Medconnect - Patient Record Management System Using Blockchain Technology

SREEHARI K(23MX325)

23MX41 - MAJOR PROJECT

REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF COMPUTER APPLICATIONS

ANNA UNIVERSITY

APRIL - 2025

DEPARTMENT OF COMPUTER APPLICATIONS

PSG COLLEGE OF TECHNOLOGY

(Autonomous Institution)

COIMBATORE - 641 004

PSG COLLEGE OF TECHNOLOGY

(Autonomous Institution)

COIMBATORE - 641 004

Medconnect - Patient Record Management System Using Blockchain Technology

Bonafide record of work done by

SREEHARI K(23MX325)

23MX41 - MAJOR PROJECT

REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF COMPUTER APPLICATIONS

ANNA UNIVERSITY

APRIL - 2025

______________________ ______________________

Faculty Guide **Head of the Department**

Submitted for the Viva – Voce Examination held on ______________________

______________________ ______________________

Internal Examiner **External Examiner**

TABLE OF CONTENTS

ACKNOWLEDGEMENT

I express our sincere thanks and gratitude to **Dr. PRAKASAN K**, Principal, PSG College of Technology, for providing me with all the necessary facilities to carry out the project.

I extend our earnest gratitude to **Dr. CHITRA A**, Professor and Head, Department of Computer Applications, PSG College of Technology, for her support and encouragement to complete the project.

I am grateful to thank **Dr. MANAVALAN R**, Associate Professor, Program Coordinator, Department of Computer Applications, PSG College of Technology, for his support and guidance.

I express our sincere gratitude to our faculty guide **Dr. BHUVANESWARI A**, Assistant Professor (Sl. Gr.), Department of Computer Applications, PSG College of Technology, for her valuable suggestions, encouragement and guidance throughout the completion of the project.

I extend our heartfelt gratitude to our tutors, **Dr. SUBATHRA M**, Assistant Professor (Sl. Gr.), and **Dr. GEETHA N**, Assistant Professor (Sl. Gr.), Department of Computer Applications, PSG College of Technology, for their support throughout the course of this project.

I also express our gratitude to all the faculty members of the Department of Computer Applications, PSG College of Technology, and our friends for their encouragement and support.

SYNOPSIS

The healthcare sector faces significant challenges in securely managing and sharing patient health records. Traditional paper based and centralized digital systems are plagued by vulnerabilities, including data breaches, lack of transparency and limited interoperability across diverse platforms. These shortcomings impede efficient patient care and compromise the integrity of health record management.

This project proposes a blockchain based solution for Next Gen health record management offering a decentralized secure and transparent framework. By leveraging blockchain technology, the system ensures enhanced data integrity ,realtime interoperability and patient centric privacy controls.Patient gain ownership and control over their health records fostering trust and empowering them in their healthcare journey.The system also adheres to regulatory standards,balancing innovation with compliance.

The proposed solution will transform health record management by mitigating risks, streamlining data exchange across electronic medical record systems,and creating a robust patient first approach to health care data security and accessibility.

CHAPTER 1

INTRODUCTION

A manual-based patient record system is a traditional method of recording and managing patient health information using physical documents such as paper files, registers, and folders. Healthcare providers manually write patient details, medical history, diagnoses, and treatments, storing these records in filing cabinets or archives for future reference. This system has been widely used for decades but comes with challenges such as time-consuming record-keeping, difficulty in retrieval, and the risk of misplacement, loss, or damage. Sharing patient information between departments or healthcare facilities is also a slow and inefficient process, which can delay treatment and affect patient care. Despite these limitations, manual record systems are still used in small clinics, rural healthcare centers, and facilities with limited digital infrastructure. They do not require electricity, specialized software, or technical expertise, making them accessible and cost-effective. However, to maintain efficiency and data reliability, healthcare providers using manual systems must implement structured documentation methods, secure storage practices, and regular audits to prevent errors and ensure accurate patient records.

1.1. Electronic Patient Record System:

Electronic patient records (EPRs) offer significant advantages over manual-based record-keeping by addressing many of its limitations (see **Fig. 1.1**). One of the key benefits is improved efficiency and accessibility. Unlike manual records, which require time-consuming searching through physical files, EPRs allow instant retrieval of patient data with just a few clicks, reducing delays in diagnosis and treatment.

Another major advantage is data security and durability. Paper records are vulnerable to damage, loss, or misplacement, whereas electronic records are securely stored in databases with backup systems, minimizing the risk of losing important medical information. Additionally, accuracy and legibility are enhanced, as EPRs eliminate issues caused by illegible handwriting or missing information, which are common in manual systems.

Interoperability and data sharing are also improved with EPRs. In manual systems, sharing patient information between departments or healthcare providers is slow and inefficient, often requiring physical file transfers. In contrast, electronic records enable seamless and secure data exchange, ensuring continuity of care and reducing errors (**Fig 1.1**).

EPRs also support automation and decision support, helping healthcare providers with alerts, reminders, and real-time analytics to improve patient outcomes. Manual systems lack these capabilities, making it harder to track patient progress and prevent medical errors.

While manual record systems are still used in resource-limited settings, electronic patient records provide a more efficient, secure, and reliable solution, ultimately improving healthcare delivery and patient care.

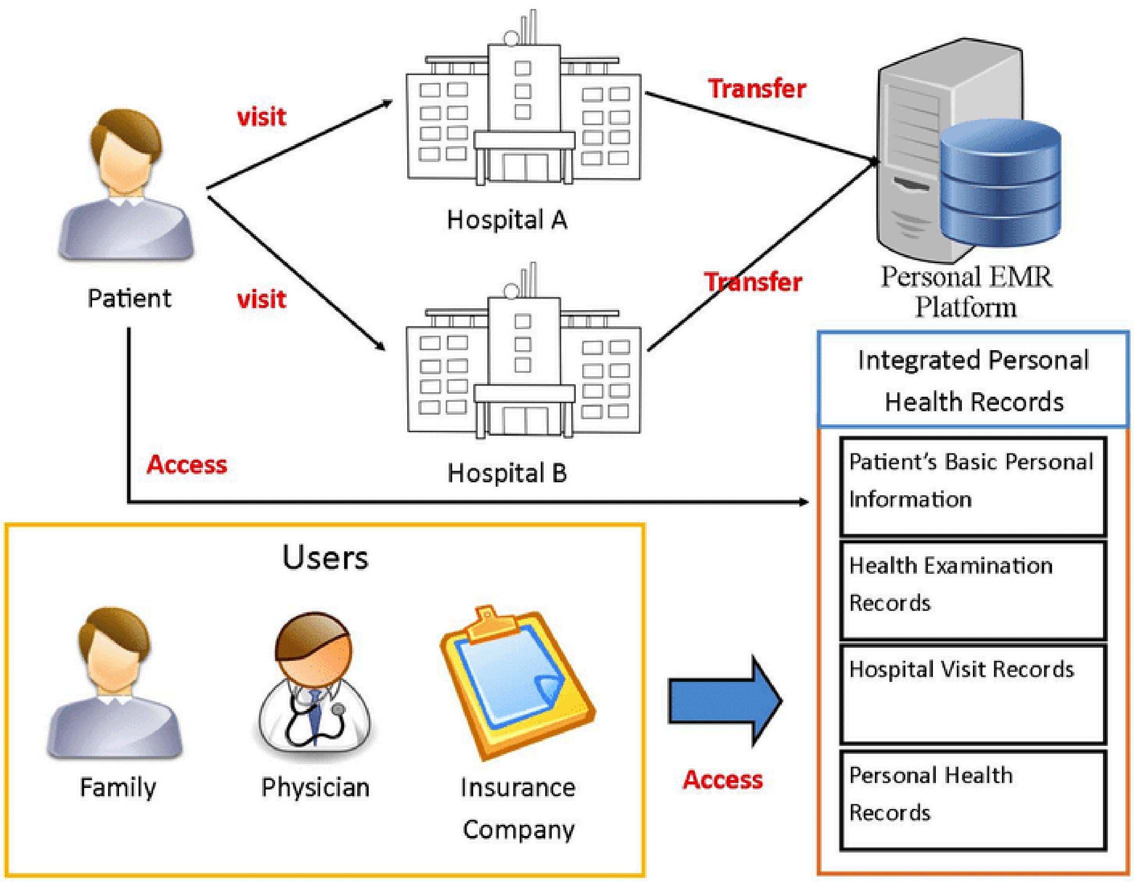

Fig.1.1 Electronic Patient Record System

1.2. The Challenge:

While electronic patient records (EPRs) offer many benefits, they also come with challenges (see **Fig 1.1**). One major concern is data security and privacy. Since records are stored digitally, they can be hacked, leaked, or accessed without permission. Strong security measures are needed to protect patient information.

Another issue is system compatibility. Different hospitals and clinics may use different EPR systems that do not easily share data with each other. This can cause delays in patient care and make it harder for doctors to access complete medical histories. Technical problems and system failures can also be a challenge. Unlike paper records, electronic records depend on computers and the internet. If the system crashes or there is a power outage, doctors may not be able to access important patient details when needed.

High costs are another drawback. Setting up and maintaining an EPR system requires expensive software, hardware, and regular updates. Smaller hospitals or clinics may struggle to afford these costs. Finally, usability and training can be an issue. Some healthcare workers may find EPR systems difficult to use or may resist switching from paper records. Proper training is needed to help them adjust and use the system effectively.

Despite these challenges, EPRs continue to improve healthcare by making patient information easier to access, reducing errors, and improving treatment quality. Overcoming these issues will help ensure a smoother transition to digital records.

1.3. Project Overview:

This project aims to develop a secure, efficient, and patient-centric electronic health record (EHR) management system that streamlines interactions between patients and doctors while ensuring data security, accessibility, and transparency. The system follows a structured workflow, as depicted in the process flowchart, enabling seamless management of patient records from appointment booking to report generation and secure data sharing.

The process begins with user authentication, where both patients and doctors must log in. If the login validation fails, the system provides an option to retry registration or exit. Once authenticated, users are categorized into two roles: Patients and Doctors, each having distinct functionalities.

Patients can book appointments, visit doctors, and record visit details, including payments and doctor-linking information. The system stores all visit data for future reference. Additionally, patients can view or create reports, check visit history, and track their doctor-patient relationship. Once consultation is completed, patients receive a diagnostic report, which can be securely shared with authorized users.

Doctors, on the other hand, have access to patient data, allowing them to add diagnoses, prescriptions, and medical updates. After submitting and updating medical records, doctors can include these details in the patient's report. The system ensures that medical records remain tamper-proof and accessible only to authorized individuals.

A key feature of the system is secure report sharing using access keys, where patients can grant or revoke access permissions. This mechanism enhances privacy control while maintaining interoperability between healthcare providers. If access is granted, the process continues, enabling authorized doctors to retrieve and update patient records. If access is revoked, the process ends, ensuring that only authorized users can interact with the data.

By integrating secure authentication, structured data management, and controlled access, this project eliminates inefficiencies in traditional patient record systems. It enhances data security, streamlines patient-doctor interactions, and ensures real-time accessibility, making healthcare management more efficient and transparent.

The shift from manual patient records to electronic patient record (EPR) systems has improved healthcare efficiency but introduced challenges like security risks, interoperability issues, and centralized data vulnerabilities. While EPR systems provide faster access and seamless sharing, they still face risks of data breaches and unauthorized access. To overcome these challenges, this project proposes a blockchain-based EHR system that ensures data security, decentralization, and patient control. By leveraging blockchain's immutable ledger and smart contracts, the system enables secure, real-time, and permissioned data sharing while maintaining patient privacy. This approach enhances trust, efficiency, and regulatory compliance, offering a secure and transparent future for healthcare data management.

This chapter provided an introduction to patient record management, covering manual record systems, electronic patient records (EPR), challenges in EPR, and the proposed blockchain-based solution. It highlighted the evolution of healthcare data management and the need for a secure, decentralized system to overcome existing limitations. The next chapter, System Study, will explore the detailed requirements, existing system analysis, and the feasibility of the proposed solution, laying the foundation for its implementation.

CHAPTER 2

SYSTEM STUDY

2.1. Existing System:

Several blockchain-based healthcare applications have emerged to address issues in traditional electronic patient record (EPR) systems. These solutions focus on security, interoperability, and patient control over medical data. However, despite their advantages, they still face certain limitations that our proposed system aims to overcome.

ess.

1. MedRec

Developed by: MIT Media Lab

Features:

- Uses blockchain to manage electronic medical records securely.
- Enables patients to control access to their records.
- Provides an audit trail for data access and modifications.

Limitations:

- Limited adoption due to complexity in integrating with existing hospital databases.
- Lacks real-time data sharing and interoperability with multiple healthcare providers.

2. Medicalchain

Developed by: Medicalchain Ltd.

Features:

- Enables secure access to medical records using blockchain.
- Patients control who can view and share their data.
- Supports telemedicine consultations using stored records.

Limitations:

- Still relies on a centralized component for some functions.
- Limited integration with insurance companies and external healthcare systems.

3. BurstIQ

Developed by: BurstIQ, Inc.

Features:

- Focuses on health data exchange using blockchain and AI.
- Ensures HIPAA-compliant secure data sharing.
- Enables data monetization where patients can sell their medical data for research.

Limitations:

- The data monetization model raises privacy concerns for some users.
- High computational cost due to AI and blockchain integration.

4. Dentacoin

Developed by: Dentacoin Foundation

Features:

- A blockchain-based dental healthcare platform.
- Uses cryptocurrency (Dentacoin) for transactions.
- Facilitates trusted dentist-patient interactions and record management.

Limitations:

- Limited real-world adoption outside dental care.
- Dependence on cryptocurrency makes it less practical for general healthcare.

2.2. Blockchain Architecture

Blockchain architecture is a decentralized system that securely records transactions in a distributed ledger, ensuring transparency, immutability, and security. Unlike traditional centralized databases, blockchain operates without a central authority, relying on cryptographic techniques and consensus mechanisms to validate and store transactions. This architecture is widely used in industries like healthcare, finance, and supply chain management due to its ability to prevent data tampering and unauthorized acc

A **block** is the fundamental unit of a blockchain. Each block contains a set of transactions, a timestamp, a cryptographic hash of the previous block, and a unique hash of its own. These cryptographic links create a secure and unchangeable chain of blocks. The block structure ensures that once data is recorded, it cannot be altered without modifying all subsequent blocks, which requires network-wide consensus. This feature makes blockchain ideal for applications requiring high data integrity, such as healthcare and financial systems.

A **blockchain** is a chain of blocks linked together through cryptographic hashes, forming a distributed and tamper-proof ledger. Since multiple copies of the blockchain exist across various network nodes, any attempt to alter data would require modifying the majority of these copies simultaneously, which is practically impossible. The decentralized nature of blockchain eliminates single points of failure, reducing risks associated with cyberattacks and unauthorized modifications. Blockchain ensures data consistency across all participants, enabling secure and verifiable transactions.

The **ledger** in blockchain is a distributed database that records all transactions across multiple nodes in a network. Unlike traditional ledgers maintained by centralized institutions, blockchain ledgers are shared and updated through consensus mechanisms, ensuring transparency and accuracy. Each transaction added to the ledger is cryptographically secured, preventing unauthorized modifications. This immutable and decentralized ledger is particularly useful in healthcare, where patient records must be securely stored, accurately updated, and accessed only by authorized entities.

Ganache is a personal Ethereum blockchain used for testing and development. It allows developers to simulate a blockchain environment without deploying smart contracts on a live network. Ganache provides test accounts with pre-allocated Ethereum, enabling developers to test transactions and interactions with smart contracts in a cost-free and controlled setting. The tool offers both a command-line interface and a graphical user interface, making it easier to monitor transactions, debug smart contracts, and analyze blockchain performance before deploying them on an actual network.

Truffle is a development framework designed to simplify the creation, compilation, and deployment of smart contracts. It provides built-in tools for testing and debugging, ensuring that smart contracts function as intended before they are launched on a blockchain. Truffle supports automated testing using JavaScript and Solidity, allowing developers to write test cases that verify the behavior of their contracts. In blockchain-based healthcare applications, Truffle helps in efficiently managing smart contracts that regulate data access, record updates, and permission-based sharing of medical records.

Ethereum is a blockchain platform that enables the development of decentralized applications (DApps) using smart contracts. Unlike Bitcoin, which primarily functions as a digital currency, Ethereum allows developers to create programmable contracts that automatically execute based on predefined conditions. Smart contracts deployed on Ethereum facilitate secure and trustless transactions, making it an ideal platform for applications requiring high data security, such as electronic health records (EHRs) and financial transactions. Ethereum's transition to Proof of Stake (PoS) enhances its efficiency, reducing energy consumption while maintaining security and scalability.

Solidity is a high-level programming language specifically designed for writing **smart contracts** on blockchain platforms like **Ethereum**. It is a statically-typed language similar to JavaScript, Python, and C++, making it accessible for developers while providing robust security for decentralized applications (**DApps**). Solidity is primarily used to create self-executing smart contracts, which **automate transactions, enforce agreements, and eliminate intermediaries** in blockchain-based systems.

A **transaction** in blockchain refers to the exchange of digital assets or execution of smart contract functions recorded in the distributed ledger. Transactions follow a structured process: they are initiated by a user, validated by network nodes through consensus mechanisms, and permanently stored in a block. Each transaction is digitally signed using cryptographic keys, ensuring authenticity and security. In a healthcare blockchain system, transactions include patient record updates, doctor approvals, and secure sharing of medical data. Since these transactions are recorded immutably, they enhance trust and prevent unauthorized modifications.

Blockchain architecture, with its decentralized ledger, cryptographic security, and automated smart contracts, provides a **secure, transparent, and tamper-proof** solution for various industries. Tools like **Ganache and Truffle** simplify blockchain development, ensuring efficient contract deployment and testing. By leveraging Ethereum's capabilities, blockchain enables **secure transactions and decentralized applications**, making it a revolutionary technology for data management, especially in healthcare and finance.

2.3. Proposed System:

To address the challenges of traditional EPR systems, this project proposes a blockchain-based electronic health record (EHR) system that ensures data security, decentralization, and patient control. The system integrates blockchain technology, smart contracts, and role-based access control to enhance healthcare data management.

Key Features of the Proposed System

1. **Decentralized Health Record Management:** Unlike centralized EPR systems, the proposed system stores medical records on a blockchain network, ensuring security, transparency, and tamper-proof data storage.
2. **Patient-Centric Data Control:** Patients have full ownership of their health records and can grant or revoke access to doctors, hospitals, and insurers through a secure permissioned access system.
3. **Smart Contracts for Automated Processes:** Smart contracts handle record updates, access permissions, and transactions without third-party involvement, reducing processing time and ensuring accuracy.
4. **Secure and Transparent Data Sharing:** Healthcare providers can securely access and update patient records without the risk of unauthorized modifications. Every transaction is logged, ensuring full transparency while protecting patient privacy.
5. **Interoperability Across Healthcare Providers**: The system ensures seamless data exchange between hospitals, clinics, and insurance companies, eliminating compatibility issues in traditional EPR systems.
6. **Enhanced Security Through Encryption and Consensus Mechanisms:** Patient data is encrypted and distributed across multiple nodes, preventing data breaches. Blockchain consensus mechanisms ensure that only verified transactions are recorded, preventing unauthorized alterations.
7. **Auditability and Fraud Prevention:** Every data transaction is recorded in an immutable ledger, allowing audits and reducing the risk of medical fraud or record manipulation.

How the Proposed System Works

1. **Patient Registration & Authentication:** Users (patients, doctors, and healthcare providers) must authenticate via secure login credentials to access the system.
2. **Managing Health Records:** Patients can upload, update, or view their records. Doctors can add diagnoses and prescriptions, ensuring real-time updates.
3. **Permissioned Data Access:** Patients grant access to doctors or hospitals using access keys, allowing temporary or permanent permissions. If permission is revoked, access is immediately restricted.
4. **Blockchain-Based Record Storage:** Medical records are stored in blocks, with each block linked to the previous one, ensuring tamper-proof storage.
5. **Real-Time Data Sharing and Validation:** Hospitals and healthcare providers can access updated patient records in real-time, improving treatment efficiency. Data modifications require network consensus, ensuring accuracy.

Advantages of the Proposed System

- **Eliminates Single Points of Failure** – Unlike centralized EPR systems, blockchain ensures that data loss or cyberattacks do not compromise records.
- **Enhances Patient Privacy and Control** – Patients decide who can access their records and for how long.
- **Improves Healthcare Efficiency** – Doctors can access real-time medical histories, reducing diagnosis errors.
- **Prevents Unauthorized Data Alteration** – Smart contracts regulate modifications, ensuring records remain accurate and trustworthy.

The proposed blockchain-based healthcare system provides a secure, patient-centric, and interoperable solution that overcomes the limitations of traditional EPR systems. By ensuring data security, transparency, and efficient record management, this system enhances trust and efficiency in modern healthcare services.

2.4. Functional Requirements

The functional requirements define the specific features and operations of the system.

- **User Authentication & Role Management**:
  - Patients and doctors must register and log in securely.
  - Role-based access control ensures only authorized users can view or modify data.
- **Patient Data Management**:
  - Patients can store, view, and manage their health records.
  - Patients can provide or revoke access to their medical data.
- **Doctor Consultation & Report Generation**:
  - Doctors can access patient records with granted permission.
  - Doctors can generate consultation reports and update medical records.
- **Appointment Booking**:
  - Patients can book appointments based on doctor specialization.
  - Doctors can view and manage scheduled appointments.
- **Blockchain Integration & Smart Contracts**:
  - Patient records are securely stored on the **Ethereum private blockchain**.
  - **Smart contracts** manage data access permissions and transactions.
- **Transaction Handling via Web3**:
  - Blockchain transactions ensure data integrity and prevent unauthorized changes.
  - Patients and doctors can sign transactions securely using **MetaMask**.
- **Data Privacy & Security**:
  - Records are encrypted and stored in an immutable ledger.
  - Only authorized users can decrypt and access medical records.

2.5. Non-Functional Requirements

The non-functional requirements define the overall system behavior and quality attributes.

- **Security & Data Integrity**
    - Blockchain ensures tamper-proof storage of medical records.
    - Smart contracts enforce strict access control and prevent data breaches.
- **Performance & Scalability**:
    - The system must handle multiple concurrent users efficiently.
    - Optimized queries and blockchain transactions ensure fast response times.
- **Reliability & Availability**:
    - The system should be highly available with minimal downtime.
    - **Backup mechanisms** ensure records are never lost.
- **User Experience & Accessibility**:
    - The UI should be intuitive and easy to navigate.
    - The system should be accessible via web browsers on multiple devices.
- **Regulatory Compliance**:
    - The system should comply with healthcare regulations (e.g., HIPAA, GDPR).
    - Patient consent and data-sharing policies must align with legal standards.
- **Maintainability & Modularity**:
    - The system should be easy to update and expand with new features.
    - Modular design ensures smooth integration of additional healthcare services.

These functional and non-functional requirements ensure the system is secure, efficient, user-friendly, and scalable, addressing the limitations of traditional EHR systems while leveraging blockchain for enhanced privacy, security, and decentralization.

In this chapter, we explored the fundamentals of blockchain architecture, including blocks, the distributed ledger, transactions, and essential development tools like Ganache and Truffle. We also discussed how Ethereum facilitates secure and transparent data management through smart contracts. This architecture provides a decentralized and immutable solution to overcome the challenges faced by traditional and electronic patient record systems, ensuring data integrity, security, and patient control.

The next chapter will focus on **System Design**, detailing the structural and functional aspects of the proposed blockchain-based healthcare system, including its components, workflows, and implementation strategies.

CHAPTER 2

SYSTEM DESIGN

3.1. System Architecture:

The system architecture, as illustrated in **Fig. 3.1**, outlines the flow of patient and doctor interactions within the blockchain-based healthcare management system. The architecture ensures secure registration, consultation, diagnosis, report generation, and controlled access to medical records using blockchain technology.

The process begins with patient registration, where essential details such as medical history, allergies, medications, and symptoms are recorded. Simultaneously, doctors undergo a registration process to validate their credentials. Upon registration, patients can consult a doctor regarding their health conditions.

During the consultation phase, doctors assess the patient's illness, allergies, medications, and symptoms. Based on their observations, they proceed with a diagnosis and generate a medical report. This report is securely stored on the blockchain and linked with an access key, ensuring that only authorized individuals, such as the patient and designated healthcare providers, can retrieve the data.

The access key mechanism guarantees patient privacy and data security by allowing patients to grant or revoke access to their health records. Additionally, the system includes a payment module, which facilitates transactions for consultations and services. The blockchain ensures transparency, immutability, and security throughout the entire process.

This architecture leverages smart contracts to automate report generation and access management, eliminating intermediaries and enhancing efficiency. By integrating blockchain, the system overcomes limitations of traditional patient record management, providing a decentralized, secure, and transparent healthcare solution.

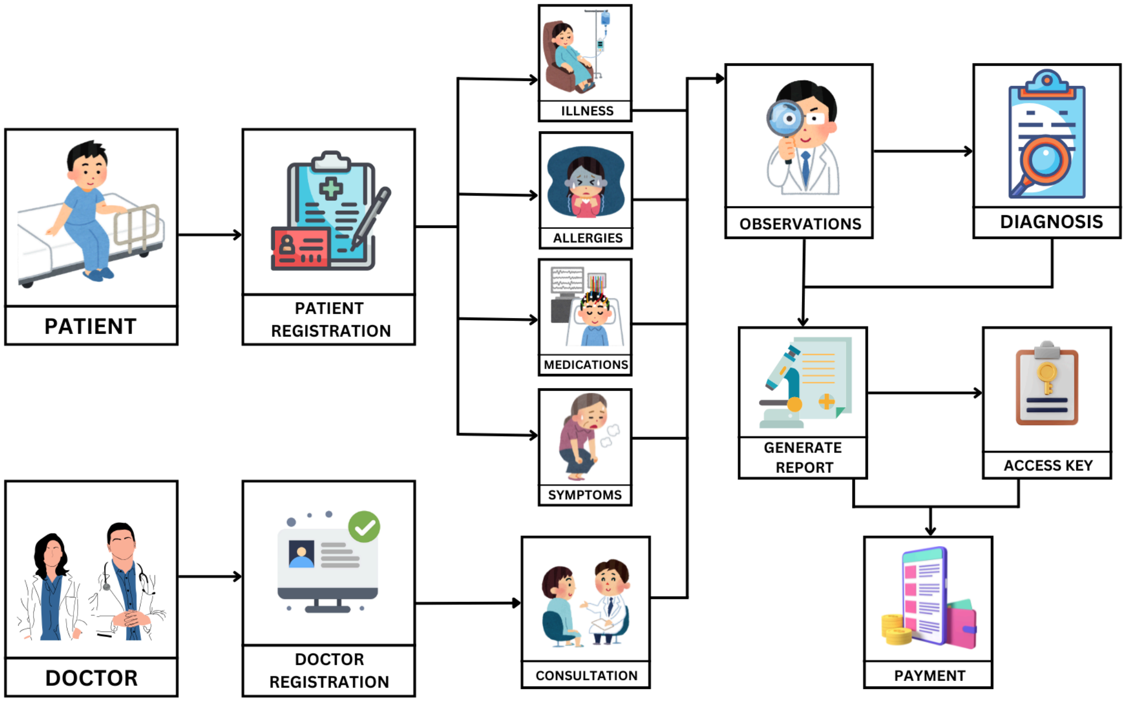

Fig 3.1. System Architecture

3.1. System Flow:

The system flows, as illustrated in **Fig. 3.1**, begins with patient and doctor registration, ensuring secure authentication and role-based access. Patients input their medical history, allergies, medications, and symptoms, which are securely stored on the blockchain. Doctors can access these records only with explicit patient permission, maintaining privacy and data security. During consultations, doctors record observations, diagnoses, and prescriptions, which are stored immutably using smart contracts. After diagnosis, a medical report is generated, and patients receive an access key to control data sharing. The system also integrates secure blockchain-based payments, where smart contracts automate transactions, ensuring transparency and fraud prevention. This decentralized approach enhances data security, interoperability, and patient ownership over health records, eliminating risks associated with centralized electronic health record (EHR) systems.

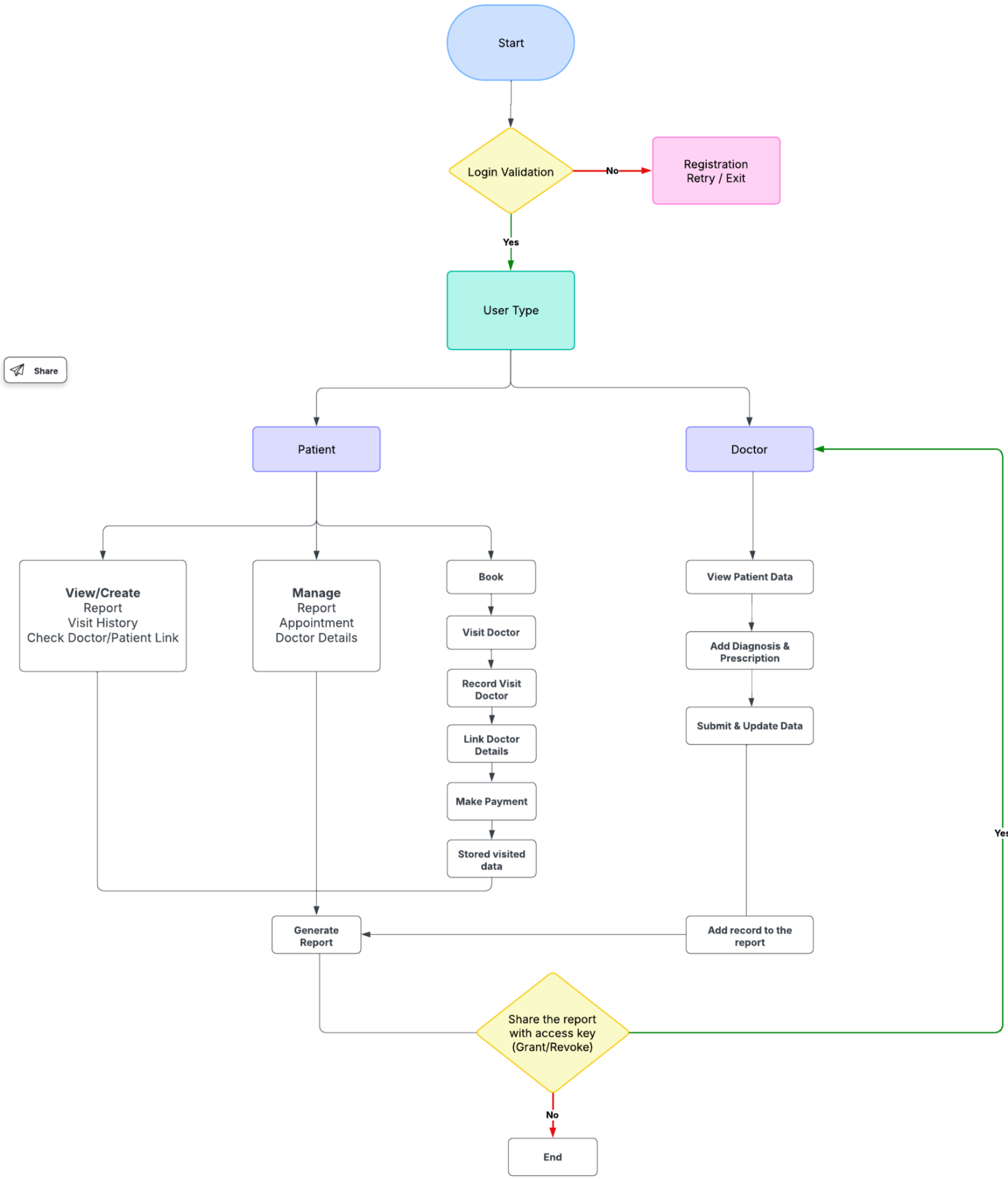

Fig. 3.1. System Flow

1. Patient Registration

The system begins with the patient registration process, where users input their personal and medical details, including illness history, allergies, medications, and symptoms. This data is securely recorded and linked to a unique blockchain identity, ensuring immutability and security. Unlike traditional systems where patient data is stored in centralized databases prone to breaches, the blockchain-based approach prevents unauthorized modifications.

2. Doctor Registration

Doctors must register in the system, where their credentials and qualifications are verified. This step ensures that only authorized and certified healthcare professionals can access and manage patient health data. The blockchain ledger maintains a transparent, tamper-proof record of registered doctors, reducing risks of fraudulent activities.

3. Patient Consultation Process

Once registered, patients can schedule appointments with doctors. During consultation, doctors access patient details such as previous health conditions, symptoms, allergies, and medications to diagnose the illness effectively. The blockchain ensures real-time, permissioned access to these records, allowing seamless and interoperable healthcare services.

4. Diagnosis & Report Generation

Based on the doctor's observations and evaluation, a diagnostic report is generated. This report contains detailed information about the patient's condition, test results, and prescribed medications. The report is stored securely on the blockchain network, ensuring it cannot be altered or deleted without authorization.

To maintain patient confidentiality, the report is encrypted and linked to an access key, which allows only authorized users (such as the patient, selected doctors, or insurance providers) to view it.

5. Secure Report Access & Sharing

A key feature of this system is controlled access to medical records. The patient holds full ownership of their health data and can grant or revoke access to specific individuals. If a doctor or insurance company requires access, the patient generates an access key to share the report securely. This method ensures that medical data remains private and accessible only to authorized personnel. The use of smart contracts automates the process of granting and revoking permissions, eliminating the need for third-party intermediaries and reducing the risk of unauthorized access.

6. Payment & Billing

After consultation and diagnosis, the system facilitates secure payment processing for medical services. The blockchain maintains a transparent, immutable record of transactions, ensuring that payments are securely processed. This enhances trust and accountability in financial transactions within the healthcare ecosystem.

By leveraging blockchain, smart contracts, and cryptographic security, this system overcomes the limitations of traditional electronic medical record systems and provides a secure, transparent, and efficient approach to healthcare management.

3.3. EHR System:

An Electronic Health Record (EHR) system is a digital version of a patient's medical history, designed to store, manage, and share healthcare information efficiently. Unlike traditional paper-based records, which are prone to errors, inefficiencies, and security risks, EHR systems provide a centralized, structured, and real-time approach to handling patient data. These systems are used by hospitals, clinics, and healthcare providers to ensure better patient care, streamlined workflows, and enhanced collaboration among medical professionals.

Key Features of EHR Systems

EHR systems typically include patient demographics, medical history, medications, lab results, radiology reports, treatment plans, and billing information. They allow real-time access to patient data, reducing the chances of misdiagnoses and enabling better decision-making. Additionally, EHRs improve coordination among healthcare providers by enabling secure information exchange, ensuring that doctors, specialists, and hospitals have access to accurate patient records.

Advantages of EHR Systems

One of the most significant advantages of EHRs is their ability to reduce medical errors. Automated alerts for drug interactions, allergies, and incorrect dosages enhance patient safety. Moreover, EHRs eliminate redundant tests and procedures, as all historical medical data is available to healthcare providers instantly. Remote access allows doctors to review and update patient records from anywhere, making telemedicine and emergency treatments more effective. EHRs also enhance patient engagement, as patients can access their records, lab results, and prescriptions through patient portals.

Challenges in EHR Systems

Despite their benefits, EHR systems also present challenges. Data security and privacy concerns are primary issues, as centralized digital systems are vulnerable to cyberattacks and unauthorized access. Additionally, interoperability issues arise when different healthcare providers use incompatible EHR systems, making it difficult to exchange patient information. The high cost of implementation and maintenance is another drawback, particularly for small healthcare providers.

Overcoming Limitations with Blockchain-Based EHR

To address these challenges, blockchain technology is being explored for decentralized, secure, and interoperable EHR systems. By leveraging blockchain's immutable ledger and smart contracts, patient records can be stored transparently and securely, reducing the risks of data breaches and unauthorized modifications. Blockchain also allows patients to have full control over their records, granting access only to authorized personnel, thereby ensuring privacy and security while maintaining seamless data exchange.

3.4. Project Modules:

The proposed blockchain-based healthcare system is designed with multiple modules to ensure secure, transparent, and efficient management of electronic health records (EHRs). The system consists of distinct patient and doctor roles, enabling seamless interaction while ensuring data security through blockchain technology. Below are the primary modules:

3.4.1. User Authentication Module

This module handles **login and registration** for both **patients and doctors**.

- **Patient Login & Registration**: Patients register by providing personal details and receive unique credentials. Upon logging in, they can manage their medical records, book appointments, and access consultation reports.
- **Doctor Login & Registration**: Doctors register with their medical credentials and are assigned a verified account. They can view patient data, add diagnoses, and generate medical reports.
- **Access Control**: Ensures role-based access where only authorized users can view and modify specific data. Blockchain stores access permissions to prevent unauthorized data breaches.

3.4.2. Patient Management Module

- Patients can book appointments with doctors based on their specialization.
- They can provide symptom details, medical history, allergies, and medications, which doctors can later review.
- Patients can access past medical reports and check their treatment progress.
- The system ensures that patients have full control over their medical records, allowing them to grant or revoke access to doctors.

3.4.3. Doctor Consultation Module

- Doctors can view patient details, medical history, and previous consultations upon receiving access.
- During consultation, they record observations, prescribe medications, and diagnose conditions.
- Doctors can update treatment plans and prescriptions in the blockchain, ensuring an immutable and tamper-proof record.

3.4.4. Report Generation Module

- After consultation, the system allows report generation based on the doctor's observations and diagnosis.
- The report includes symptoms, medications, test results, and recommended treatments.
- Reports are securely stored on the blockchain, ensuring data integrity and preventing unauthorized modifications.
- Patients receive an access key to their report, allowing them to share it with other healthcare providers when needed.

3.4.5. Access Control and Data Sharing Module

- Patients can grant or revoke access to doctors using smart contract-based permission management.
- Data sharing is done in a secure and transparent manner, ensuring privacy and compliance with healthcare regulations.
- Blockchain encryption and cryptographic keys ensure that only authorized users can decrypt and access medical records.

3.4.6. Payment Module

- Patients make secure payments for consultations and medical services through blockchain-based transactions.
- The system ensures transparent billing without hidden charges.
- Payment history is recorded on the blockchain, ensuring tamper-proof financial transactions.

3.4.7. Blockchain and Smart Contract Integration Module

- Ganache is used as a local Ethereum blockchain for deploying and testing smart contracts.
- Truffle helps in developing, testing, and deploying smart contracts that manage patient records and access control.
- Smart contracts automate data access permissions, ensuring a decentralized and trustless system.

3.5. Technology Used:

Our blockchain-based healthcare application is built using a modern, secure, and scalable technology stack to ensure data security, decentralization, and seamless access to medical records. The platform integrates blockchain, smart contracts, Flask, and Web3 to provide a secure, transparent, and efficient health record management system.

Ethereum Private Blockchain – Secure & Decentralized Health Records

- Stores patient records securely with no central authority.
- Prevents unauthorized access and data tampering.
- Ensures transparent and immutable medical transactions.

Smart Contracts (Solidity) – Automated Access Control

- Defines who can access or update medical records.
- Ensures tamper-proof logs and data integrity.
- Automates patient consent and data sharing.

Web3.py – Connecting Blockchain & Backend

- Allows Flask to interact with Ethereum blockchain.
- Handles secure transactions and data retrieval.
- Ensures real-time updates and smooth blockchain integration.

Flask – Secure Backend API

- Manages user authentication and role-based access.
- Provides RESTful APIs for patient and doctor interactions.
- Integrates with Web3.py to handle blockchain transactions.

Ganache & Truffle – Blockchain Development & Testing

- Ganache: Local Ethereum blockchain for testing.
- Truffle: Tool for developing and deploying smart contracts.

MetaMask – Secure User Authentication

- Allows patients and doctors to log in securely.
- Enables safe signing of blockchain transactions.

3.6. System Specification

The hardware & software environments utilized for the web application are described below:

Hardware Requirements

The minimal hardware requirements for the project are listed below:

- **Processor**: Intel Core i5 or higher
- **RAM**: 8GB or more
- **Storage**: At least 256GB SSD (512GB recommended)
- **GPU**: Integrated GPU (Dedicated GPU recommended for high-performance processing)
- **Network**: Stable broadband internet connection
- **Operating System**: Windows 10 or higher, macOS, or Linux

Software Requirements

The minimal software requirements for the project are listed below:

- **Blockchain Platform**: Ethereum Private Blockchain
- **Smart Contract Language**: Solidity
- **Backend Framework**: Flask (for managing API requests and blockchain interactions)
- **Blockchain Interaction**: Web3.py (to connect Flask with Ethereum)
- **Development Tools**: Ganache (local blockchain testing), Truffle (smart contract development)
- **Authentication**: MetaMask (secure login and transaction verification)
- **Frontend Technologies**: HTML, CSS, JavaScript, Bootstrap (for UI development)
- **Database**: MongoDB
- **Code Editor**: Visual Studio Code

This setup ensures a secure, efficient, and scalable environment for decentralized healthcare record

The system design phase has established a well-structured architecture for a blockchain-based healthcare system, ensuring secure, transparent, and efficient electronic health record (EHR) management. By integrating patient and doctor authentication, report generation, access control, and blockchain-based data security, the design ensures seamless medical record handling while maintaining patient privacy and regulatory compliance. The flow of data and interactions between patients, doctors, and the system has been carefully structured to provide an efficient and decentralized approach to healthcare management.

With the system design finalized, the next chapter focuses on system implementation, detailing the development process, tools used, and the integration of smart contracts, blockchain transactions, and user interface components into the application.

CHAPTER 4

SYSTEM IMPLEMENTATION