Figure 8.4: Doctor Dashboard

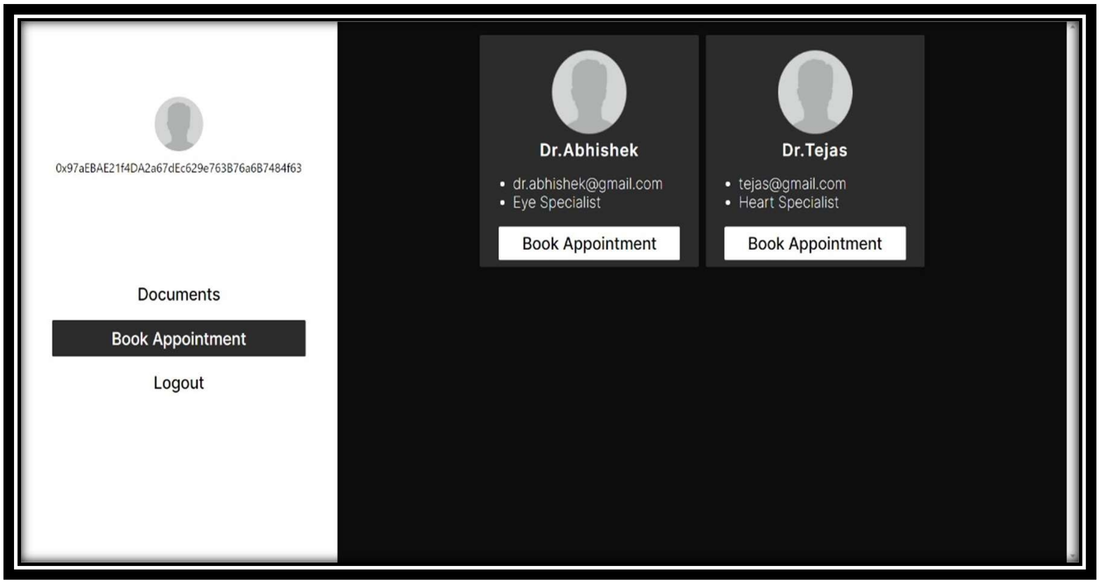


Figure 8.5: Patient Appoinment Dashboard

CHAPTER 9

CONCLUSIONS

9.1 Conclusions

In conclusion, the implementation of the blockchain-based healthcare records management system represents a significant milestone in addressing the complex challenges inherent in healthcare data management. Leveraging cutting-edge blockchain technology, alongside robust encryption, decentralized architecture, and smart contracts, the system offers a groundbreaking solution for enhancing data security, integrity, and interoperability in healthcare.

Throughout the project lifecycle, meticulous attention has been paid to critical factors including performance, safety, security, and compliance with regulatory standards such as HIPAA and GDPR. By employing a rigorous testing regime encompassing diverse scenarios and user interactions, the system's functionality and robustness have been thoroughly validated, ensuring reliability and usability.

Proactive risk management strategies have been integral to identifying and mitigating potential risks, safeguarding project execution and data integrity. Furthermore, the system's external interface requirements have been meticulously addressed through seamless integration with existing healthcare systems, utilization of appropriate programming languages, databases, and cloud services, fostering interoperability and communication. Effective project scheduling and team organization have facilitated smooth execution, with clear task assignments and regular progress tracking ensuring optimal communication and coordination among team members.

Looking ahead, the system's continuous evolution holds promise for further enhancements in areas such as interoperability with other systems, advanced analytics, mobile application enhancements, and scalability optimization, thereby reinforcing its role as a transformative solution in healthcare data management. In summary, the blockchain-based healthcare records management system delivers unparalleled benefits including heightened accuracy, enhanced security, improved data management, and operational efficiency, thus addressing the multifaceted challenges faced by healthcare institutions and paving the way for a more secure and interoperable healthcare ecosystem.

9.2 Future Work

In considering future work for the blockchain-based healthcare records management system, several key areas emerge for further enhancement and development:

1. Integration with Other Healthcare Systems: Expanding the interoperability of the system by integrating it with other existing healthcare systems, such as Electronic Medical Records (EMRs), Electronic Health Records (EHRs), and Health Information Exchanges (HIEs). This integration would enable seamless data exchange and interoperability, improving coordination and continuity of care across different healthcare providers and organizations.

2. Advanced Analytics and Reporting: Enhancing the system's analytics and reporting capabilities to provide deeper insights into healthcare data. Implementing advanced analytics algorithms to identify trends, patterns, and anomalies in patient records, enabling predictive analytics for disease management, resource allocation, and healthcare planning.

3. Mobile Application Enhancements: Continuously improving the mobile application interface for healthcare professionals and patients to enhance user experience and accessibility. Adding features such as real-time notifications for critical health events, medication reminders, appointment scheduling, and telehealth consultations to improve patient engagement and adherence to treatment plans.

4. Integration with Patient Portals and Telemedicine Platforms: Integrating the healthcare records management system with patient portals and telemedicine platforms to provide patients with secure access to their medical records, appointment scheduling, virtual consultations, and remote monitoring services. This integration would empower patients to take a more active role in managing their health and accessing healthcare services conveniently from their homes.

9.3 Applications

The application of the blockchain-based healthcare records management system aligns with the provided points as follows:

1. Streamlined Healthcare Data Management: The project offers a digital and automated solution for managing healthcare records, eliminating the need for manual paper-based systems or fragmented electronic health record (EHR) platforms. By leveraging blockchain technology, healthcare providers can securely access and update patient records in real-time, ensuring data integrity and transparency.

2. Enhanced Efficiency: Through the integration of blockchain, smart contracts, and cryptographic techniques, the system streamlines data management processes for healthcare professionals and administrators. Tasks such as patient record updates, access permissions, and data sharing are automated, saving time and reducing the risk of errors or discrepancies in healthcare records.

3. Real-time Data and Reporting: The blockchain-based system captures healthcare data in real-time, enabling healthcare providers to access up-to-date patient information for individual cases or population health management. This real-time data can be utilized for generating reports, monitoring health trends, and identifying patterns or issues that require attention.

4. Improved Security and Authentication: The combination of blockchain's decentralized architecture, encryption protocols, and smart contracts enhances security and authentication measures for healthcare data.

CHAPTER 10

APPENDIX

10.1 Appendix A

When considering the classification of the problem at hand, it's essential to differentiate between the complexity classification of decision problems and the broader task of privacy-preserving multi-object detection. Typically, complexity classes such as P, NP-Complete, or Hard are applied to decision problems, necessitating the framing of the problem as such for accurate classification. However, in the context of privacy-preserving multi-object detection using federated learning, modern algebra and mathematical models are not directly applicable for assessing complexity or feasibility. Instead, the focus shifts to complexity theory, algorithms, and performance evaluation techniques specific to machine learning and computer vision.

The feasibility assessment of privacy-preserving multi-object detection using federated learning demands a comprehensive analysis that spans various factors. These include privacy preservation mechanisms, object detection accuracy, dataset size, the number of objects, model architecture, algorithms, and communication overhead. Such an assessment integrates insights from machine learning, computer vision, and privacy preservation techniques, rather than relying solely on modern algebra or mathematical models. Thus, a holistic understanding of the problem's intricacies emerges, guiding the development and evaluation of viable solutions in the realms of machine learning, computer vision, and privacy preservation.

10.2 Appendix B

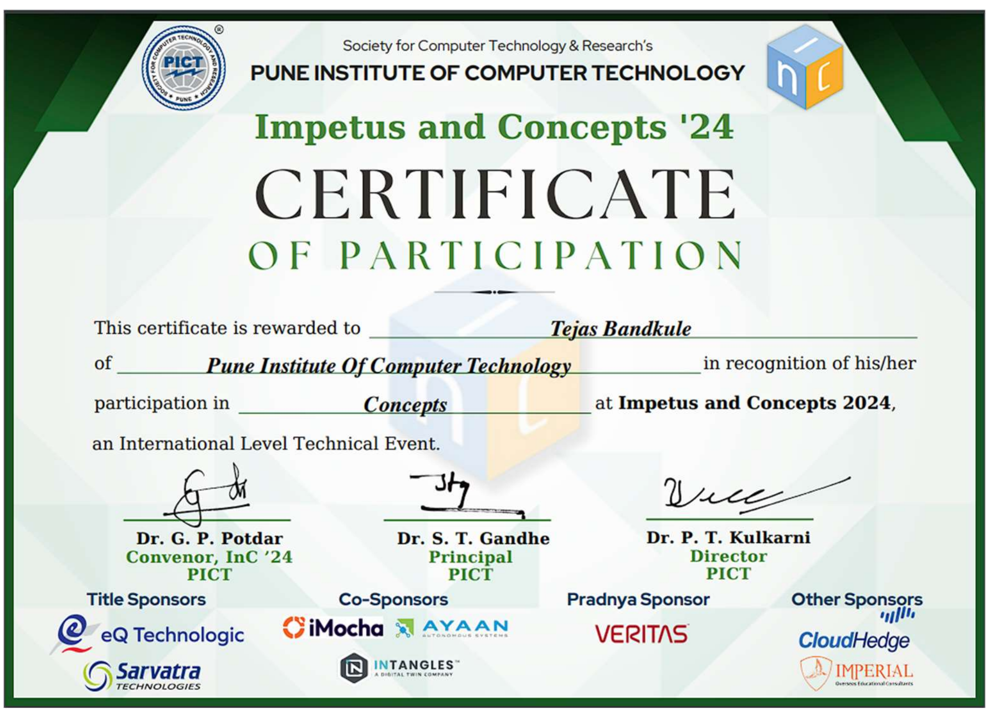
INC Certificates


Society for Computer Technology & Research's
PUNE INSTITUTE OF COMPUTER TECHNOLOGY
Impetus and Concepts '24
CERTIFICATE
OF PARTICIPATION

This certificate is rewarded to *Atharva Sandeep Deshmukh* of *Pune Institute Of Computer Technology* in recognition of his/her participation in *Concepts* at **Impetus and Concepts 2024**, an International Level Technical Event.

Dr. G. P. Potdar	Dr. S. T. Gandhe	Dr. P. T. Kulkarni
Convenor, InC '24	Principal	Director
PICT	PICT	PICT

Title Sponsors: eQ Technologic, Sarvatra Technologies
Co-Sponsors: iMocha, AYAAN, INTANGLES
Pradnya Sponsor: VERITAS
Other Sponsors: CloudHedge, IMPERIAL


Society for Computer Technology & Research's
PUNE INSTITUTE OF COMPUTER TECHNOLOGY
Impetus and Concepts '24
CERTIFICATE
OF PARTICIPATION

This certificate is rewarded to *Tejas Bandkule* of *Pune Institute Of Computer Technology* in recognition of his/her participation in *Concepts* at **Impetus and Concepts 2024**, an International Level Technical Event.

Dr. G. P. Potdar	Dr. S. T. Gandhe	Dr. P. T. Kulkarni
Convenor, InC '24	Principal	Director
PICT	PICT	PICT

Title Sponsors: eQ Technologic, Sarvatra Technologies
Co-Sponsors: iMocha, AYAAN, INTANGLES
Pradnya Sponsor: VERITAS
Other Sponsors: CloudHedge, IMPERIAL

10.3 Appendix C

Plagiarism Report of project report.

Document Information

Analyzed document	Nikhil-PS-II.pdf (D190741708)
Submitted	2024-04-24 05:17:00 UTC+02:00
Submitted by	Rajani Jadhav
Submitter email	rrjadhav@pict.edu
Similarity	1%
Analysis address	rrjadhav.pict@analysis.urkund.com

Sources included in the report

W	URL: https://www.chainalysis.com/blog/blockchain-security/ Fetched: 2023-10-21 01:15:35	1
W	URL: https://www.linkedin.com/pulse/blockchain-security-safeguarding-your-assets-debiprasad-bandopadhyay-es5ef Fetched: 2023-11-13 03:40:22	1
W	URL: https://www.researchgate.net/publication/336439409_Health_Record_Management_through_Blockchain_Technology Fetched: 2020-04-13 08:12:27	1
W	URL: https://www.researchgate.net/publication/357669751_Blockchain-Based_Electronic_Health_Records_Management_A_Comprehensive_Review_and_Future_Research_Direction Fetched: 2023-02-07 00:36:27	1

Entire Document

A PROJECT REPORT ON Healthcare Records Management System Using Blockchain SUBMITTED TO THE SAVITRIBAI PHULE UNIVERSITY, PUNE IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF ENGINEERING (Computer Engineering) SUBMITTED BY Atharva Walke Exam No: B190054217 Nikhil Awatade Exam No: B190054220 Tejas Bendkule Exam No: B190054227 Atharva Deshmukh Exam No: B190054261 DEPARTMENT OF COMPUTER ENGINEERING Pune Institute of Computer Technology Dhankawadi, Pune - 411043 SAVITRIBAI PHULE PUNE UNIVERSITY 2023-2024

CERTIFICATE This is to certify that the project report entitled Healthcare Records Management System Using Blockchain Submitted by Atharva Walke Exam No: B190054217 Nikhil Awatade Exam No: B190054220 Tejas Bendkule Exam No: B190054227 Atharva Deshmukh Exam No: B190054261 is a bonafide student of this institute and the work has been carried out by him/her under the supervision of Prof. R.R.Jadhav and it is approved for the partial fulfillment of the requirement of Savitribai Phule Pune Univer- sity, for the award of the degree of Bachelor of Engineering (Computer Engineering). Prof. R.R.Jadhav Dr. G.V. Kale Internal Guide Head Dept. of Computer Engg. Dept. of Computer Engg. Place:Pune Date: Dr. S.T. Gandhe Principal Pune Institute of Computer Technology

ACKNOWLEDGEMENT It gives us great pleasure in presenting the project report on 'Healthcare Records Management System Using Blockchain . We would like to take this opportunity to thank Prof. R.R.Jadhav giving me all the help and guidance we needed. We are really grateful to them for their kind support. Their valuable suggestions were very helpful. We are also grateful to Dr. G.V. Kale , Head of Computer Engineering Department, PICT for his indispensable support, suggestions. In the end our special thanks all faculty members for their whole hearted cooperation for completion of this report. We also thank our laboratory as- sistants for their valuable help in laboratory. Atharva Walke Nikhil Awatade Tejas Bendkule Atharva Deshmukh (B.E. Computer Engg.)

Figure 10.1: Plagiarism Report

CHAPTER 11

REFERENCES

[1] Beltramini, Elizabeth, " Blockchain Technology in Healthcare: A Review," 2019 International Journal of Medical Informatics, Volume 123, Pages 103–116, doi: 10.1016/j.ijmedinf.2018.12.009.

[2] Johnson, Emily, " Decentralized Electronic Health Records Management Using Blockchain Technology," 2020 IEEE Access, Volume 8, Pages 37788-37802, doi: 10.1109/ACCESS.2020.2973790.

[3] Brown, Sarah," A Review of Personal Health Record (PHR) Systems: Features, Benefits, and Challenges", Journal of Medical Systems, Volume 43, Issue 2, Article Number: 40, 2019 , DOI: 10.1007/s10916 -018-1150-8.

[4] Martinez, Maria, "Integrated Health Information Exchange Systems: A Systematic Review", Journal of Medical Internet Research, Volume 19, Issue 7, Article Number: e236 , DOI: 10.2196/jmir.7473.

[5] Garcia, Carlos ," Federated Health Information Systems: Challenges and Opportunities," 2019 Journal of Biomedical Informatics, Volume 89, Pages 135-145, doi: 10.1016/j.jbi.2018.12.002.

[6] Patel, Ravi," Clinical Data Warehousing Systems: Architecture, Implementation, and Challenges", Journal of Biomedical Informatics, Volume 89, Pages 135-145 , DOI: 10.1016/j.jbi.2018.12.002.