PATIENT RECORD MANAGEMENT

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

Use Case Report

submitted by

K.Lavanya Sri

(22501A0588)

Under the guidance of

Mr. A. Prashant, Asst. Prof.

Department of Computer Science and Engineering

Prasad V Potluri Siddhartha Institute of Technology

(Permanently affiliated to JNTU-Kakinada, Approved by AICTE)

(An NBA & NAAC accredited and ISO 9001:2015 certified institute)

Kanuru, Vijayawada-520 007

2024-25

Prasad V Potluri Siddhartha Institute of Technology

(Permanently affiliated to JNTU-Kakinada, Approved by AICTE)

(An NBA & NAAC accredited and ISO 9001:2015 certified institute)

Kanuru, Vijayawada-520 007

CERTIFICATE

This is to certify that the Use Case report entitled **"PATIENT RECORD MANAGEMENT"** that is being submitted by **K.Lavanya Sri(22501A0588)** as part of Assignment-1 and Assignment-2 for the **Blockchain Technology**(**20CS4601C)** course in **3-2** during the academic year **2024-25**.

Course Coordinator
Mr. A. Prashant
Assistant Professor,
Department of CSE,
PVPSIT, Vijayawada

Head of the Department
Dr. A. Jayalakshmi,
Professor and Head,
Department of CSE,
PVPSIT, Vijayawada

MARKS

ASSIGNMENT-1: ____/5

ASSIGNMENT-2:_____ /5

INDEX

1. INTRODUCTION

Efficient and secure management of patient records is a critical aspect of modern healthcare systems. Electronic Medical Records (EMRs) have replaced traditional paper-based records, enhancing accessibility and reducing human errors. However, current EMR systems face challenges related to interoperability, security, and data privacy. These issues arise due to centralized data storage, limited patient control, and the lack of seamless data sharing among healthcare providers. In many healthcare systems, patient records are stored in isolated silos, making it difficult for different medical institutions to access a patient's medical history when needed, leading to inefficiencies and potential risks to patient safety [1].

Blockchain technology offers a promising solution to these challenges by providing a decentralized, tamper-resistant, and secure data management system. Unlike traditional EMR systems, blockchain ensures that medical records are securely stored and accessed only by authorized entities[3].The implementation of blockchain-based patient record management allows patients to have full control over their medical data, deciding who can access their records and under what conditions. This enhances security, transparency, and trust in healthcare systems [2].

A permissioned block-chain framework is well-suited for healthcare applications, as it allows only authorized participants, such as hospitals, doctors, and insurance providers, to access medical records. Smart contracts further streamline access control, ensuring compliance with healthcare regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) [3]. By integrating block-chain technology into EMR management, healthcare institutions can improve data integrity, prevent unauthorized modifications, and facilitate secure data sharing across institutions.[2]

This report presents a blockchain-based patient record management system that aims to enhance security, accessibility, and interoperability in healthcare. The proposed system leverages blockchain technology to ensure efficient record-keeping, controlled access, and seamless data sharing among stakeholders while giving patients full ownership of their health data[10].

2. BACKGROUND

The implementation of Electronic Medical Records (EMRs) has significantly improved healthcare efficiency by enabling better data management, accessibility, and decision-making. However, traditional EMR systems face critical limitations in terms of interoperability, security, patient control, and data integrity. These challenges often lead to fragmented patient records, privacy concerns, and inefficiencies in healthcare services [1].

2.1 Challenges in Traditional EMR Systems

2.1.1 Data Fragmentation and Limited Interoperability

Most healthcare institutions operate isolated EMR systems, making it difficult to share patient data across hospitals, clinics, and specialists. This results in incomplete medical histories, leading to delayed diagnoses, redundant tests, and inefficient treatment plans. Patients receiving treatment from multiple providers often face difficulty in consolidating their records, which can impact the quality of care [4].

2.1.2 Security and Privacy Risks

Traditional EMRs store patient data in centralized databases, making them vulnerable to hacking, ransomware attacks, and unauthorized access. Cybersecurity threats in healthcare have increased, with incidents of data breaches exposing sensitive medical and personal information. Moreover, patient data is often shared without explicit consent, raising concerns about privacy violations and regulatory non-compliance [2].

2.1.3 Lack of Patient Control Over Medical Records

In most conventional EMR systems, healthcare providers control access to medical records, limiting patient autonomy. This lack of transparency makes it difficult for patients to monitor who accesses their data or grant selective permissions. Unauthorized modifications can also compromise data integrity, potentially leading to misdiagnoses or medical malpractice issues [1].

2.2 Blockchain as a Solution for Patient Record Management

Blockchain technology provides a decentralized, secure, and transparent alternative to traditional EMR systems. By leveraging permissioned blockchain frameworks such as Hyperledger Fabric, healthcare providers can enhance data security, interoperability, and patient-centric control.

2.2.1 Key Benefits of Blockchain-Based EMR Systems

- **Decentralized and Secure Data Storage** – Eliminates centralized points of failure, reducing cybersecurity threats.
- **Seamless Interoperability** – Enables secure sharing of medical records across healthcare institutions.
- **Patient-Controlled Access** – Empowers patients to decide who can view or modify their medical records.
- **Immutability and Data Integrity** – Ensures medical records cannot be altered or deleted without proper authorization.

By integrating Blockchain, healthcare institutions can establish a secure, permissioned blockchain network, ensuring compliance with healthcare data protection regulations and enhancing overall efficiency in patient record management [3].

The limitations of traditional EMR systems highlight the urgent need for a secure, interoperable, and patient-centric healthcare record management system. Blockchain technology addresses these challenges by providing data integrity, transparency, and decentralized access control. The following sections will explore the technical aspects and real-world applications of blockchain in healthcare, demonstrating its potential to revolutionize patient record management.

3.BLOCKCHAIN BASICS

3.1 Overview of Blockchain Technology

Blockchain is a distributed ledger technology (DLT) that ensures secure, transparent, and immutable transaction recording across a decentralized network [1]. Unlike traditional centralized databases, blockchain stores information across multiple nodes, reducing risks of data manipulation, single points of failure, and unauthorized modifications. Each block contains a cryptographic hash, a timestamp, and transaction details, forming a chain of blocks where each block is linked to the previous one, ensuring data integrity [2][10].

3.1.1 Key Components of Blockchain

- **Blocks** – Data structures that store a batch of transactions and link to previous blocks through a hash [3].
- **Cryptographic Hashing** – A security mechanism that converts transaction data into a unique fixed-length string, ensuring data integrity.
- **Consensus Mechanism** – A process that allows network participants to agree on valid transactions (e.g., Proof of Work, Proof of Stake) [5].
- **Smart Contracts** – Self-executing contracts stored on the blockchain that automatically enforce agreements when predefined conditions are met [6].
- **Decentralized Network** – A distributed architecture where multiple nodes maintain and validate records without relying on a central authority [2].

3.2 Types of Blockchain

Blockchain networks are categorized based on their accessibility, governance, and participation rights :

3.2.1 Public Blockchain – Open networks where anyone can participate in transactions and validation (e.g., Bitcoin, Ethereum) [7].

3.2.2 Private Blockchain – Restricted networks controlled by a single organization, allowing only authorized participants to access and validate data [4].

3.2.3 Consortium Blockchain – Semi-decentralized networks managed by a group of organizations, balancing security and transparency (e.g., R3 Corda, Hyperledger Fabric) [5].

3.2.4 Hybrid Blockchain – A combination of public and private blockchains, ensuring selective transparency while maintaining security and efficiency [6].

3.2.5 Permissionless Blockchain – Also known as open or public blockchains, these networks allow anyone to participate in transaction validation without restrictions. Examples include Bitcoin and Ethereum, where no central authority controls access .

3.2.6 Permissioned Blockchain – A controlled blockchain where only authorized participants can validate transactions and access stored data. This model is widely used in enterprise applications for security and regulatory compliance, with Hyperledger Fabric being a prominent example [5].

3.3 Advantages of Blockchain Technology

Blockchain offers numerous benefits, making it suitable for applications in finance, healthcare, supply chain, and identity management :

3.3.1 Security and Immutability – Transactions recorded on the block-chain are immutable, preventing tampering and fraud[4].

3.3.2 Transparency and Trust – Decentralized consensus mechanisms ensure that all participants have access to verifiable records .

3.3.3 Reduced Operational Costs – Eliminates intermediaries, reducing transaction and verification costs [5].

3.3.4 Improved Data Integrity – Cryptographic hashing and decentralized validation enhance data accuracy and reliability

3.3.5 Efficient Record-Keeping – Automates and streamlines documentation processes, ensuring easy access and auditability [4].

3.4 Challenges in Blockchain Adoption

Despite its advantages, blockchain faces several challenges that impact its widespread implementation :

3.4.1 Scalability Issues – Public blockchains like Bitcoin and Ethereum experience slow transaction processing times due to network congestion [7].

3.4.2 Energy Consumption – Proof of Work (PoW) consensus mechanisms require extensive computational power, raising environmental concerns [5].

3.4.3 Regulatory and Legal Uncertainty – The evolving legal landscape surrounding blockchain creates compliance challenges for businesses.

3.4.4 Interoperability – Different blockchain networks lack seamless communication and data exchange standards [3].

3.4.5 High Initial Implementation Costs – Integrating blockchain with existing systems can be expensive and require specialized expertise .

3.5 Blockchain in Healthcare

Blockchain has emerged as a promising solution for enhancing data security, patient privacy, and interoperability in healthcare:

3.5.1 Secure Medical Records Management – Blockchain ensures tamper-proof storage and controlled access to patient records, reducing data breaches [2].

3.5.2 Patient-Centric Data Access – Enables patients to control and grant permissions for sharing medical records with healthcare providers [4].

3.5.3 Drug Traceability – Ensures transparency in the pharmaceutical supply chain, reducing counterfeit drugs [6].

3.5.4 Clinical Trials and Research – Enhances the integrity and reproducibility of medical research by providing an immutable data history .

4.USE CASE OVERVIEW

The rapid advancement of digital technologies has led to significant improvements in the healthcare industry. One of the most critical aspects of healthcare is Electronic Health Records (EHRs), which store a patient's complete medical history, including diagnoses, treatments, lab reports, prescriptions, and administrative records. However, existing EHR systems suffer from issues such as security vulnerabilities, data breaches, lack of patient control, and poor interoperability between different healthcare institutions[10].

To address these challenges, this proposed system integrates blockchain technology into a Next.js-based web application, leveraging Ethereum blockchain and InterPlanetary File System (IPFS) for decentralized storage, security, and seamless access control. The system is designed to ensure that:

- Patient data is securely stored and encrypted.
- Only authorized individuals can access the records.
- Patients have full control over their medical data.

By utilizing blockchain's immutable and decentralized nature, the system eliminates the need for centralized authorities, reducing the risks of data breaches, unauthorized access, and data tampering.[8][9].

4.1 Objectives

- To develop a secure and decentralized Electronic Health Record (EHR) management system using blockchain technology.
- To provide patients with full control over their medical data, ensuring privacy and security.
- To enable seamless interoperability between healthcare providers for efficient medical data exchange.
- To leverage IPFS for cost-effective and scalable storage of medical records.
- To implement robust authentication and authorization mechanisms for access control.

4.2 Scope

- The system will provide a web-based interface for patients and healthcare providers to interact securely.
- It will utilize Ethereum-based blockchain for recording transactions related to medical data access.
- The system will incorporate IPFS for decentralized storage of encrypted EHRs.
- Patients will have the ability to grant or revoke access to their medical records for specific healthcare providers.
- The system will support audit logging to track all access requests and modifications.
- Future enhancements may include integration with AI for predictive healthcare analytics and mobile application support.

4.3 Key Features:

4.3.1 Patient-Centric Access Control: Patients can selectively grant or revoke access to healthcare providers, ensuring data privacy.

4.3.2 Decentralized & Secure Data Storage: EHRs are stored securely in a distributed network, reducing the risk of data breaches.

4.3.3 Interoperability: Enables secure data exchange among healthcare institutions for better patient care.

4.3.4 Efficient Record Management: Uses IPFS (InterPlanetary File System) for scalable storage and blockchain for transactions, ensuring immutability and security.

4.4 System Architecture

The system architecture is structured into three distinct layers, each handling specific functionalities for managing EHRs securely and efficiently as demonstrated in **Fig. 4.1.**

4.4.1. User Management Layer

- Provides an interactive interface for patients and healthcare providers.
- Allows users to input, view, and retrieve their medical records securely.

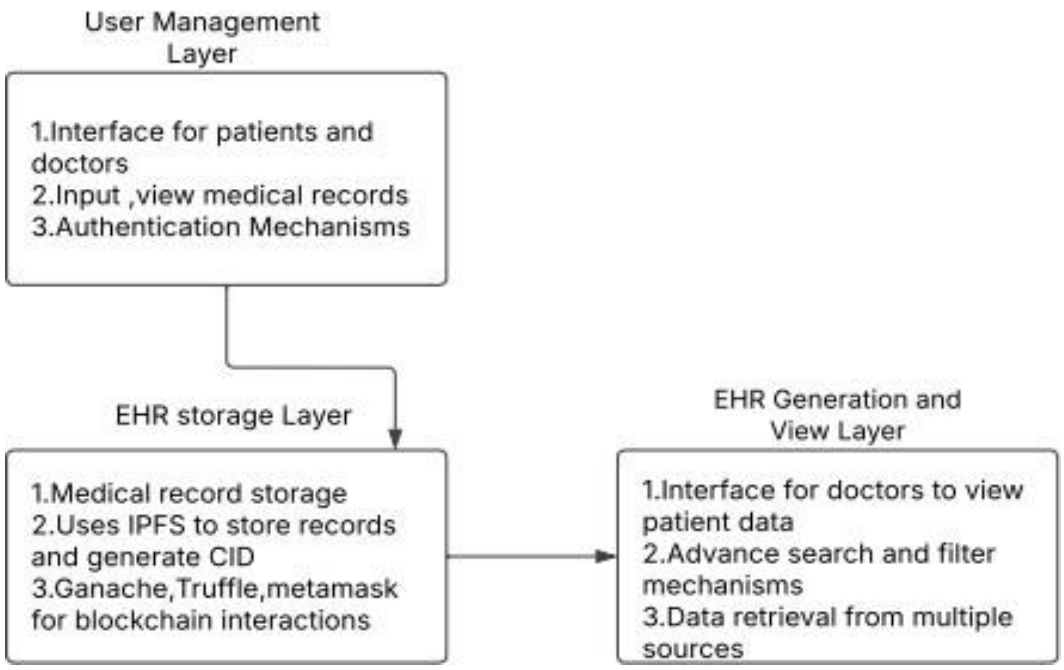
- Implements authentication mechanisms (private and public key-based access control).

4.4.2. EHR Storage Layer

- Acts as the backbone of the system, managing data storage.
- Uses IPFS to store encrypted medical records and Ethereum blockchain to store the hash of each record (CID).
- Incorporates APIs for seamless data exchange between the frontend and storage components.
- Utilizes Next.js, Ganache, Truffle, and MetaMask for blockchain interactions.

4.4.3. EHR Generation and View Layer

- Provides an interface for healthcare providers to access patient data.
- Includes advanced search, filtering, and visualization tools for analyzing patient records.
- Enables data retrieval from multiple sources, ensuring a comprehensive overview of a patient's health history.[8]


User Management Layer

1.Interface for patients and doctors
2.Input ,view medical records
3.Authentication Mechanisms

EHR storage Layer

1.Medical record storage
2.Uses IPFS to store records and generate CID
3.Ganache,Truffle,metamask for blockchain interactions

EHR Generation and View Layer

1.Interface for doctors to view patient data
2.Advance search and filter mechanisms
3.Data retrieval from multiple sources

Fig. 4.1: Layers of Patient record management system

4.5 Flow of the System

Flow of the system is represented in 6 steps as shown in **Fig. 4.2**

4.5.1 Registration & Key Generation

- Each user (patient or doctor) registers in the system.
- Three cryptographic keys are generated:

Private key: Stored securely on the user's device

Public key: Stored in the blockchain database.

Symmetric key: Encrypted using the public key and stored on the server.

4.5.2 Encrypting & Storing EHRs in IPFS

- Medical records are converted into encrypted PDF files.
- Each file is encrypted using a symmetric key and uploaded to IPFS.
- IPFS generates a unique **CID (Content Identifier)**, which is recorded on the blockchain

4.5.3 Granting Access to Healthcare Provider

- The patient provides their private key to authorize access.
- The blockchain is queried to retrieve the CID of the requested medical record.
- The encrypted file is retrieved from IPFS and decrypted using the symmetric key.

4.5.4 Retrieving & Viewing Medical Records

- Authorized users (doctors, lab technicians) request access to EHRs.
- Upon verification, the requested records are decrypted and displayed securely.

4.5.5 Secure Data Retrieval Process

- The system verifies the access request by checking the user's credentials.
- If authorized, the corresponding CID is retrieved from the blockchain.
- The encrypted data is fetched from IPFS and decrypted using the provided symmetric key.
- Access logs are updated to ensure transparency and security monitoring.

4.5.6 Auditing and Logging

- Every transaction is recorded on the blockchain for transparency.
- Patients can view access logs to monitor who accessed their records and when.
- Any unauthorized access attempts are flagged and notified to relevant authorities.

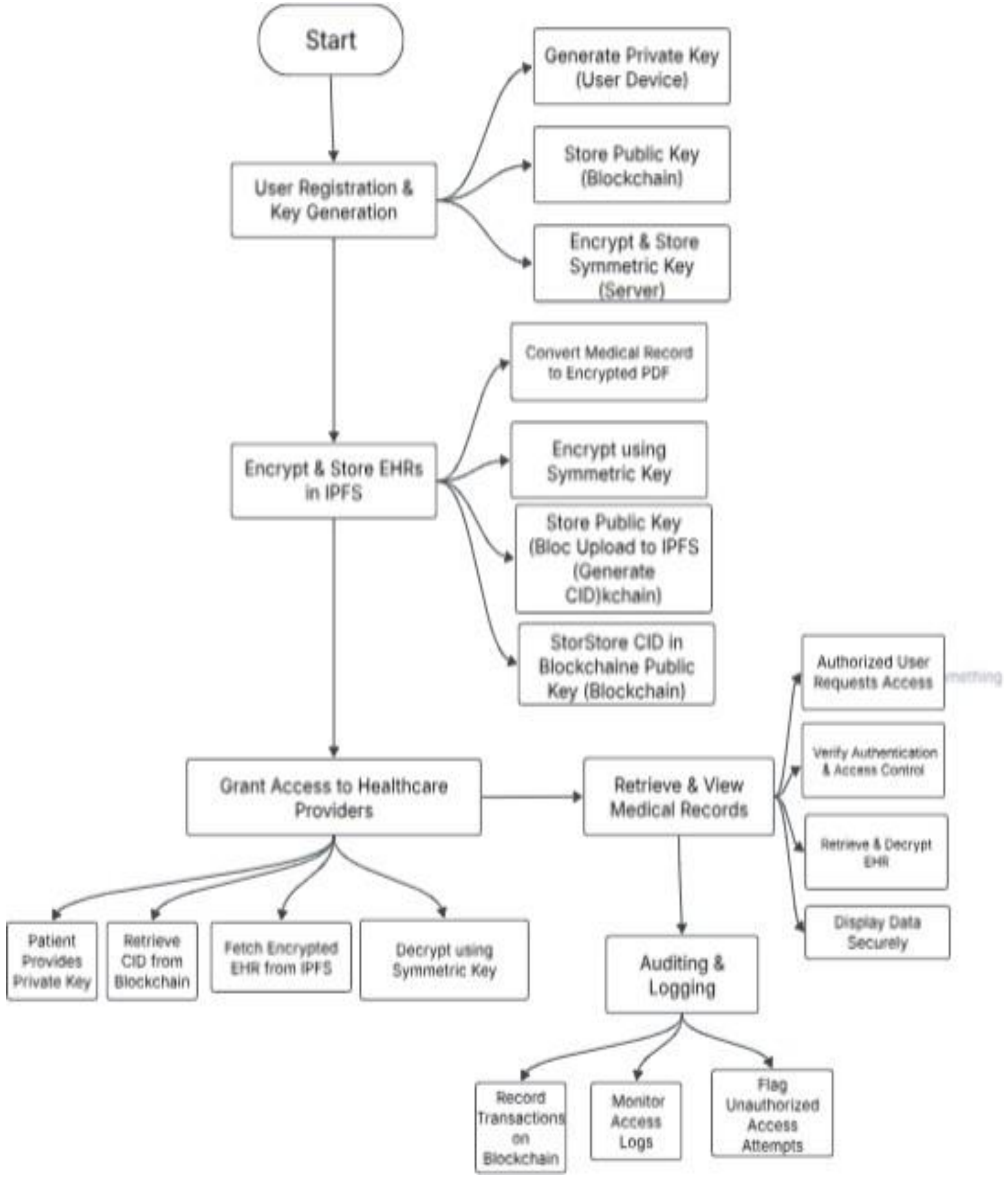

Start
User Registration & Key Generation
Generate Private Key (User Device)
Store Public Key (Blockchain)
Encrypt & Store Symmetric Key (Server)
Encrypt & Store EHRs in IPFS
Convert Medical Record to Encrypted PDF
Encrypt using Symmetric Key
Store Public Key (Bloc Upload to IPFS (Generate CID)kchain)
StorStore CID in Blockchaine Public Key (Blockchain)
Grant Access to Healthcare Providers
Patient Provides Private Key
Retrieve CID from Blockchain
Fetch Encrypted EHR from IPFS
Decrypt using Symmetric Key
Retrieve & View Medical Records
Authorized User Requests Access
mething
Verify Authentication & Access Control
Retrieve & Decrypt EHR
Display Data Securely
Auditing & Logging
Record Transactions on Blockchain
Monitor Access Logs
Flag Unauthorized Access Attempts

Fig. 4.2: Flow of the EHR management

5.IMPLEMENTATION

5.1 Define the EHR Workflow:

- Identify stakeholders: Patients, Doctors, Hospitals, Laboratories, Pharmacies.
- Determine what data will be stored: Patient ID, Medical History, Diagnosis Reports, Treatment Records, Prescriptions, Lab Results, Access Permissions.
- Define key operations: Patient Registration, Data Encryption & Storage, Access Control & Authorization, Medical Record Retrieval, Audit & Logging.

5.2 Choose the Blockchain Type:

- Type: Public-Permissioned Blockchain
- Blockchain Used: Ethereum for transactions and IPFS for decentralized storage
- Permission Model: Patients and doctors require authorization to access medical records.

5.3 Design Smart Contracts for the Supply Chain

5.3.1 Smart contracts automate:

- Medical Record Registration (Immutable storage of patient data.
- Access Control (Grant/Revoke permissions to doctors)
- Data Retrieval (Securely fetch and decrypt patient records)

5.4 Develop & Deploy Smart Contracts

Example Solidity Code for Electronic health records:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract EHRSecurity {
    struct MedicalRecord {
```

```
    string cid; // IPFS Content Identifier
    address patient;
    address doctor;
    bool accessGranted;
}
mapping(uint256 => MedicalRecord) public records;
mapping(address => uint256[]) public patientRecords;
mapping(address => mapping(address => bool)) public accessPermissions;
uint256 public recordCount;
event RecordAdded(uint256 recordId, string cid, address indexed patient);
event AccessGranted(address indexed patient, address indexed doctor);
event AccessRevoked(address indexed patient, address indexed doctor);
modifier onlyPatient() {
    require(patientRecords[msg.sender].length > 0, "Not a registered patient");
    _;
}
function addRecord(string memory _cid) public {
    recordCount++;
    records[recordCount] = MedicalRecord(_cid, msg.sender, address(0), false);
    patientRecords[msg.sender].push(recordCount);
    emit RecordAdded(recordCount, _cid, msg.sender);
}
function grantAccess(address _doctor) public onlyPatient {
    accessPermissions[msg.sender][_doctor] = true;
    emit AccessGranted(msg.sender, _doctor);
}
function revokeAccess(address _doctor) public onlyPatient {
    accessPermissions[msg.sender][_doctor] = false;
```

```
            emit AccessRevoked(msg.sender, _doctor);}
        function viewRecord(uint256 _recordId) public view returns (string memory) {
            MedicalRecord storage record = records[_recordId];
            require(record.patient == msg.sender || accessPermissions[record.patient][msg.sender],
        "Access denied");
            return record.cid;
}
      }
      function registerProduct(string memory _name, string memory _origin) public {
        productCount++;
        products[productCount] = Product(_name, _origin, block.timestamp, msg.sender); emit
        ProductRegistered(productCount, _name, _origin, msg.sender);
      }
      function transferOwnership(uint _productId, address _newOwner) public {
        require(products[_productId].owner == msg.sender, "Only owner can transfer");
        address oldOwner = products[_productId].owner;
        products[_productId].owner = _newOwner;

        emit OwnershipTransferred(_productId, oldOwner, _newOwner);

      } }
```

5.5 Frontend & Web3 Integration

- Use React.js/Next.js for the UI.
- Use Web3.js or Ethers.js to interact with smart contracts.
- MetaMask for wallet-based authentication.

5.6 Test the Smart Contracts:

- Deploy on Ganache (Local Ethereum Blockchain) for testing.

- Perform unit tests with Truffle or Hardhat.
- Check for vulnerabilities using Slither (Solidity analyzer).

5.7 Deploy on a Blockchain Network

- Deploy on Ethereum (Mainnet or Testnet like Goerli, Sepolia).
- Use IPFS (InterPlanetary File System) for decentralized data storage.

5.8 Monitor & Maintain the System

- Use Chainlink oracles for external data verification.
- Implement event logging & real-time monitoring.
- Regularly update smart contracts to improve security.

5.9 Ensure Compliance & Scalability

- Align with HIPAA, GDPR, and healthcare data regulations.
- Optimize gas fees using Layer 2 solutions (Polygon, Optimism).
- Scale using sidechains or sharding for enterprise adoption.

By implementing blockchain smart contracts, EHRs become fully transparent, fraud- proof, and efficient.[7]

6.ADVANTAGES

Blockchain in EHR enhances security, ensures patient control over data access, and enables seamless, tamper-proof record sharing. It improves interoperability, reduces fraud, and streamlines healthcare operations while ensuring compliance with regulations like HIPAA and GDPR.

6.1 Enhanced Security & Privacy

- Utilizes cryptographic encryption (AES, RSA) to protect sensitive medical data.
- Ensures tamper-proof storage using blockchain immutability.
- Multi-factor authentication (MFA) prevents unauthorized access.

6.2 Patient-Centric Data Control

- Patients have full ownership of their medical records.
- Access permissions can be granted or revoked in real-time via smart contracts.
- Eliminates reliance on third-party data custodians.

6.3 Interoperability Across Healthcare Providers

- Blockchain enables seamless data exchange between hospitals, labs, and pharmacies.
- FHIR (Fast Healthcare Interoperability Resources) compatibility ensures integration with existing EHR systems.
- Reduces duplicate tests and administrative delays.

6.4 Reduced Fraud & Data Manipulation

- Immutable blockchain ledger prevents alteration of medical records.
- Access logs & audits track every request and modification.
- Eliminates fraudulent insurance claims and fake prescriptions.

6.5 Faster & Cost-Effective Data Retrieval

- Decentralized storage (IPFS) allows quick access to medical records.
- Eliminates costly centralized data storage fees.
- Smart contracts automate medical data retrieval without intermediaries.

6.6 Increased Transparency & Compliance

- Blockchain ensures compliance with HIPAA, GDPR, and other healthcare regulations.
- Smart contracts enforce ethical data handling and audit trails.
- Patients and regulators can verify access history transparently.

6.7 Disaster Recovery & Data Redundancy

- Decentralized storage (IPFS) prevents data loss from server failures.
- Ensures availability and redundancy across multiple nodes.
- Patients never lose access to their medical history.

6.8 Elimination of Third-Party Dependencies

- Traditional EHR systems rely on centralized institutions for record storage and access management.
- Blockchain removes intermediaries, allowing direct and transparent interactions between patients and healthcare providers.

7.CHALLENGES

7.1 Scalability Issues:

- ·Blockchain networks, particularly Ethereum, have limited transaction throughput, leading to delays in processing medical data.
- High network congestion can increase transaction fees (gas costs), making frequent medical record updates costly.
- Layer 2 solutions (e.g., rollups, sidechains) may be required to enhance scalability.

7.2 High Computational & Storage Costs:

- Storing large medical records directly on the blockchain is impractical due to high storage costs and slow retrieval speeds.
- Off-chain storage solutions like IPFS (InterPlanetary File System) or cloud-based encrypted storage must be integrated, adding complexity.
- Efficient hashing mechanisms are required to link large data files securely without bloating the blockchain.

7.3 High Transaction Costs

- Gas fees on public blockchains like Ethereum can be expensive.
- Utilize Layer 2 scaling solutions or hybrid blockchain models for cost efficiency.

7.4 Data Ownership & Governance Issues:

- Determining who owns the medical data (patients, healthcare providers, or institutions) is a critical challenge.
- Blockchain ensures data immutability, but disputes over incorrect records or malicious data entry need a resolution mechanism.
- Governance frameworks must be established to handle data disputes, unauthorized changes, and accountability.

7.5 Energy Consumption Concerns:

- Public blockchains like Ethereum (Proof of Work-based) historically required high energy consumption, raising sustainability concerns.
- Transitioning to Proof of Stake (PoS) or using private/permissioned blockchains can mitigate environmental impact but may reduce decentralization.

7.6 Latency in Data Retrieval & Updates:

- Retrieving medical records from blockchain-based storage can be slower than centralized databases.
- In emergency medical situations, real-time access to patient history is crucial, but blockchain verification may introduce delays.
- Hybrid solutions integrating on-chain verification with off-chain storage can improve response times.

8.CONCLUSION

The implementation of a blockchain-based Electronic Health Record (EHR) system enhances the security, privacy, and efficiency of healthcare data management. By leveraging blockchain for transactions and decentralized storage, the system ensures data integrity, immutability, and patient control over medical records. The use of smart contracts automates key processes such as access control, auditing, and data sharing, reducing the risks of fraud and unauthorized access. This approach contributes to advancements in healthcare by improving data security, fostering innovation, and promoting transparency in medical record management. Additionally, it supports sustainable development by strengthening digital infrastructure, enhancing patient-centric care, and ensuring equitable access to secure health information. Future advancements may include AI-driven analytics, IoT integration for real-time health tracking, and interoperability across healthcare systems, further improving the overall efficiency and effectiveness of digital healthcare.

9.SDG’s ADDRESSED

The blockchain-based Electronic Health Record (EHR) system addresses multiple Sustainable Development Goals (SDGs) by enhancing healthcare security, accessibility, and efficiency:

- **SDG 3: Good Health & Well-being**

  Justification: Ensures secure, tamper-proof medical records, improving patient safety, diagnosis, and healthcare quality.
- **SDG 9: Industry, Innovation & Infrastructure**

  Justification: Strengthens digital healthcare infrastructure through secure data storage, smart contracts, and interoperability.
- **SDG 10: Reduced Inequalities**

  Justification: Promotes equitable healthcare access, benefiting underserved and remote populations.
- **SDG 12: Responsible Consumption & Production**

  Justification: Enhances resource efficiency by eliminating redundant tests and optimizing medical supply chains.
- **SDG 16: Peace, Justice & Strong Institutions**

  Justification: Ensures transparency, compliance, and fraud prevention in medical data management.

By integrating blockchain technology in EHR management, this system contributes to a secure, efficient, and patient-centric healthcare model, aligning with global efforts to improve healthcare accessibility and digital transformation.

10.REFERENCES

1. S. R. Simon, R. Kaushal, P. D. Cleary, et al., “Electronic Health Records: Barriers, Expectations, and Benefits,” *American Journal of Medicine(* vol. 114, no. 5, pp. 397-403) 2003.

2. J. Zhang, B. Schmidt, J. White, et al., “Blockchain Technology Use Cases in Healthcare,” *Advances in Computers(*vol. 111, pp. 1-42) 2018.

3. M. Benchoufi and P. Ravaud, “Blockchain Technology for Improving Clinical Research Quality,” *Trials,*(vol. 18, no. 335, pp. 1-5) 2017.

4. X. Yue, H. Wang, D. Jin, et al., “Healthcare Data Gateways: A Case Study of a Smart Contract-Based Data Marketplace,” *IEEE Access(* vol. 6, pp. 60136-60146) 2018.

5. M. Kuo, T. Rojas, and R. Ohno-Machado, “Comparison of Blockchain Platforms: A Systematic Review and Healthcare Applications,” *Journal of the American Medical Informatics Association(*vol. 26, no. 5, pp. 462-478) 2019.

6. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using Blockchain for Medical Data Access and Permission Management,” *Proceedings of the IEEE International Conference on Open and Big Data (OBD)(* pp. 25-30) 2016.

7. P. Zhang, D. Walker, J. White, and D. Schmidt, “A Blockchain-Based Approach to Health Information Exchange Networks,” *Future Generation Computer Systems(*vol. 72, pp. 477-486)2017.

8. https://www.researchgate.net/publication/374510360_Blockchain-based_Electronic_Health_Record_Management_System. (last date of visit : 14-03-2025)

9. Yang, Huihui, and Bian Yang. "A blockchain-based approach to the secure sharing of healthcare data." In Proceedings of the norwegian information security conference(pp. 100-111.)Oslo, Norway: Nisk J, 2017.

10. Nishi, Farjana Khanam, Mahizebin Shams-E-Mofiz, Mohammad Monirujjaman Khan, Abdulmajeed Alsufyani, Sami Bourouis, Punit Gupta, and Dinesh Kumar Saini. "Electronic healthcare data record security using blockchain and smart contract." Journal of Sensors 2022 (2022): 1-22.

11.APPENDIX A

https://drive.google.com/drive/folders/1Z5edJbD-OHlsog68SVO5oT5CTNRQUhmb?usp=sharing